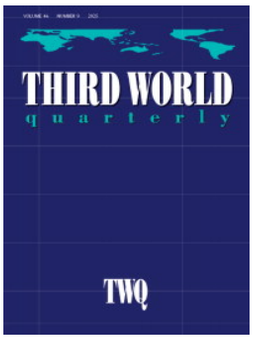

Routledge
Taylor & Francis Group

Third World Quarterly

ISSN: 0143-6597 (Print) 1360-2241 (Online) Journal homepage: www.tandfonline.com/journals/ctwq20

Biometric coloniality: digital consensus and the biometric state in Africa

Victor Chidubem Iwuoha & Martin Doevenspeck

To cite this article: Victor Chidubem Iwuoha & Martin Doevenspeck (21 Aug 2025): Biometric coloniality: digital consensus and the biometric state in Africa, Third World Quarterly, DOI: 10.1080/01436597.2025.2539731

To link to this article: https://doi.org/10.1080/01436597.2025.2539731

THIRD WORLD QUARTERLY
https://doi.org/10.1080/01436597.2025.2539731

Biometric coloniality: digital consensus and the biometric state in Africa

Victor Chidubem Iwuoha[a,b] and Martin Doevenspeck[c]

[a]Bayreuth Academy of Advanced African Studies, University of Bayreuth, Bayreuth, Germany; [b]Department of Political Science, University of Nigeria, Nsukka, Nigeria; [c]Department of Geography, University of Bayreuth, Bayreuth, Germany

ABSTRACT

This article frames the concept of biometric coloniality of power in the Global South – to explain how alliances of powerful global institutions, big tech companies and the compliant emerging biometric states operate on the basis of a lucrative digital consensus to carry out techno-capitalist biometric ID interventions, which reproduce colonial relations of domination. We use Nigeria's experience and examples from other African countries to demonstrate that the emergence of biometric states is linked to specific interconnected spaces of biometric data struggle and exploitation where the uses/abuses of biometric data are performed and contested. This article maps out new biometric orders of power at multiple levels/scales, and explicitly draws out ways biometric categories and social hierarchies are used to produce racialised and gendered subjects. The article argues that biometric coloniality inherently creates a biometric state with a peculiar character of biometric dysfunctionality and authoritarianism, both effectively institutionalised to the exclusion and disempowerment of the citizens/biometric subjects. We conclude that the chain of unbridled extraction of digital data, its commodification and dispossession, which is bounded by digital consensus, can only be broken by the conscious awakening of digital subjects.

ARTICLE HISTORY
Received 31 August 2024
Accepted 23 July 2025

KEYWORDS
biometric coloniality
digital consensus
biometric ID system
biometric state
ID4D

Introduction

Legal identity for all is a critical item on the agenda of the global community, pencilled in the UN's sustainable development goals (SDG 16.9). The target is to capture over 1.1 billion people without proof of legal identity, half of whom live in Sub-Saharan Africa, in a biometric ID system. This agenda has spiralled into the creation of a competitive global biometric market estimated at US$50.6 billion annually (Acuity Market Intelligence 2022). The World Bank estimates approximately US$6 billion to meet the cost of Africa's digital identification and civil registration needs. Consequently, African countries are rapidly developing multiple biometric identification systems to drag into a digital economy over 500 million people on the continent without proof of identity. Nigeria, Africa's most populous country, represents

CONTACT Victor Chidubem Iwuoha victor.iwuoha@unn.edu.ng

a major signpost of biometric digital penetration on the continent. In the past decade, Nigeria invested over US$3 billion on functional biometric ID systems. In 2015 alone, over US$627 million was spent on biometric elections, including US$200 spent on biometric voting technology (Gelb and Diofasi 2016). In 2023, US$95 million was spent on biometric voting technology (INEC 2024). Biometric enrolment of employees in federal agencies uncovered over 60,000 ghost workers on the payroll, saving about US$1.12 billion in salaries between 2007 and 2014 (World Bank 2018).

Currently, Nigeria's biometric identity programme (ID4D), managed by the National Identity Management Commission (NIMC), is financed to the tune of US$415 million by the World Bank and partners. The aim is to develop a robust and inclusive foundational ID system that issues a national ID number (NIN) to residents, particularly to facilitate their access to public and private services. Nigeria's burgeoning biometric market has attracted major multinational corporations including DERMALOG Identification Systems, and Idemia and Trüb (a Gemalto subsidiary) which are in charge of the NIN project in which over 104.16 million people had been captured as at January 2024. However, since Nigeria keyed into the World Bank's digital initiative in 2020, the government's drive for mandatory biometric enrolment has been intolerably drastic and exclusionary. In what can be described as state-sponsored disempowerment of the most vulnerable groups, over 38 million people, out of Nigeria's approximately 224 million population (Nnorom 2023), who are still unbanked and without Bank Verification Number (BVN) and NIN have been completely cut off from accessing the government's social security scheme, cash transfers and public services.

Biometrics is a pillar of global capitalism and spread as a travelling technology at the end of the nineteenth century. This was facilitated in the course of the transcontinental mobility of people and goods between India, South Africa and the United Kingdom in the Global North (Breckenridge 2014). Then and now, biometric data is used to prove identity, control mobility and for surveillance (Medina-Doménech 2009). In Africa, digital registration systems and other instruments for the mass identification of people have been increasingly introduced over the past two decades within the framework of development goals such as good governance and have been largely prescribed by the World Bank with its programme 'Identification for Development (ID4D)'. The need for biometric data to modernise administrative structures or organise elections is argued to be a key condition for economic, social and political development (Dalberto et al. 2021). Despite being penetrable as a result of inadequate data protection regulations, these emerging technologies are generating interest from all sides due to the huge African data market (see Figure 1).

The 'coloniality of power' (Quijano 2000, 2007; Mignolo 2007) of biometric identification in contemporary Africa materialises not only in targeted profiling and surveillance for migration control across European external borders (Browne 2012; De Genova 2016; Nishiyama 2015; Pugliese 2010) but also in creating technological dependence, which facilitates a data colonialism that has received relatively less attention so far. Colonial practices are evident in the contemporary domination of Africa's digital sector by external powers, even though they appear subtle, invisible and apparently benign. As with the colonial thrusting of Africa's natural resources on multinational bulwarks that enjoyed trading monopolies and accruable profit, so are today's biometric technology corporations in Africa profiting from Africa's large digital economy and expansive biometric market. Musoni, Domingo, and Ogah (2023) capture the incursion of global capital into Africa's digital market. We represent this information more clearly in Figure 2.

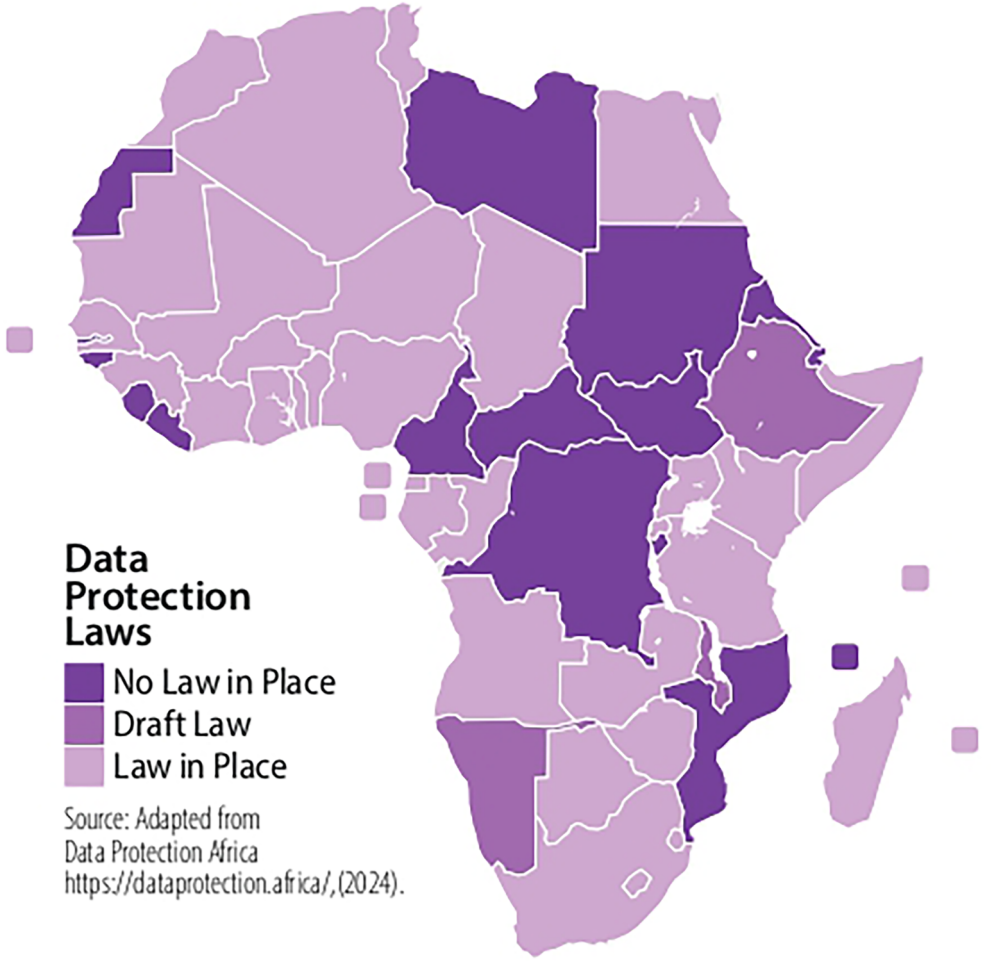

Figure 1. State of data protection laws in Africa. Source: Data Protection Africa.
Source: By Authors.

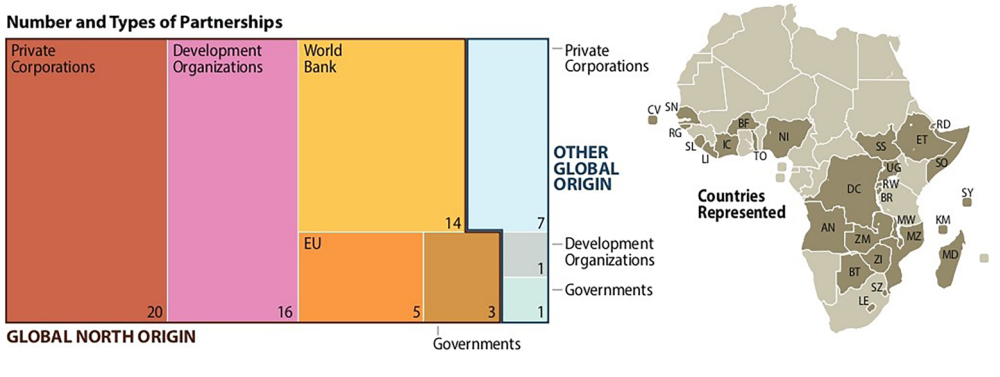

Figure 2. International funding partners behind digital projects in Africa.
Source: By Authors.

The outline of the rest of the paper is as follows: We first present our concept of biometric coloniality. Following our methodological approach, in the main empirical section we present our findings on the biometric state and digital identification landscape in Nigeria and then discuss citizenship exclusion and disempowerment in the Biometric Digital ID Ecosystem before concluding.

Biometric coloniality of power

Today's biometric identification is closely entangled with European colonialism and its racial legacy. Keith Breckenridge described South Africa (2014, 20) as a 'twentieth century laboratory of empire'. In the 19th and 20th centuries, Western scientists, including Francis Galton, who were bent on proving the 'superiority' of 'white people over non-white people across the world', used fingerprinting as anthropological data not only to identify individuals but to trace heredity, ethnicity and race (Cole 2001, 97) and particularly to establish the racial classification of previously unclassified social practice, groups and relationships (Omi and Winant 2015).

In 1857, the British colony of India adopted the fingerprinting system alongside other methods including the use of tattoos and the use of photographs. However, the difficulty in perfecting racial classificatory objectives quashed the utility of some of these methods. Subsequently, Edward Henry, the Police Commissioner in Bengal, adopted the 'Henry System', in which he used mathematical means to conduct fingerprint classification for the Witwatersrand police force. In the beginning of twentieth century, Gandhi used the fingerprinting system to identify the Indian population and control their migration into the Transvaal. Unfortunately, the Transvaal government used the fingerprinting records to apply discriminatory policies against Indian migrants, which sparked public resentment and rejection of Western ID technology in India. In Latin America, including Mexico and Brazil, the fingerprinting system also became a tool for racial classification and discrimination. Under apartheid regime, the state adopted the fingerprinting system in which the biometrics of individuals are harnessed into the new computer technology. Basically, the fingerprinting system promoted racial classification and targeted mostly African illiterates working in the mining sector with fraudulent identification profile, thus enforcing coercion and criminalisation of black labour (Breckenridge 2014).

The 'coloniality of power' entrenches racial hierarchical differences, both mental and cultural, which are structured along the lines of colonial domination (Quijano 2007, 171). Particularly, this coloniality of power deals with knowledge production, which creates a subject-object relation, objectivising the 'other' who is absent and to be observed (Quijano 2007, 172–173). Following on from this, Nishiyama (2015) suggests the concept of coloniality of biometric power to illustrate a specific form of reproduction of colonial structures, knowledge and subject-object relationships. Coleman (2019, 147) reflects on digital colonialism as 'a modern-day "Scramble for Africa" where large-scale tech companies extract, analyse and own user data for profit and market influence with nominal benefit to the data source'. Benefiting from inadequate data protection legislation, powerful technology companies are using their resources to access yet unexploited data of citizens of new biometric states. In this form of colonialism, data are a means of capitalist accumulation by dispossession (Thatcher, David, and Dillon 2016).

Data use and commodification in neoliberal capitalism are performed through the deliberate formation of biometric categories and social hierarchies to produce racialised and gendered subjects across time and space (Couldry and Mejias 2019; Dona 2022). These linkages between biometrics and coloniality inform what we propose as biometric colonialism: the use of a modern biometric identification system to facilitate classification or profiling of individuals, Eurocentrification of technological knowledge and the reproduction of colonial power structures and global digital inequality to reinforce domination and subjugation of clientele states. It describes the instrumentalisation of emerging biometric states in the Global South and in Africa in particular. External power alliances engineer their way and team up with political elites who share intersecting interests to facilitate biometric objectification of individuals for a specific modality of institutionalised discrimination and disempowerment (Iwuoha and Edgar 2024). Doing this usually involves the dispatch of digital aids, tech conglomerates and policies to control Africa's digital economy. In their digital dependence, such as relying on external support/funding from global institutions and tech companies for the development of digital ID infrastructures, biometric states get subjugated as they receive external mandates to enforce colonial interests. The biometric state thus assumes a peculiar character that institutionalises a ruthless and authoritarian approach in the enforcement of externally sponsored biometric ID intervention programmes, often resulting to the oppression, exclusion and disempowerment of the citizens/biometric subjects.

We crafted a novel framework of global digital empire to calibrate three interlinked cycles of biometric coloniality and depict actor-specific analysis (see Figure 3). These biometric categories and social hierarchies are used to produce racialised and gendered subjects.

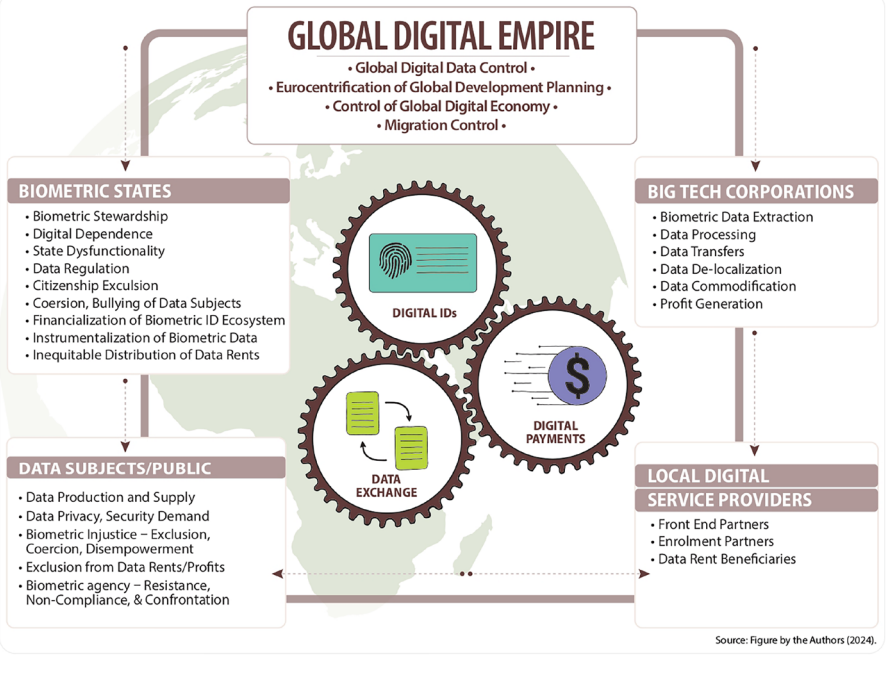

Figure 3. Global digital empire framework and its interconnecting components.
Source: By Authors.

Methods and data

This research is based on qualitative data analysis, semi-structured interviews, FGDs and informal conversations. About 42 in-depth interviews were conducted while 55 FGDs and informal discussions were held across five of Nigeria's cities, namely Abuja, Lagos, Benin, Nsukka and Enugu, between September 2022 and March 2024. A purposive sampling method was used to select 42 stakeholders and experts in biometric ID and the digital enrolment programme for in-depth interviews. These included six NIMC officials (three officials from Abuja headquarters, two officials from Benin regional office and one official from Enugu regional office); 15 NIN enrolment agents (three agents were selected in each of the five study areas); three bank officials (two central bank staff from Enugu regional office and one bank staff member from a commercial bank in Nsukka); and 18 lecturers who specialised in computer science, information and communication technology, mass communication and political science (10 lecturers from University of Nigeria, three lecturers from University of Lagos and five lecturers from Federal University Otuoke). A variety of interview methods were used such as face-to-face contact, zoom meetings, emails, telephone calls and Whatsapp calls/chats. As the majority of the key participants had very tight work schedules, face-to-face contact was not possible in all cases. In such cases, participants were asked to choose alternative interview methods and did so.

FGDs and informal discussions were based on arbitrary cross-sectional sampling in order to elicit the maximum variation of responses from diverse groups of people. These included 55 NIN applicants (including taxi/bus drivers, skilled workers, vendors, shop owners, artisans, public servants, petty traders and passers-by met in the study areas) who were considered to be valuable participants and were asked open-ended questions. The convenience/pre-designed availability research design helped to engage respondents who were conveniently or accidentally available to participate in the research across the study areas. For each study area visited, a snowball approach was used to prevail upon agreed participants to reach out to other prospective participants. Outskirts and remote neighbourhoods within the study areas were visited, but the absence of registration centres in these interior areas indicated that the residents lacked access to biometric ID enrolment, except for those who could afford to visit the city centres.

Overall, the study engaged a total of 97 participants, which included 52 men and 45 women, all above 18 years. The female gender and vulnerable groups including the elderly, extremely poor and physically challenged persons, were given proper attention. Thick descriptions and analysis of all observed phenomena were carried out using a qualitative descriptive, interpretative and logical framing method. All field research ethics and practices, including informed consent, were adhered to in all cases.

Huge African digital data market and global capitalism: arousing desires and challenges from all sides

Africa's technological and digital ID gap forms a major market for global capitalism. The World Bank reports that Africa accounts for more than half of the 850 million people in the world without a proof of identity. This puts Africa on the spot as a lucrative market for biometric ID companies (World Bank 2021). The specialist firm Acuity Market Intelligence estimates that Africa's digital identity and biometrics market alone is worth €1.4 billion (Aït-Hatrit

2020). The rapidly expanding digital ID technology market in Africa records a 21% growth per year more than any other world region (Toesland 2021).

Mostly, companies from the Global North are the primary beneficiaries of this expansion. For example, a global tech giant, Idemia (€2.5 billion in revenues), controls digital ID project in 25 African countries; Idemia is responsible for the largest biometric database on the continent, in Nigeria. Belgium's Semlex, also a significant player, won the big ID market in Côte d'Ivoire, with a contract to manage the new Carte nationale d'identité (CNI) project and supply biometric ID cards, worth €703 million (Angoua 2022). Germany's Veridos (€167 million in revenues in 2017) is active in Uganda, Zambia and Morocco, while French public company IN Groupe (€283.2 million in revenues in 2017) and the German company Mühlbauer (€266.4 million in 2017) control Mozambique and other markets in Africa. Uganda also has a $250 million contract with Russia's Joint Stock Company Global Security and a $126 million agreement with China's Huawei, on CCTV, face, fingerprint and iris-recognition ion technologies (Solon 2024). Some 139 million biometric and digital identity papers were produced in 2019 in Africa and the Middle East (Aït-Hatrit 2020). In Nigeria, Idemia and Trüb (a Gemalto subsidiary) are contract partners for the NIN project through which, as of January 2024, over 100 million Nigerians had received a unique identity number. Safran Identity & Security, a subsidiary of Idemia, handles the upgrade of the ABIS into the new MorphoBSS (Morpho Biometric Search Services) enabled by three types of biometrics: face, iris and fingerprints (Indemia 2017).

Many African countries have also queued up seeking financial aid from global institutions to develop their digital ID platforms. The World Bank has provided €4.4 million to ECOWAS; €1.8 million to Côte d'Ivoire; and €5.3 million to Djibouti to support new identity card projects. Similarly, the United Nations provided support to Cameroon for the production of biometric ID cards issued to 6000 refugees from the Central African Republic (Aljazeera News 2022). In April 2023, the World Bank authorised a $390 million financing agreement for the Kenya Digital Economy Acceleration Project's initial phase (Sehloho 2024).

It is exactly this crystalisation of the biometric compliant states, global institutions and the techno-capitalist sphere that accentuates the growing importance of Africa's digital data market to global capitalism. More importantly, the techno-capitalist relationship between global digital powers and the emerging biometric state in Africa is very remarkable. This relationship particularly underscores a condition of coloniality of power and technological dependence in which the local technological gaps account for the dominance of Africa's biometric industry by big corporations, over local tech companies. Nevertheless, Indian firms are also increasingly becoming relevant in this market, with their growing influence (particularly in software). This rise holds potential to offset the international mechanisms of domination.

Four key actors in the digital ID ecosystem are significant, namely, the global digital empire, biometric states, tech companies and data subjects. These actors represent contested power structures that produce specific forms of biometric colonialities. First is the overbearing character of dominant global digital controllers who enforce global biometricisation and digitalisation, digital governance, dictation and control of biometric states. In this regime, three dominant geopolitical players stand out – the European Union, United States and China – and they mainly constitute the new digital empire. Others include the World Bank, UNDP and the Bill and Melinda Gates Foundation. Despite divergent competing interests, a digital consensus prevails among these key players. The pre-eminent and overarching role

of this digital empire is often legitimised by slanted neoliberal discourses and narratives, fashioned to justify the urgency for external digital intervention and control, thus, technically, perpetuating global digital inequality.

Second are the compliant biometric states, which are subjugated by the global digital empire. There is a hallmark of intersection of interests forged between the digital empire and biometric states which, in effect, coalesce into consensual biometric coloniality. Owing to their resource constraints, biometric states are digital-dependent, concede to colonial domination and control, and enforce authoritarian digital mandates locally, on behalf of the digital empire, to the detriment of their own citizens. More importantly, through the provision of capital and digital investment, under difficult conditionalities, the global digital cohort disarticulates the digital sector in biometric states, thus transforming the states into powerful surveillance states. Third are the tech corporations (multinational and local) which act as intermediaries or middle-points for delivering the digital mandates of the digital empire and biometric states, while chasing their capitalist interests on the sidelines of the digital data economy. Usually, the big techs create oligopolistic markets and hijack biometric industries in developing countries. Hiring big techs results in enormous spending for biometric states, which must pay out huge amounts as matching grants to augment externally borrowed funds for digital projects.

Third are the biometric or digital subjects who supply raw personal data. Dalberto et al. (2021, 34) note that the biometric ID system serves as 'the instrument of a new digital capitalism, less concerned with the social inclusion of citizens and "vulnerable groups" than with differentiating them according to creditworthiness criteria'. These biometric subjects are targeted for exploitation and are oppressed in the materialism of digital data production by the first three complicit actors (digital empire, biometric state and tech corporations). This includes coercive digital enrolment, data privacy and security breach, biometric disempowerment, social/financial exclusion and data extraction without compensation. In Kenya, for example, the $72 million Huduma Namba project entrenched the exclusion of ethnic minority and historically marginalised groups including Nubians, Somalis, Swahilis, Boranas, Maasais, Indians and Arabs, who were denied access to government services (Musoni, Domingo, and Ogah 2023). Kenyan officials cross-checked or shared fingerprints of anyone who applied for a biometric ID with UNHCR data (Speed 2020).

In Uganda, Ndaga Muntu has affected access to health care and social security for over 33% of women, older persons and other marginalised groups (CHRGJ & ISER 2021). The government converted the biometric ID system as a powerful tool for monitoring public officials, media, human rights advocates and ordinary citizens. One police officer admitted that he had direct computer access to a database holding National Identity and Registration Authority (NIRA) data, which included images, fingerprints and biographical information. He conducted custom searches, unconnected to potential criminal activity, for friends and associates without court orders (Solon 2024). Findings from a 2022 report by Uganda's Auditor General, revealed that 41 of 67 private companies and state-run organisations that have 'irregular' and 'ad hoc' access to citizens' information in the NIRA databases abuse the use of personal data (Solon 2024, 1). To obtain the CNI in Côte d'Ivoire, citizens pay as much as 5,000FCFA (US$8.40), plus an estimated 10,000–13,000 FCFA ($17–$20) required to obtain the supporting documents (World Bank 2016). This created a strong mechanism of exclusion and selection, and reinforced government's discriminatory policies against marginalised and disadvantaged groups (Banégas and Cutolo 2024).

Biometric state and digital consensus: examining the digital identification landscape in Nigeria

Biometric states are digital-dependent countries that enjoy alliances with powerful external institutions and tech companies on the basis of a lucrative digital consensus and, consequently, carry out techno-capitalist interventions in the form of biometric ID programmes. Essentially, we use the term digital consensus to capture the intersection of interests and mutual agreement forged between the digital empire (such as powerful external institutions and tech companies) and compliant biometric states in the process of biometric ID intervention in the latter's country. There is digital consensus on the provision of finance, technical standards, technologies and digital infrastructures as 'all-in-one' subscription package to ID4D countries, including Nigeria. Incidentally, this digital consensus or collaboration turns into considerable advantage to the powerful external interests who carry out techno-capitalist digital interventions in biometric states. To depict this more lucidly, we describe the prevailing character of the biometric state in Nigeria, showing the problematic aspects of biometric ID programme interventions, as well as the deleterious effects of digital consensus and dependence. We foreground important aspects of external domination and control, as well as specific ways by which the digital subjects enforce their biometric agency. We anchor on the Nigerian case because its the most populous African country with the highest digital penetration.

Moving from documentary to biometric state

One critical aspect of digital consensus is the transition from documentary to biometric state, but such has been a rugged adventure. We shall dissect the arenas of both the documentary and biometric states, to see how they are intrinsically distinct, especially in defining the logic of the functioning of the state and the citizenship practices at play. The documentary state deals with register – writing of biographical information, birth and social status of individuals, demands consent and operates a localised/decentralised system (Breckenridge 2021). This classificatory logic of bureaucracies implies that register links individuals to proper legal identity and makes them 'legible', in order to enforce state control, administrative centralisation and the institutionalisation of nations (Scott 1998). In contrast, the biometric state deals with digital systems, imposed consent and extraction of body data, and operates a centralised and globalised system of biometric database (Breckenridge 2014; Dalberto et al. 2021). To eliminate social identity, biometrics uses digital fingerprints, iris and face recognition, or what Agamben (2011, 50) calls a 'biological datum', to generate/assign long digital numbers to body, thus, obliterating the bureaucratic mediation and social classification associated with the documentary state's registers. Dalberto et al. (2021, 38) contend that 'biometrics effectively silences a priori any social authority in the identification process, becoming an instrument of individualisation, desocialization, and therefore of the depoliticisation of identities, in so doing breaking radically with the logic of the documentary system'.

Biometric reforms are thus presented as recipes for compensating for the structural and historical weaknesses of the old civil registers of the documentary state. The World Bank has long pushed its agenda to replace weak civil registries with a new foundational system in Africa. But African states have resisted at different points, sometimes going so far as to depart from the Bank's ID4D 'traveller model', hybridising its 'universal' foundational system with

new biometric CRVS devices (Civil Registration and Vital Statistics). This practice implies that digital techniques generate a unique ID number that is then, at a second stage, linked up with an individual's biographical data (legal identity), combining, so to speak, the logic of the system with elements from social classification. Incidentally, the mutual integration or synchronisation of both the biographical and biological data presents a fresh layer of embedded contradiction. This problem bothers on the veracity of each individual's biographical data claims in association with their generated digital identity. In this reality, biometrics not only designates 'identity without the person' as claimed by Agamben (2011, 46, 50) but extends to the classificatory incorporation of the social 'persona' at the second stage, instead of serving a purely neutral function of biological datafication. In many cases, social classification of individuals, viewed as 'social nudity' by Dalberto et al. (2021, 39), entangles and weighs on individual liberties and rights (Ferguson 2015). It is undoubtedly in this connection that the new forms of civic, social and economic inclusion/exclusion are being played out today in biometric states in Africa. More precisely, the new biometric system reasserts and prolongs the discriminatory logics of the documentary state, thus interfering with individual liberties and rights.

Technical and financial dependence: Nigeria's ID4D

Nigeria's ID4D is a country-level component of the broad World Bank's ID4D initiative financed by key global institutions, governments and private interests. Nigeria's digital ID4D agenda is articulated along development discourses:

> The project objective is to increase the number of persons with a national ID number, issued by a robust and inclusive foundational ID system, that facilitates their access to services. The project aims to strengthen the foundational ID system, and in doing so, improve national data protection, bolster Nigeria's digital economy, and close gender and inclusion gaps in access to identification and related key services. (World Bank 2020a, 12–13)

The International Development Association (IDA) provided US$100 million, while the Agence Française de Développement (AFD) and European Investment Bank (EIB) contributed US$100 million and US$215 million, respectively, to cover the full US$430 million-cost of the Nigeria ID4D project. In addition, Phase II of the project is anticipated, for which the EIB will contribute US$60 million in co-financing in order to enable continuous digital enrolment, CR system digitisation and issuance of NINs at birth, including the provision of digital certificates, linked to the foundational ID system.

As shown in Figure 4, the four components of Nigeria's ID4D project reflect the key agenda of the global digital sponsors. There is digital consensus on the provision of finance, technical standards, technologies and digital infrastructures as an 'all-in-one' subscription package to ID4D countries, including Nigeria. Beyond financing, the World Bank and development partners argue that the organisation has developed 'substantial in-house technical expertise, analytics and operational guidance specific to the roll-out of robust, sustainable, and inclusive foundational ID systems' in Nigeria and have closely cooperated with key experts on 'technical standards, costs and technologies' (World Bank 2020a, 28).

More importantly, the World Bank and partners have tied the financing of Nigeria's digital ID project to some difficult conditionalities. These apply to the first disbursement of funds from each co-financing partner to NIMC. The IDA insists that (i) Nigeria should establish a

Component	Subcomponent	Funding Partners/ Contributions
1. Strengthening the legal and institutional framework	**Legislation, regulation, strategy, and policy develwopment supporting data protection and privacy** **Institutional and governance framework** • Finance the reform of the ID legal, regulatory, and institutional framework **Institutional capacity building and technical assistance** • Support drafting, enactment, amendment and enactment of regulatory/legislative frameworks for Nigeria digital economy, such as National Population Commission (NPC), National Information Technology Development Agency (NITDA) • Amendment of the NIMC Act 2007 • Amendment and enactment of legislation on electronic transactions and digital signatures • Amendment and enactment of legal legislation on cybercrime and cybersecurity • Finance technical assistance, insitutional assistance and capacity building for the establishment of the data protection authority	IDA $3M AFD $5M EIB $9M **Total:** $17M
2. Establishing a robust and inclusive foundational ID system	**Reinforcing the National Identity Management System (NIMS)** • Reinforce deduplication capacity at NIMC **Reinforcing the foundational ID ecosystem** • Harmonization of existing functional IDs • Deliver NINs at birth linked with a digitized civil registration **Development of the enrollment system** • Establishment of digital foundational ID platform that issues free of charge a national ID number (NIN) to all persons in Nigeria and Nigerians abroad **Reinforcing information security and privacy** **Registration of the population** **Training of ecosystem partners and their enrollment staff**	**Funding Partners/ Contributions** IDA $59M AFD $78M EIB $169M **Total:** $306M
3. Enabling access to services through IDs	**Developing authentication services at NIMC** **Developing authentication services within the ecosystem** **Facilitating service delivery using foundational ID**	**Funding Partners/ Contributions** IDA $12M AFD $17M EIB $37M **Total:** $66M
4. Project management and stakeholder engagement	**Project management and stakeholder engagement in the Ecosystem Coordination Strategic Unit (ECSU)** **Project management and stakeholder engagement in the Project Implementation Unit (PIU)**	**Funding Partners/ Contributions** IDA $41M AFD $0M EIB $0M **Total:** $41M
	TOTAL:	**$430 Million**

Figure 4. Phases of the Nigeria ID4D project and breakdown of partner contributions.
Source: World Bank (2020c) Nigeria Digital Identification Development Project. https://documents1.worldbank.org/curated/en/250181582340455479/text/Nigeria-Digital-Identification-for-Development-Project.txt.
Note: IDA – International Development Association; AFD – Agence Française de Développement; European Investment Bank.

Project Ecosystem Steering Committee whose 'leadership and composition are [approved] or acceptable to IDA'; (ii) the World Bank should assess or determine the enrolment system architecture including technical components; business model and per-enrolment payments; enrolment partner licencing, assurance and onboarding framework; data protection, security and authentication system. The EIB insists on (i) the enactment and effective operation of data protection law, and a new independent national authority for its enforcement,[1] (ii) the World Bank's written confirmation that EIB's procurement requirements are fulfilled and (iii) the use of a performance/auditing programme, including an operating model and systems approved by the EIB, for assessing the volumes of digital ID registrations by enrolment partners. The AFD tied its financing to the 'satisfactory progress on certain critical legal reforms'. Finally, among the strict conditions for the second batch of IDA funds' disbursement to NIMC partners is the 'mandatory use of the NIN for access to services[2]; and NIMC's mandate related to sharing of personal data with third parties to align with the project design and objective to promote universal coverage, inclusion, and nondiscrimination' (World Bank 2020a, 112–113).

The foregoing is emblematic of the complexities and character of digital consensus, struck between the global digital sponsors and compliant biometric states, which mainly reproduce an inescapable intricate web of biometric coloniality of power and control. This implies that such digital consensus is characteristically skewed to the advantage of the dominant external powers, which issues out assertive digital project implementation mandates and guidelines to digital-dependent states for utmost compliance, as conditionality for their funding and technological support. Incidentally, this system of digital consensus is deliberately schemed to effectively reward big tech companies from the Global North to benefit directly from the award of most lucrative biometric ID contracts.

State dysfunctionality: biometric ID system and contract scam

Going by Busza's (1997) claim, state dysfunctionality is essentially epitomised by decay or paralysis of the administrative, regulatory, legal, social and enforcement authorities that constitute its purpose. The point here is that the establishment of a regime of coloniality of biomeric power has negatively shaped the character of the biometric state and its ruling elites, resulting in state dysfunctionality. For instance, the state actors employ a ruthless and authoritarian approach in the enforcement of external mandates and directives on digital ID projects, resulting in oppression, exclusion and disempowerment of the people. However, beyond the original problems associated with the regime of coloniality of biomeric power, biometric state actors are also directly implicated in untold institutional corruption accounting for the poor development of their digital ID sector. In reality, the implementation of digital ID programmes provides leeway for state actors to engage in fraudulent activities and contract scams for personal enrichment. This situation describes recent developments in the Nigerian identity management system.

Remarkably, Nigeria's national ID system began in 1978 with the creation of the Department of National Civil Registration by Nigeria's Federal Ministry of Interior. Since 1981, Nigeria has signed costly but questionable contracts with foreign and local private companies to produce national ID cards, including Avant Incorporated, Chams Plc, Sagem and Mastercard. However, the national ID system contracts in Nigeria had been marred by vendor lock-ins, contract scam, 'executive high-handedness, mind-boggling corruption, sheer

irresponsibility of government officials and asinine abuse of power' (Ibekwe 2015, 1). Between 1981 and 2015, over N121 billion (US$99 million) was spent on the national ID projects with little impact. In 1981, a contract of $100 million was awarded to Avant Incorporated and the company, Afro-Continental, of one Arab-Jew, Nessim Goan. In 2001, a new $214 million contract with Sagem Ltd (A French Tech Company partly owned by the French government) to produce 70 million ID cards became a big fiasco. With five years spent on collection of national data, Sagem only delivered 35 million ID cards. Meanwhile, three Nigerian ministers, including the Minister of Interior who was in charge of the digital identity project, were implicated in a bribery scandal of payments of €22,000 and €36,000 which they received from Sagem between 2000 and 2003 to influence the award of the contract in Sagem's favour. A Paris court fined Sagem €500,000 for using fraudulent means to secure the $214 million contract (BBC 2012).

Importantly, the NIMC Act (2007) established the NIMC, with a mandate to: (a) create, own, operate, maintain and manage the National Identity Database; (b) register and assign a Unique NIN; (c) issue General Multi-Purpose Cards to Nigerian citizens and all legal residents in Nigeria; (d) harmonise/integrate all databases in Nigeria; and (e) provide the required identity verification and authentication service infrastructure. However, NIMC does not issue the e-ID cards as mandated in the NIMC Act (2007), implying that many Nigerians do not have a valid e-ID card, only the 11-digit NIN slip. Instructively, NIMC received a whopping N80.2 billion funding from the federal government in the seven years between 2010 and 2017 including a N30 billion takeoff fund in 2010, N17.9 billion in 2011, N12.35 billion in 2012, N7.19 billion in 2014, N6.276 billion in 2015 and N6.535 billion in 2017 (Udofia 2017). However, the Commission itself had been implicated in some fraudulent contract awards revealing the Commission's high level of executive recklessness, lack of accountability and transparency, official corruption, outright ineptitude and gross mismanagement of public funds (Adebanwi 2012). Unfortunately, attempts at probing institutional corruption have constituted the most common methods for justifying abnormal institutional changes and compromise at NIMC. This further reproduces systemic crisis with a thieving ruling class (Adebanwi 2012). For example, in 2015 alone, NIMC management was probed for spending N30.5 billion on questionable contracts and procurement (Udofia 2017). The alarming rate of contract scam in NIMC culminated in August 2022 with the federal government accusing the Commission's management and governing board members of fighting themselves every day over fraudulent contract awards (Pantami 2022). Figure 5 presents the cases of contract scam and institutional corruption in which NIMC was implicated.

This problem goes beyond Nigeria. In some other countries, the challenge is not because of the coloniality of power entanglement per se, but rather a postcolonial character of ruling elites who utilise the biometric ID system to facilitate vested political agenda. For example, Uganda's biometric ID contract, even though managed by the German's Mühlbauer company, involved an $80 million deal that bypassed government procurement rules (Solon 2024). The foregoing clearly informs the level of institutional dysfunctionality in biomeric states. As Herdt and Oliver de Sardan (2015) observe, even when the global development institutions set projects' rules and procedures as a precondition for their technical and financial support, stakeholders on the ground breach the rules for their selfish interest. This illustrates how the African governance system is burdened with a multitude of conflicting and overlapping laws and regulations that inevitably lead to institutional collapse. In reality, the lens of practical norms diverges extensively from public rules. This contradiction constitutes

Date	Contract/Procurement Details	Contract Amount ($)	Fraudulent Actions/Infractions	Culprit	Investigation Report/ Contract Reference
2012	Installation and maintenance of 19 No. Garret PD65001 walk-through metal detector (N2.5 million per detector)	$ 39,318.48	i. Fraudulent documentation. ii. Low quality materials supplied. iii. Contract inflation by N30.4 million.	NIMC/ Contractor	via a letter referenced NIMC/LS/VGSNL/12/12
2018	Supply of 600 units of HP Flatbed scanners	$9,720.37	i. Fraudulent documentation. ii. Contract payment violated Public Procurement Act 2007.	NIMC/ Contractor	via letter referenced NIMC/ LS/MLS/1/13/3
2013	Engagement of consultant to conduct market study on the smart card industry in Nigeria	$18,155.39	i. Contract document falsification. ii. Contract payment violated Public Procurement Act 2007.	NIMC/ Contractor	via a letter referenced NIMC/LS/A&CO/1/13/1
2014	A vendor engaged to provide tripwire via security information and event monitoring tools (SIEM) and SCM License fees, implementation training, first year support and maintenance	$ 18,878.40	i. Contract payment violated Public Procurement Act 2007.	NIMC	
2014	Deployment of VSAT to local government areas by 1st August 2014	$ 13,255.04	i. Contract payment violated Public Procurement Act, 2007.	NIMC	Auditor General of the Federation (AGF)
2014	A consultant engaged to provide 8 modules licenses for the NIMC Enterprise Monitoring System	$ 13,576.38	i. Fraudulent documentation. ii. Contract payment violated Public Procurement Act, 2007.	DG/CEO NIMC	via a letter referenced NIMC/LS/SWSE/1/14. The total contract sum was paid to the consultant vide PV. No. NIMC/236/CA/14.
2014	Engaged and paid a media vendor as an agent to provide it with newspaper/magazine campaign	$ 17,593.06	i. Fraudulent documentation. ii. Contract award/payment violated Public Procurement Act, 2007. iii. Contract not executed.	DG/CEO NIMC	via a mere memo written by an aide to the DG/CEO

Date	Contract/Procurement Details	Contract Amount (N)	Fraudulent Actions/Infractions	Culprit	Investigation Report/ Contract Reference
2014	Procurement of Affina Enterprise Smartcard Life Cycle Management System (a software)	$1.4 million (at the exchange rate of N170/ Dollar	i. Fraudulent documentation. ii. No evidence of contract execution.	NIMC	
2015	Five contractors engaged for awareness campaign on the need for national identification enrolment across the six geo political zone	$ 72,460.91	i. Fraudulent documentation. ii. No evidence of contract execution	NIMC	
2017	22 units of HP blade servers for Morpho BSS upgrade	$ 184,526.28	i. Contract award/payment violated Public Procurement Act 2007, and Financial Regulation 2907 (1). ii. Multiple contract awards for the same project.	NIMC	Senate Public Accounts Committee

Figure 5. Cases of contract scam and institutional corruption involving NIMC.
Source: Authors.

the space within which different actors navigate to make and unmake the state (Herdt and Oliver de Sardan 2015).

Biometric data extraction/mining by digital data processors

It is worthy of note that the regime of coloniality of biomeric power maps out new orders of power at multiple levels/scales. One such significant power player is the big tech group which plays a key role in the digital ID ecosystem. The big tech companies engage in data mining in biometric states and act as digital data processors. The Nigeria Data Protection Regulation (2023) specifically establishes the privacy rights of data subjects, data security and obligations on data controllers and processors.[3] However, despite the enactment of the Nigeria Data Protection Act, 2023, personal data security risks remain extremely high amidst the expanding digital ID ecosystem – increasingly defined by multiplicities of data controllers, advanced technology and explosive volumes of biometric data by big techs. More

importantly, the Act accords big tech data miners/processors full cross-border data processing rights to the detriment and exploitation of data subjects.

Looking at Figure 6, one important point to keep in mind is the contradiction and, of course, the illusion of data 'sovereignty', 'ownership', 'residency' and 'localisation' as proclaimed in the Nigeria National Data Strategy (2022). Data subjects are thus, by default, exposed to the highest risks of data exploitation by data controllers and processors who consider data as a power and resource, and extract data for political and economic interests. This presents a replication of colonial practices of extractivism as evident in the contemporary domination of Africa's digital sector by external powers, even though they appear subtle, invisible and apparently benign. Pereira and Tsikata (2021) reveal how the different stages of extractivism are implicated in the fortification of a regime of coloniality of power, which manifest at the social, economic and political dimensions. Coleman (2019, 147) captures the essence of digital colonialism in Africa, more aptly, as 'a modern-day 'Scramble for Africa'

Sections	
Part VIII. Section 41-43 Cross-border transfers of personal data by data controllers /processors	
Legal Provisions	
41(1) Cross-border personal data recipient of personal data must be subject to a law, contractual rules, certification mechanisms, and operates data protection law.	**42(6)** NDPC may rely on decision by other countries to approve cross-border transfers of personal data.
41(2) Data controller to record the basis for personal data transfer to another country.	**43(1)** Data controllers/processors can transfer personal data from Nigeria to another country in the absence of adequacy of data protection if; (a) data subjects give consent, (b) data transfer is necessary for performance of contract to which the data subject is involved, (c) data transfer is to the sole benefit of data subject; in this case, consent is not compulsory. (d) data transfer is necessary for public interests. (e) data transfer necessary for legal claims, and defense.
41(3) NDPC may request data controllers /processors to notify it on measures for data protection in recipient country.	**43(2)** No specific international, multi-national cross-border data transfer codes, rules, certification mechanisms, shall be adopted as Nigeria standard for protection of data subject without approval from National Assembly.
41(4) NDPC may designate some personal data to be of high risks, and restrict them from being transferred to another country.	
42(1) Adequacy of data protection for all cross-border data transfers.	
42(4) NDPC determines whether a country, territory, region, or specific sector within a country, fulfills adequate level of data protection in case of transfers.	
Gaps and Implications	
i. Nigeria becomes a major personal data export country.	**vi.** Unspecified costs for the use of personal data overseas.
ii. External (oversea) transfer of personal data with without data subject's consent.	**vii.** Data subjects are vulnerable to risks of fraud, surveillance and privacy rights breaches abroad.
iii. External (overseas) transfer of personal data in the absence of data protection regime in the data import country.	**viii.** Exclusion of data subjects from acruable financial benefits in data transfer contract between data processors/controllers and overseas recipients.
iv. Data subject objectification and abstraction – with no discretionary powers to define their "sole benefit" in data transfers.	**ix.** Sec. 42(1), 42(6) and 43(2) depict high degree of external dependence, subjugation, and externalization of data protection obligations in the case of oversea data transfers.
v. Unspecified purpose/use of personal data oversees.	

Figure 6. Critique of Part VIII of NDPA in connection with cross-border personal data transfers.
Source: Adapted from Nigeria Data Protection Regulation 2023. Federal Republic of Nigeria Official Gazzete. Lagos, 1 July 2023, Vol. 110 (119). Note: NDPC means Nigeria Data Protection Commission. CC BY 4.0.

where large-scale tech companies extract, analyse and own user data for profit and market influence with nominal benefit to the data source'. Dalberto et al. (2021, 31) confirm that 'Since the early 2000s, the "new scramble for Africa" has been digital'. Hence, powerful technology companies who exploit the weakness of data protection legislation use their resources to access yet unexploited data of citizens of new biometric states. This presents a new form of data colonialism, in which data serve as a means of capitalist accumulation by dispossession (Thatcher, David, and Dillon 2016). This accounts for the deepening of inequalities within and among nations, and the growing power of transnational corporations. At this nexus lies a regime of global capitalism that condoles the erosion of sovereignty and decision-making power in national contexts. More importantly, data extraction has had clear consequences: the creation of biometric state, loss of social integration, economic exclusion, the increasing use of violence to repress resistance and the creation of new orders of power and social formations.

Citizenship exclusion and disempowerment

The engagement with the global digital sponsors, including international formations like the World Bank's ID4D and the big tech corporations, and its manifestation in biometric states enable us to see how biometric states and these forms of power are emerging along lines that reproduce the coloniality of power. This informs the evolving character of the new biometric state and its ruling elites, in which a ruthless and authoritarian approach is employed in the enforcement of externally mandated biometric reforms. In Nigeria, as elsewhere, consolidating the foundational ID system requires that the data of individuals captured in civil registers and issued with IDs be upgraded to a biometric system in which their personal data are authenticated (Iwuoha 2025a, 2025b). This also involves encouraging multiple public and private service providers to use the biometric system to authenticate people for services. This consolidation is combined with the World Bank's target for NIMC of 148 million ID enrolment by June 2024 at the behest of the Nigeria ID4D programme (World Bank 2020b). As a result, on the one hand the government is pushing key public and private service providers to prioritise linking their several databases to the foundational ID system, and to use NIN to authenticate individuals for transactions, and on the other hand the government is compelling individuals to obtain NIN or be prevented from accessing public services.[4] Section 27 (1&2) of the NIMC Act (2007) enforces the mandatory use of NIN for all public services and financial transactions, and slams serious penalties, including imprisonment, on all defaulters.

In Nigeria, the drive for NIN linkage across existing multiple digital databases has been vehement, sporadic and drastic since 2020, taking the form of biometric policing. However, this forced 'digital inclusion' always met resistance with push-backs from the people who face the nagging challenges of exclusion and state-sponsored discrimination in their everyday lives.[5] For example, in the telecoms sector, after a total of eight mandatory deadlines for 300 million mobile network subscribers to link their SIM to NIN (including the initial 31 December 2020 and, subsequently, 31 March 2022 deadlines), only 125 million SIM cards were successfully linked to NINs (Biometric Update 2022). The federal government began full implementation of the NIN-SIM Linkage Policy on 4 April 2022, which compelled mobile network providers to block all mobile phone users in Nigeria without NINs – and about 72

million SIMs were blocked from making calls. Despite these radical moves, over 12.3 million Nigerian mobile subscribers refused to link with NIN (Business Day 2023).

In the banking sector, the Central Bank of Nigeria (CBN) mandated Nigerian banks to validate all customer BVNs and NINs electronically by 31 January 2024, and subsequently imposed an order of 'Post No Debit or Credit' or froze all customer accounts and wallets without verified BVN linked to NIN, effective from 1 April 2024.[6] This implied that there would be no further transactions permitted on all funded accounts without NIN–BVN linkage (Innovation Village 2023). For the social security scheme, the government imposed severe restrictions on vulnerable persons without BVN and NIN, preventing them from gaining access to social security funds thus institutionalising disproportionate economic disempowerment of the poor and of women.[7] In 2023, only 1.5 million out of a targeted 15 million vulnerable Nigerian households received the government's N25,000 conditional cash transfers sourced from a World Bank loan of $400 million. In this social security scheme, only 0.1% of Nigerians received N25,000. The federal government stated that the funds' disbursement had been impeded by the low number of poor and vulnerable people with NINs, and so those without were not listed in the National Social Register (Ariemu 2023). Again, the federal government issued another draconian order on 26 February 2024 as it approved digital-only identity-linked cash transfers to vulnerable people for the 2024 social security scheme. The Minister of Finance noted:

> So, the direct payments to 12 million households comprising 60 million Nigerians is to resume immediately with the important proviso that every beneficiary will be identified by their NIN and BVN. Therefore, payments will be made into bank accounts or mobile money wallets. So, that whether it is before or after, there is verification of the identity of beneficiaries. Each person that receives 25,000 Naira for a total of three months will be identifiable, even after they have received the money. (Edun 2024, 1)

Unfortunately, this economic disempowerment policy came without any recourse for the vulnerable groups, without any form of identity documents, which constitute a significant proportion, about 20.1%, of the over-38 million people out of Nigeria's approximately 224 million population (Nnorom 2023) who are still unbanked and without BVN and NIN. Of course, lack of access to owning a bank account or obtaining BVN or NIN is primarily a result of poverty, as well as complex forms of socio-economic, documentation, educational, geographic, environmental and psychological barriers.[8] These marginalising conditions have been reinforced by the newly imposed policy of the digital-identity-linked social security system, thus strongly indicating state complicity in citizenship exclusion, as non-ID holders, especially the most vulnerable populations, are completely shut out from gaining access to the government's social security services. These subtle forms of 'biometric threat' and forceful population biometricisation, or, simply, 'digital authoritarianism', deeply reflect, reincarnate, replicate or reinforce the historical trajectories of colonial forms of residents' subjugation in which coercive or brutal force was used to enforce rules and orders to maintain firm control of the local natives. Therefore, this regime of mandatory biometric ID enrolment, such as the use of coercive legislative and policy proclamations to enlist and populate a biometric register, and consequently produce a resource of biometric subjects primarily for the interests of external and state authorities, shows clear manifestations of the biometric state's authoritarian and repressive character.

As expected, the NIMC database, having only 39 million enrolments in 11 years, i.e. 2010–2020, surged to over 100 million enrolments in just three years between 2020 and 2023 (Pantami 2023). Figure 7 shows NIMC's NIN enrolment data, 2012–2023. As at December 2023, NIN enrolments hit 104.16 million (59.12 million male and 45.04 million female), representing a 10.77% increase from the 94.03 million recorded in December 2022. In the diaspora, only 530,345 Nigerians have obtained NINs across over 152 enrolment centres in 38 countries (Innovation Village 2024). Also, NIMC enrolment centres nationwide increased from 1,060 in February 2021 to 5,500 in July 2023 (Egole 2023). While these figures highlight some progress, they are still minimal considering Nigeria's staggering 226 million population, thus underscoring the difficulty in enforcing mandatory ID enrolment.

More importantly, there is a rapid financialisation of Nigeria's biometric digital ID ecosystem. Currently, Nigeria's digital ID enrolment ecosystem framework (run *via* the use of Front-End Partners [FEPs]) operates purely on a neoliberal business model, a form of biometric stewardship, which relinquishes the state's regulation of the digital ID market economy to external control. Essentially, the ID enrolment partners or FEPs had been classified into three groups of stewards – A, B and C, which receive funds disbursements under the per-enrolment fees component of the ID4D, for covering operational enrolment costs, so that enrolment can be free for all persons. Group A comprises government agencies eligible to obtain and lease registration gadgets at subsidised amounts, while Group B comprises private-sector actors who directly purchase their enrolment gadgets, or lease them at market costs, and recoup expenses by per-enrolment fees. Both Groups A and B operate under national licence through a competitive bidding and pricing regime, and receive per-enrolment fees initially set at US$0.71 and US$0.90, respectively. Group C involves private-sector companies under contract arrangement with NIMC to handle enrolment in hard-to-reach geographical zones. And as Group C is fully dedicated, unlike A and B, which also engage in their normal businesses alongside registration, they are expected to achieve larger volumes of NIN enrolments. Above all, Groups A and B have a flow-on advantage in the sense that their enrolment facilities can be simultaneously (or after mass ID enrolment) used for other

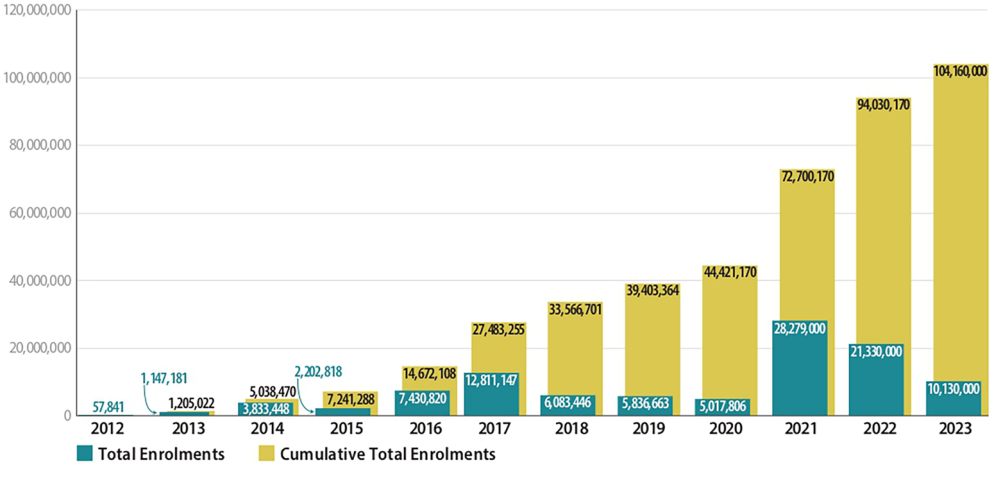

Figure 7. NIMC's enrolment data including total and cumulative enrolments by year.
Source: Authors.

services such as identity authentication. Finally, a last but somewhat undocumented group exists – roadside vendors. These are roadside agents engaged by licensed individual private companies operating under Group B, owing to the rising need to widen the enrolment net to reach national coverage and capture a larger population into the database. These vendors pay huge amounts of money, ranging to above N1 million, to their principal,[9] who in return sublets, leases or provides them with the required registration equipment and also pays them a per-enrolment fee.[10] In total, approximately 30 state governments/public sector institutions and 173 agents/stewards have been approved and licensed by NIMC to conduct national ID enrolment in Nigeria, while 31 private companies are licensed for diaspora enrolment (NIMC 2024).

However, the per-enrolment fee structure appears problematic and poorly funded, as enrolment partners/agents/stewards complain of non-payment of per-enrolment fees. For example, the FEPs are owed per-enrolment fees for 22 months by NIMC after registering 60 million people (Naija News 2023).

NIMC officials[11] too complain of inadequate funding for covering operational expenses, including costs for generator fuelling, estates, printing materials, buying of internet data, etc., for each registration at an estimated time of 10–15 min depending on the speed of the internet network. The assumption that offline enrolment is insecure and incurs more expenses and delay/timeled to the introduction of new software, RESWEB, which attempted to cut registration fields and time by half, but this was impeded by poor internet connectivity. As revealed in an interview:

> RESWEB does only online registration. We use two layer security login – password and fingerprint before you have access to enrollment page. This is Nigeria where almost nothing works 100% let alone internet connection, I can tell you for sure I have gone to enroll people in a farm, call it forest but no way. Here even in town you struggle for connection whether 4G, 5G or 6G, all of them don't work well. So the point is, without strong connection you can't connect and can't do anything.[12]

This is corroborated further:

> When server is down in Abuja, nobody can work anywhere in Nigeria. We also encounter problems of camera – sometimes it cannot snap. RESWEB controls the camera, GPS, signature pad, fingerprint scanner, everything; so if RESWEB has any issue, you cannot login or register anyone. These impede online enrollment. We use FortiClient VPN which some internet networks like Airtel cannot connect. Owing to processing delays, the intention to make enrollment faster is defeated.[13]

Besides, no per-enrolment fees are provided for all 'unsuccessful' or uncompleted enrolments, whereby an agent completed the enrolment process, but no NIN was generated, mostly owing to network problems. This problematic ID enrolment structure has thrown open a wide door for applicants' exploitation, extortion and institutional corruption, leading to inefficient ID services. For example, one NIMC's desk officer claims;

> For 13 years now, the government hasn't been able to procure new computers and the ones available are crashing or packed up, sometimes they catch fire, and once each system spoils, the encoded license goes with it, and the licenses are bought in dollars. There is poor maintenance culture.[14]

The same story goes for Abuja registration centre:

> The issuance of plastic ID cards is provided in the law, and supposed to be issued to the applicants, but they said there is no money to produce. The A4 paper we use, we workers buy them, they don't supply, we use to have a customized NIN slip, but now we no longer have it, we just print NINs on ordinary black and white paper. We have colored printer, but now the government cannot afford to buy the original four-colored cartridge refills.[15]

Over the years, NIMC staff have been poorly remunerated and not adequately motivated, except in 2023 when a new Minister increased their monthly salary by 200%. Even though ID enrolment is free as provided by law, it is never entirely free in practice:

> The truth is that NIN is free but they don't provide money for us to do it free; we disturb them [government] so much before they can do anything. In fact, what they do is that sometimes when NEPA [energy supply] goes off, applicants who are on the queue contribute money, from 2k, 3k or 4k, to fuel generator instead of waiting for NEPA to come back. Some workers silently ask applicants for money; and by the time you begin to collect it becomes difficult to stop.[16]

Candidates for various types of NIN modifications such as change of name, date of birth, etc. even face multiple forms of exploitation and extortion. Modifications require formal modification fees through bank payment, court affidavit and newspaper publication at the cost of N600, N3,000 and N8,000, respectively. And, since the modification services are generally conducted in Abuja headquarters, FEP's roadside vendors and agents charge applicants higher fees to process modifications at Abuja, ranging between N15,000 and N20,000.[17] Meanwhile, the roadside vendors carried on whatever sharp practices they wished, and whatever money they made was their own. Even though their contractors pay them per-enrolment fees such as N300–500, they still collected about N1,500 or N2,000 directly from applicants. During rush periods or registration deadlines, vendors, sometimes in collaboration with NIMC officials, collected higher prices from applicants depending on the location, ranging from N5000 to N10,000.[18] In fact, the mandatory use of NIN boosted this new ID business, now tainted with elements of extortion and corrupt practices.

For diaspora enrolment, different fee regimes are charged for specific ID services (see Figure 8). This clearly shows the true techno-capitalist undertones of the digital ID project. The implication of the ID enrolment business model is that its over-focus on revenue generation acts as a barrier to people's access to public services, and consequently results in citizens' exclusion. The worst experience occurs in the education sector.[19] Lack of access to enrolment, poor internet connectivity, problematic ID authentication and unsuccessful uploads of NINs to the NIMC central server are major barriers that prevent many Nigerian students seeking higher education from undertaking the required examinations.[20]

These examples show how biometric states have become stooges and willing tools in the hands of neocolonial masters and their oligopolies in enforcement of acts of biometric criminalisation against innocent migrants, of citizenship exclusion and surveillance, and of oppression, as well as of orchestrated economic disempowerment of vulnerable groups who lack any understanding of the European concept of 'proper' identity, or digital identification. Worst of all is the replication of colonial injustice and utter economic oppression using the pretext and assumption of algorithmic neutrality of biometric technology (Breckenridge 2021). Instead, this technology turns out to be an embedded subjective instrument for dictating who has the rights to access economic benefits and who does not, what a person is entitled to and what they are not entitled to, and what resources an individual is permitted to access (Dona 2022).

ID Service	Services at Licensed Partner Offices (in US $)		Services Outside Licensed Partner Offices (in US$)
	Outside Africa	Within Africa	(Mobile Services) -All Countries-
1. Enrolment & NIN Issuance: Persons 16 years and above	50.00	30.00	70.00
2. Enrolment & NIN Issuance: Persons below 16 years	40.00	20.00	50.00
3. NIN Slip re-issue	5.00	3.00	10.00
4. NIN Validation	10.00	5.00	15.00
5. NIN & Demographic Data Validation	15.00	10.00	20.00
6. Biometric Verification	25.00	15.00	30.00
7. Modification of all fields other than Date of Birth	10.00	5.00	15.00
8. Modification of Date of Birth (Day, Month, Year or all)	35.00	35.00	45.00
9. GMPCard Issuance/re-issuance & Activation	35.00	35.00	60.00
10. GMPCard Number Authentication	20.00	10.00	30.00
11. Re-issuance of PIN for issued GMPC on paper	5.00	5.00	5.00
12. Request for written Certification/Confirmation of Identity (inclusive of delivery by registered courier)	75.00	75.00	75.00

Figure 8. Various categories of diaspora ID enrolment services and fee structure in different parts of the world.
Source: NIMC (2023) Diaspora Services Facts Sheet. NIMC, 18 April 2023. https://nimc.gov.ng/docs/diasporaEnrolmentFactS_april2023.pdf CC BY 4.0.

Conclusion

We have shown that Nigeria is one of many sites of biometric coloniality in the Global South where alliances of powerful external institutions, tech companies and the compliant emerging biometric state operate on the basis of a lucrative digital consensus to carry out techno-capitalist interventions, reproducing colonial relations of domination. The emergence of the biometric state is linked to specific interconnected data spaces. These transnational spaces of data exploitation are open to the unauthorised use and sharing of data for purposes of personalised advertising, fraud, exclusion and surveillance, to the point of targeted persecution and other concrete materialisations of biometric spaces for Nigerian citizens in very concrete places. The unequal patterns of power through control of data on faces, bodies, preferences and financial means are developing across and between local, national and global spaces (Gillespie 2022; Iwuoha and Doevenspeck 2025). However, the digital subject is far from being just a victim. Future work should explore these fragmented digital and physical spaces of resistance and the (digital) practices employed to (re)produce them as subaltern answers to biometric coloniality.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Ethics statement

The author declares that the author received ethics approval from the Faculty of Social Science, University of Nigeria and conformed with all approved research ethics and standards including receiving informed consent of the research participants.

Funding

This work was supported by Deutsche Forschungsgemeinschaft [grant number EXC 2052/1 –3907 13894].

Acknowledgements

We sincerely thank Elbie Bentley Kivilcim, a seasoned cartographer at the Department of Geography of the University of Bayreuth, Germany, for her immense contribution in designing the figures and maps used in this article.

Notes on contributors

Dr Victor Chidubem Iwuoha holds a PhD in International Relations from the Department of Political Science, University of Nigeria, Nsukka, where he also serves as senior lecturer. His research interest is on international migration and security.

Prof. Dr. Martin Doevenspeck teaches at the Department of Geography, University of Bayreuth, Germany. He has served as Principal Investigator in the Cluster of Excellence Africa Multiple, spokesperson of the Research Section Mobilities and member of the Executive Committee in the Cluster of Excellence. His research interest focuses on political geography.

Notes

1. Nigeria Data Protection Regulation 2019 and Nigeria Data Protection Bureau were replaced with Nigeria Data Protection Act 2023 and the Nigeria Data Protection Commission in 2023, respectively, to fulfil EIB digital-aid conditions.
2. Interview with 3 NIMC officials at Abuja headquarters, 23 September 2022.
3. See NDPR Articles 2(6–10), and 3(1).
4. Interview with NIMC official at Benin, 2 November 2023.
5. Interview with six lecturers, University of Nigeria, 10–24 November 2023.
6. Personal observation and confirmed by all interviewees.
7. FGDs with NIN applicants, including 21 participants without NINs across study areas, September 2022 and February 2024.
8. Interview with three bank commercial officials at Nsukka and Enugu, 18 and 26 April 2023, respectively; FGDs with NIN applicants across the study areas.
9. Interview with three enrollment agents at Abuja, 28 March 2023.
10. Interview with 12 enrollment agents at Lagos, Enugu, Nsukka, and Benin, 20 March 2023 to 26 April 2023. The agents say the enrolment tool kit includes an i-5 core desktop, printer, fingerprint scanner, camera and signature device.
11. Interview with 1 NIMC official at Benin, 2 November 2023.
12. Interview with one NIMC official in Abuja, 28 March 2023.
13. Ibid.
14. Interview with 1 NIMC official at Abuja office, 23 March 2023.
15. Interview with 1 NIMC official at Enugu, 8 November 2023.
16. Ibid.
17. Interview with three enrollment agents at Lagos, October 16 2023.
18. Interview with 2 NIMC officials at Benin, 2 November 2023.
19. Interview with five lecturers, Federal University Otuoke, 3–5 November 2023.
20. Interview with four lecturers, University of Nigeria, 10–24 November 2023.

Data availability statement

The data associated with this research will be provided by the authors upon request.

References

Acuity Market Intelligence. 2022. "The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy." https://www.acuitymi.com/product-page/the-global-biometrics-and-mobility-report.

Adebanwi, W. 2012. *Authority Stealing: Anti-Corruption War and Democratic Politics in Post-Military Nigeria*. Durham: Carolina Academic Press.

Agamben, G. 2011. *Nudities*. Translated by D. Kishik and S. Pedatella. Stanford: Stanford University Press.

Aït-Hatrit, S. 2020. "Biometric Identification: A Coveted African Market." The Africa Report, 22 June. Accessed November 18, 2022. https://www.theafricareport.com/30838/biometric-identification-a-coveted-african-market/.

Aljazeera News. 2022. "In Cameroon, Refugees Get a New Lease of Life with Digital IDs." 29 August. Accessed November 20, 2022. https://www.aljazeera.com/news/2022/8/29/in-cameroon-refugees-get-a-new-lease-of-life-with-digital-ids.

Angoua, A. 2022. "Expiry of 2009 National Identity Cards: ONECI Invites People Who Have Not Renewed Their Cards to Register Now." L'infodrome, 24 February 2022. https://www.linfodrome.com/politique/74250-expiration-des-cni-de-2009-l-oneci-invite-les-personnes-n-ayant-pas-renouvele-leur-carte-a-se-faire-enroler-des-maintenant.

Ariemu, O. 2023. "Only 1.5m of 15m Households Received FG's N25,000 Cash Transfer – World Bank." Daily Post, 18 December 2023. https://dailypost.ng/2023/12/18/only-1-5m-of-15m-households-received-fgs-n25000-cash-transfer-world-bank/.

AU (African Union). 2014. "African Union Convention on Cyber Security and Personal Data Protection." https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Banégas, R., and A. Cutolo. 2024. "Biometrics, Citizenship, and the Documentary State." In *ID Wars in Côte D'Ivoire: A Political Ethnography of Identification and Citizenship*, edited by R. Banégas and A. Cutolo. Oxford: Oxford University Press.

BBC. 2012. "Safran Fined in Nigerian Bribery Case." BBC, 6 September 2012. https://www.bbc.com/news/business-19498916.

Biometric Update. 2022. "Nigeria Requires Partial Block on SIMs Not Linked to Digital ID." Biometric Update, 4 April. https://www.biometricupdate.com/202204/nigeria-requires-partial-block-on-sims-not-linked-to-digital-id.

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

Breckenridge, K. 2021. "Documentary Government and Mathematical Identification: On the Theoretical Significance of African Biometric Government." In *Identification and Citizenship in Africa: Biometrics, the Documentary State and Bureaucratic Writings of the Self*, edited by S. A. Dalberto and R. Banégas, 49–64. New York: Routledge.

Browne, S. 2012. "Everybody's Got a Little Light under the Sun: Black Luminosity and the Visual Culture of Surveillance." *Cultural Studies* 26 (4): 542–564. https://doi.org/10.1080/09502386.2011.644573.

Business Day. 2023. "NIN: 12m Mobile Subscribers May Be Blocked." Business Day, 19 December 2023. https://businessday.ng/news/article/nin-12m-mobile-subscribers-may-be-blocked/.

Busza, E. 1997. "The Dysfunctional State and International Collaboration: New Challenges to National Security Regimes." CSIS, September 1997. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/ruseur_wp_003.pdf.

CHRGJ & ISER. 2021. "Chased Away and Left to Die. CHRGJ & ISER." Accessed 8 June 2021. https://drive.google.com/file/d/1EOgwFPMK_8TY_qUhWAASMk_b4f3HgRM3/view.

Cole, S. A. 2001. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. London: Harvard University Press.

Coleman, D. 2019. "Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws." *Michigan Journal of Race & Law* 24 (24.2): 417. https://doi.org/10.36643/mjrl.24.2.digital.

Couldry, N., and U. Mejias. 2019. "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject." *Television & New Media* 20 (4): 336–349. https://doi.org/10.1177/1527476418796632.

Dalberto, S. A., R. Banégas, A. Cutolo, and R. Robertson. 2021. "African Citizenships–A Biometric Turn?." In *Identification and Citizenship in Africa: Biometrics, the Documentary State and Bureaucratic Writings of the Self*, edited by S. A. Dalberto and R. Banégas, 29–48. London: Routledge.

De Genova, N. 2016. "The European Question: Migration, Race, and Postcoloniality in Europe." *Social Text* 34 (3 128): 75–102. https://doi.org/10.1215/01642472-3607588.

Dona, G. 2022. "Migration Management, Borders and Digital Technologies: The Coloniality of Power in Techno-Borderscapes." A Keynote Presented at the Conference Digitized Migrants, by IWM/CRG Europe-Asia Research Platform on Forced Migration, in September 2022 in Turkey.

Edun, W. 2024. "FG to Pay Youth Unemployment Benefits, Sets Up Consumer Credit Programme." 27 February 2024. https://punchng.com/fg-to-pay-youth-unemployment-benefits-sets-up-consumer-credit-programme/.

Egole, A. 2023. "5,500 Enrollment Centers Active Nationwide – NIMC." Punch, 27 July 2023. https://punchng.com/5500-enrollment-centers-active-nationwide-nimc/.

Ferguson, J. 2015. *Give a Man a Fish. Reflections on the New Politics of Distribution*. North Carolina.

Gelb, A., and A. Diofasi. 2016. "Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment?." Working Paper 435, Center for Global Development, World Bank, Washington, DC.

Gillespie, K. 2022. "Facing Geography: A New Research Agenda." *Progress in Human Geography* 46 (1): 198–214. https://doi.org/10.1177/03091325211050061.

Herdt, T. D., and J.-P. Oliver de Sardan. 2015. *Real Governance and Practical Norms in Sub-Saharan Africa: The Game of the Rule*, 1–278. London: Routledge.

Ibekwe, N. 2015. "Over N121 Billion Wasted, Nigeria's Troubled National ID Card Project in Fresh Controversy." Premium Times, 27 May. https://www.premiumtimesng.com/news/headlines/183720-over-n121-billion-wasted-nigerias-troubled-national-id-card-project-in-fresh-controversy.html?tztc=1.

Indemia. 2017. "Nigeria Retains Safran Identity & Security to Provide an Upgraded Automatic Biometric Identification System and Maintenance Support." Indemia, 4 April 2017. https://www.idemia.com/press-release/nigeria-retains-safran-identity-security-provide-upgraded-automatic-biometric-identification-system-and-maintenance-support-2017-04-04.

INEC. 2024. "Report of the 2023 General Elections." https://inecnigeria.org/wp-content/uploads/2024/02/2023-GENERAL-ELECTION-REPORT-1.pdf.

Innovation Village. 2023. "CBN to Freeze Accounts without NIN, BVN Effective April 2024." Innovation Village, 4 December 2024. https://innovation-village.com/cbn-to-freeze-accounts-without-nin-bvn-as-from-april-2024/#:~:text=To%20facilitate%20a%20smooth%20transition,guidelines%20within%20a%20specified%20timeframe.

Innovation Village. 2024. "Nigerians with NIN Reach 104.16 Million as at December 2023 but Falls Short of Government Targets." 4 January 2024. https://innovation-village.com/nigerians-with-nin-reach-104-16-million-as-at-december-2023-but-falls-short-of-government-targets/.

Iwuoha, V. C. 2025a. "European Biometric ID Program in West Africa: Between European External Border Securitization and ECOWAS Free Movement." *African Security*: 1–32. https://doi.org/10.1080/19392206.2025.2491206.

Iwuoha, V. C. 2025b. "European Biometric Borders and (im)Mobilities in West Africa: Reflections on Migrant Strategies for Border Circumvention and Subversion." *Politics & Policy* 53 (1):1–32. https://doi.org/10.1111/polp.12653.

Iwuoha, V. C., and A. D. Edgar. 2024. "European Biometric Border System, Securitization and (im) Mobilities in West Africa." *Alternatives*. 1–12. https://doi.org/10.1177/03043754241287603.

Iwuoha, V., and M. Doevenspeck. 2025. "'Dilemmas of Biometric Nationality': Migration Control, Biometric ID Technology and Political Mobilization of Migrants in West Africa." *Territory, Politics, Governance* 13 (3): 279–304. https://www.tandfonline.com/doi/abs/10.1080/21622671.2023.2205885. https://doi.org/10.1080/21622671.2023.2205885.

Medina-Doménech, R. 2009. "Scientific Technologies of National Identity as Colonial Legacies: Extracting the Spanish Nation from Equatorial Guinea." *Social Studies of Science* 39 (1): 81–112. https://doi.org/10.1177/0306312708097658.

Mignolo, W. D. 2007. "Introduction: Coloniality of Power and De-Colonial Thinking." *Cultural Studies* 21 (2-3): 155–167. https://doi.org/10.1080/09502380601162498.

Musoni, M., E. Domingo, and E. Ogah. 2023. "Digital ID Systems in Africa: Challenges, Risks and Opportunities." Discussion Paper No. 360. https://ecdpm.org/application/files/5517/0254/4789/Digital-ID-systems-in-Africa-ECDPM-Discussion-Paper-360-2023.pdf.

Naija News. 2023. "NIMC Contractor Writes Minister over Non-Payment of Contract Fees for 22 Months." Naija News, 17 October 2023. https://www.naijanews.com/2023/10/17/nimc-contractor-writes-minister-over-non-payment-of-contract-fees-for-22-months/.

Nigeria Data Protection Regulation. 2023. "NITDA." https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf.

Nigeria National Data Strategy. 2022. National Data Strategy (NDA). https://nitda.gov.ng/wp-content/uploads/2022/11/Final-Draft-National-Data-Strategy.pdf.

NIMC. 2023. "Diaspora Services Facts Sheet." NIMC, 18 April 2023. https://nimc.gov.ng/docs/diasporaEnrolmentFactS_april2023.pdf.

NIMC. 2024. "NIMC Approved/Licensed Service Providers." https://nimc.gov.ng/approved-licensed-service-providers/#l4.

NIMC Act. 2007. "National Identity Management Commission Act 2007." https://www.nimc.gov.ng/docs/reports/nimc_act.pdf.

Nishiyama, H. 2015. "Towards a Global Genealogy of Biopolitics: Race, Colonialism, and Biometrics beyond Europe." *Environment and Planning D: Society and Space* 33 (2): 331–346. https://doi.org/10.1068/d19912.

Nnorom, N. 2023. "Over 50% Unbanked Population May Lose Savings to CBN's Currency Redesign – Report." 24 January 2023. https://www.vanguardngr.com/2023/01/over-50-unbanked-population-may-lose-savings-to-cbns-currency-redesign-report/.

Omi, M., and H. Winant. 2015. *Racial Formation in the United States*. 3rd ed. New York: Routledge.

Pantami, I. 2022. "Stay Away from Contract Awards, Pantami Warns NIMC, NIPOST, NITDA Governing Boards." Vanguard, 24 August 2022. https://www.vanguardngr.com/2022/08/stay-away-from-contract-awards-pantami-warns-nimc-nipost-nitda-governing-boards/.

Pantami, I. 2023. "Over 100 Million Nigerians Issued National Identification Number by NIMC." *The Guardian*, 26 May 2023. https://guardian.ng/news/over-100-million-nigerians-issued-national-identification-number-by-nimc/.

Pereira, C., and D. Tsikata. 2021. "Contextualising Extractivism in Africa." *Feminist Africa* 2 (1): 14–48.

Pugliese, J. 2010. *Biometrics: Bodies, Technologies, Biopolitics*. Oxon: Routledge.

Quijano, A. 2000. "Coloniality of Power and Eurocentrism in Latin America." *International Sociology* 15 (2): 215–232. https://doi.org/10.1177/0268580900015002005.

Quijano, A. 2007. "Coloniality and Modernity/Rationality." *Cultural Studies* 21 (2-3): 168–178. https://doi.org/10.1080/09502380601164353.

Sehloho, M. 2024. "Gabon, World Bank Ink $68.5M Digital Finance Agreement." Connecting Africa, 1 August 2024. https://www.connectingafrica.com/author.asp?section_id=816&doc_id=786702.

Scott, J. C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven, CT: Yale University Press.

Solon, O. 2024. "Uganda's Sweeping Surveillance State Is Built on National ID Cards." Bloomberg, 4 June 2024. https://www.bloomberg.com/news/features/2024-06-04/uganda-yoweri-museveni-s-critics-targeted-via-biometric-id-system?leadSource=uverify%20wall.

Speed, M. 2020. "Activists Sound Alarm over African Biometric ID Projects." Aljazeera, 10 December 2020. https://www.aljazeera.com/economy/2020/12/10/activists-sound-alarm-over-african-biometric-id-projects.

Thatcher, J., O. David, and M. Dillon. 2016. "Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data." *Environment and Planning D: Society and Space* 34 (6): 990–1006. https://doi.org/10.1177/0263775816633195.

Toesland, F. 2021. "African Countries Embracing Biometrics, Digital IDs." Africa Renewal, 5 February 2021. https://www.un.org/africarenewal/magazine/february-2021/africancountries-embracing-biometrics-digital-ids.

Udofia, G. 2017. "NIMC: Fast on Cash Liquidation, Slow on ID Card Production and Delivery." Punch, 16 December 2017. https://www.vanguardngr.com/2017/12/nimc-fast-cash-liquidation-slow-id-card-production-delivery/.

World Bank. 2016. "ID4D Country Diagnostic: Côte d'Ivoire." https://documents1.worldbank.org/curated/en/220221473398778343/pdf/Cote-dIvoire-ID4D-Diagnostic-Web040618.pdf.

World Bank. 2018. *Public Savings and Revenue from Identification Systems: Opportunities and Constraints*. Washington, DC: World Bank Group.

World Bank. 2020a. "Nigeria Digital Identification Development Project." https://documents1.worldbank.org/curated/en/250181582340455479/text/Nigeria-Digital-Identification-for-Development-Project.txt.

World Bank. 2020b. "Nigeria Digital Identification for Development (ID4D)." https://financeincommon.org/sites/default/files/2020-11/ID4D.pdf.

World Bank. 2020c. "Nigeria Digital Identification Development Project." https://documents1.worldbank.org/curated/en/250181582340455479/text/Nigeria-Digital-Identification-for-Development-Project.txt.

World Bank. 2021. "Digital Gabon Project." 15 June 2021. https://documents1.worldbank.org/curated/en/301741627956043619/pdf/Gabon-Digital-Gabon-Project.pdf.