International Journal of Development and Economic Sustainability, 14 (1), 33-44, 2026
Print ISSN: 2053-2199 (Print),
Online ISSN: 2053-2202(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Administrative Reach and State Capacity: Interoperability Failures in Nigeria's Digital Identification Infrastructure

Daramola Joseph Omoyele
Independent Researcher
ORCID: 0009-0006-0347-0499
Email: dju78@yahoo.com

doi: https://doi.org/10.37745/ijdes.13/vol14n13344 Published March 24, 2026

Citation: Omoyele D.J. (2026) Administrative Reach and State Capacity: Interoperability Failures in Nigeria's Digital Identification Infrastructure, *International Journal of Development and Economic Sustainability*, 14 (1), 33-44

Abstract: *Nigeria maintains multiple parallel identification systems, including the National Identity Number (NIN), Bank Verification Number (BVN), voter registration, and telecommunications SIM registration, each operating without shared infrastructure. Drawing on qualitative comparative institutional analysis of policy documents, official agency materials, and published scholarship, this paper examines how this fragmented architecture affects administrative reach and state capacity. The analysis finds that parallel registries produce systematic verification inconsistencies, raise transaction costs for citizens and government, constrain financial inclusion, and generate enforcement gaps that weaken service delivery and regulatory effectiveness. The paper argues that the central problem is not the absence of digital identification but the lack of interoperability between systems. By reframing digital identity as public administrative infrastructure, the paper contributes to debates on governance and service delivery in developing states and proposes an evidence based institutional pathway for harmonisation centred on the NIN.*

Keywords: administrative reach, digital identification, financial inclusion, interoperability, state capacity, Nigeria

INTRODUCTION

Nigeria faces a paradox in its digital governance infrastructure. Despite significant investment in identification systems over two decades, citizens must navigate a complex landscape of multiple, uncoordinated identity credentials. The National Identity Number (NIN), administered by the National Identity Management Commission (NIMC), was designed as the foundational national identifier. Yet Nigerians simultaneously maintain Bank Verification Numbers (BVN) for financial services, voter registration cards for electoral participation, driver's licences for vehicle operation, passport numbers for international travel, and Subscriber Identity Module (SIM) registrations for telecommunications access. Each system operates in isolation, maintaining separate databases, registration processes, and verification mechanisms.

This paper asks: how does fragmentation across Nigeria's digital identification systems affect administrative reach and state capacity? The question matters because digital identification has been widely promoted as a mechanism for improving public service delivery, financial inclusion, and state effectiveness in developing countries (World Bank, 2018; Gelb and Clark, 2013). Yet the conditions under which identification systems actually enhance state capacity remain poorly understood, particularly where multiple systems exist without interoperability.

This fragmentation did not emerge through deliberate policy design but through incremental institutional evolution. Each agency responsible for service delivery independently developed identification requirements tailored to its specific mandate. While individually rational, these parallel efforts have produced a costly and inefficient system architecture that undermines the objectives each agency seeks to achieve. The costs are multidimensional: administratively, separate databases duplicate infrastructure and create reconciliation challenges; economically, multiple registration requirements create barriers for unbanked populations; socially, registration fatigue erodes citizen confidence in government digital initiatives; institutionally, verification becomes contingent on which database is queried rather than a consistent cross-agency identification of individuals.

It is important to acknowledge from the outset that unified identification systems are not without risk. Centralised identity infrastructure raises legitimate concerns about government surveillance, data misuse, and exposure in the event of a security breach. These risks are taken seriously in this paper and are addressed directly in the discussion. The argument is not that harmonisation is costless, but that its potential benefits, combined with appropriate legal and oversight safeguards, represent a substantially better institutional arrangement than the fragmented status quo.

This paper argues that Nigeria possesses the foundational infrastructure for unified digital identity but has not implemented the necessary data harmonisation. Drawing on international comparisons with India, South Africa, and the United Kingdom, the study develops an evidence-based institutional pathway for integration centred on the NIN as a universal identifier. Digital identification is treated throughout as a component of public administrative infrastructure, an institutional arrangement with direct implications for state capacity, service delivery, and administrative reach rather than as a primarily technological problem.

The paper is organised as follows. Section 2 reviews the relevant literature and theoretical framework. Section 3 sets out the methodology. Section 4 presents the findings. Section 5 discusses their implications. Section 6 considers implications for research and practice. Section 7 concludes. Section 8 identifies directions for future research.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

Digital Identity Systems and Development

The academic literature on digital identity systems has evolved from technical discussions of implementation toward broader examinations of governance, development impacts, and institutional dynamics. Early scholarship, exemplified by Gelb and Clark (2013), focused on the technical feasibility and administrative benefits of digital identification in developing countries, emphasising efficiency gains and fraud reduction. This work established that digital identity systems could improve service delivery and reduce duplication but gave limited attention to implementation challenges, institutional politics, and coordination failures.

More recent research has adopted a more critical and multidimensional approach. The World Bank's Identification for Development (ID4D) initiative has produced empirical work documenting both successes and failures in digital identity implementation globally (World Bank, 2018; 2021). This research demonstrates that technical capability alone is insufficient: successful implementation requires supportive legal frameworks, institutional coordination mechanisms, privacy protections, and inclusive enrolment strategies. Studies have also shown that simplified identity verification can meaningfully expand access to financial services in underserved populations (Demirguc-Kunt et al., 2018).

The literature on digital identity in Africa has grown considerably. Research on South Africa (Breckenridge, 2014; Razzano, 2021), Kenya (Makulilo, 2016; Nyabola, 2018), and Nigeria (Gelb and Metz, 2018) has documented the complex political economy of identity systems, including tensions between state surveillance capabilities and citizen privacy, the challenge of achieving universal enrolment, and difficulties of inter-agency coordination. These studies document important country-level dynamics but tend to examine individual cases rather than offer systematic frameworks for understanding how architectural choices fragmented versus harmonised shape administrative outcomes across agencies and populations.

System Fragmentation and Institutional Coordination

Public administration scholarship has long recognised that institutional fragmentation creates coordination challenges and inefficiencies (Peters, 2015; Hood and Margetts, 2007). The literature on whole-of-government approaches emphasises that complex policy problems require coordinated action across organisational boundaries, yet institutional incentives frequently promote siloed behaviour and resistance to integration (Christensen and Laegreid, 2007). Research on interoperability and data sharing in government has identified technical, legal, and organisational barriers to integration, including database incompatibilities, legal restrictions on data sharing, and agency resistance to losing control over their own data (Gil-Garcia et al., 2007; Janssen and Estevez, 2013).

New Public Management reforms emphasising agency autonomy and performance metrics may inadvertently encourage fragmentation when each agency optimises for its own metrics rather than system-wide outcomes (Dunleavy et al., 2006). This produces a pattern where rational institutional behaviour at the micro level generates suboptimal outcomes at the macro level, a dynamic observable in Nigeria's proliferation of identification systems. Much of this literature, however, examines developed-country contexts where baseline institutional capacity is relatively high. The additional challenges posed by limited fiscal resources, variable regulatory enforcement, and complex political environments in developing states remain inadequately theorised.

Infrastructural Power and Administrative Reach

Mann’s (1984) concept of infrastructural power, the capacity of the state to penetrate civil society and implement decisions throughout its territory, provides a useful theoretical anchor for this study. a useful theoretical anchor for this study. Digital identification systems can be understood as one component of modern infrastructural power because they extend the state’s practical ability to identify, reach, and serve its population reliably across agencies and across distance. Where identification systems are fragmented and unreliable, the state’s infrastructural capacity is constrained, not because the state lacks authority or technology, but because its institutional arrangements do not enable consistent identification across administrative contexts.

This framing distinguishes the present study from accounts that treat digital ID primarily as a technological or security matter. The central question is not whether Nigeria has identification technology, but whether its institutional arrangements enable consistent and reliable identification across agencies, particularly for populations distant from administrative centres or dependent on multiple agencies for access to services.

Contribution of This Study

A growing but still limited body of scholarship examines digital identity governance in sub-Saharan Africa. This paper contributes to that literature by providing an integrated institutional analysis of Nigeria's identification ecosystem that brings together administrative, economic, and governance perspectives not addressed together in existing studies. It develops a comparative analytical framework for assessing how fragmented and harmonised identification architectures produce different administrative outcomes, drawing on evidence from India, South Africa, and the United Kingdom as reference cases. It documents the specific mechanisms through which fragmentation constrains state capacity and administrative reach and proposes an evidence-based institutional pathway for harmonisation grounded in Nigeria's existing institutional conditions. The study does not claim to be the definitive or exhaustive treatment of digital identity governance in Nigeria; it offers a systematic institutional analysis intended to advance both scholarly understanding and policy deliberation.

METHODOLOGY

Research Design

This study employs qualitative comparative institutional analysis, using Nigeria as the primary case and drawing on India, South Africa, and the United Kingdom as analytical reference points. This comparative case approach is appropriate given the research question, which concerns how institutional arrangements, specifically the degree of interoperability between identification systems, shape administrative outcomes across agencies and populations. across agencies and populations. Cases were selected to reflect variation in institutional architecture (fragmented versus harmonised systems) and relevance to the Nigerian context in terms of scale, developmental stage, and governance challenges. India was selected because of its comparable scale and developing-economy context; South Africa because of its regional proximity and the maturity of its integrated national identification system; and the United Kingdom because of its established model of using a single functional identifier across multiple government services.

Data Sources

The analysis draws on three categories of evidence reviewed for the period from approximately 2005 to 2024, selected to capture the main phases of digital identification development in Nigeria and the reference cases. The first category comprises primary documentary evidence, including legislation, policy frameworks, regulatory documents, and official publications issued by the National Identity Management Commission (NIMC), the Nigeria Inter-Bank Settlement System (NIBSS), the Independent National Electoral Commission (INEC), and relevant government ministries, accessed through official agency websites and government gazettes. The second category comprises comparative documentary materials from India, South Africa, and the United Kingdom, including official publications from the Unique Identification Authority of India (UIDAI), South Africa's Department of Home Affairs, HM Revenue and Customs, and World Bank ID4D reports. The third category comprises peer-reviewed scholarship in public administration, development economics,

African governance, and information systems. Sources were selected on the basis of direct relevance to identity architecture, interoperability, service delivery, administrative coordination, and state capacity.

Analytical Approach

The analysis proceeds in two stages. The first stage maps Nigeria's identification infrastructure by examining the origins, institutional mandates, data governance arrangements, and interoperability status of the major systems currently in use. This stage focuses on how these systems were established, the degree to which they operate independently or in coordination, and the administrative consequences of parallel development across sectors.

The second stage applies the theoretical framework of infrastructural power and administrative reach to interpret how fragmentation produces specific institutional effects in verification reliability, administrative cost, financial inclusion, service delivery, and regulatory coordination. Themes were identified through systematic comparison of recurring patterns across the documentary evidence, with particular attention to duplication, inconsistency, access burden, and coordination failure. The international reference cases were then used as analytical benchmarks to assess what alternative institutional arrangements look like in practice and what forms of governance support interoperability. The analysis is interpretive rather than causal: it develops an institutional argument from documentary and comparative evidence rather than testing formal hypotheses.

Limitations

Several limitations should be noted. This study is not based on original survey data, administrative microdata, or primary fieldwork. It is a conceptual and policy-focused institutional analysis whose claims rest on documentary and comparative evidence rather than original data collection. Quantitative figures cited from agency publications and secondary sources have not been independently verified. The comparison cases differ from Nigeria in important institutional and developmental respects, and lessons drawn from international experience require contextual qualification before application. These limitations are acknowledged in the interpretation of findings, which favours indicative and directional claims over precise causal assertions.

FINDINGS

Structural Fragmentation of Nigeria's Identification Infrastructure

Nigeria's identification ecosystem has evolved through sector-specific initiatives rather than coordinated national planning. The NIN, administered by NIMC, was specifically designed as a comprehensive national identifier incorporating biometric capture, demographic data, and a unique number for each citizen and legal resident. Official NIMC publications indicate that enrolment has expanded substantially since the NIN's introduction, though universal population coverage remains incomplete, particularly in rural and remote areas (National Identity Management Commission, 2023).

The BVN, managed by the NIBSS and launched in 2014, was designed to reduce banking fraud and enable customer verification across financial institutions. It has achieved notable penetration within the banked population while replicating many of the biometric capabilities already present in the NIN system. Beyond these two primary systems, Nigerians also interact with voter registration databases (INEC), international passports (Nigeria Immigration Service), driver's licences (Federal Road Safety Corps), and SIM registration databases held by telecommunications providers under regulatory

oversight. Each system serves a legitimate purpose within its domain but operates with minimal integration with the others.

The technical infrastructure varies considerably across systems. Some employ sophisticated biometric capture; others rely primarily on document verification and manual data entry. Database architectures, data formats, and access protocols differ across agencies. Available evidence suggests that the primary barriers to harmonisation are institutional rather than technical: each agency has built administrative interests around independent data control, and existing mandates do not require cross-agency coordination.

Recent policy episodes illustrate the practical consequences of this fragmentation. The rollout of NIN-SIM linkage requirements demonstrated both the growing centrality of the NIN and the institutional strain created when one system is expected to authenticate identities that were previously managed through separate sectoral arrangements. Similarly, efforts to strengthen BVN-NIN linkage reflect a recognition by policymakers that fragmented identifiers create avoidable verification and compliance problems across the financial system. These developments do not in themselves amount to full interoperability, but they indicate that the pressures generated by institutional fragmentation are already shaping administrative reform efforts in Nigeria.

Verification Inconsistencies Across Public Institutions

The coexistence of parallel registries without linkage mechanisms produces data quality problems that accumulate over time. Citizens may supply inconsistent information across different registration systems through innocent error, changes in circumstances, or administrative transcription differences. A person's name may be rendered differently across NIN, BVN, and voter registration records. Addresses may be current in one database but outdated in others. Biometric data captured at different times using different equipment may not match precisely, generating verification failures even for individuals with legitimate credentials.

The structural consequence is that verification outcomes depend on which database is queried and its current state of accuracy at that moment, rather than on a consistent cross-agency identification of the individual. Where institutions attempt cross-system verification, the absence of a shared authoritative source means that corrections and updates must be propagated manually across multiple databases a process prone to delays, inconsistencies, and divergence over time. This is not primarily a problem of data quality in any individual system; it is a structural property of uncoordinated parallel registries.

Administrative Costs and Resources Duplication

Maintaining separate identification infrastructures imposes recurring fiscal costs. Each system requires dedicated hardware and software, physical registration centres and biometric equipment, personnel for enrolment, verification, and maintenance, cybersecurity measures, and public communication campaigns. While precise aggregate cost data is not publicly available, maintaining functionally duplicated infrastructure across multiple agencies with overlapping mandates likely generates substantial inefficiencies relative to a consolidated approach (Gelb and Metz, 2018; World Bank, 2018).

The citizen-facing burden is more directly observable. Registration centres tend to be concentrated in urban areas, requiring rural residents to travel significant distances. Documentation requirements vary across systems, obliging citizens to navigate different procedures for what is functionally the same task: establishing their identity. When personal information changes, address, marital status, and name

updates must be submitted separately to each system without any guarantee of consistency across records. This burden falls disproportionately on lower-income populations who can least absorb the time and financial cost of multiple registrations.

Constraints on Financial Inclusion and Service Delivery

Multiple identification requirements create barriers to financial participation, particularly for vulnerable and rural populations. Available data suggests that a significant portion of Nigeria's adult population remains unbanked, and access to financial services is constrained in part by the cumulative burden of obtaining multiple identifiers (Demirguc-Kunt et al., 2018; World Bank, 2021). Each additional mandatory identifier raises the threshold of entry into the formal financial system for individuals who may already face obstacles of distance, documentation, or cost.

The implications extend beyond banking. Government social protection and welfare programmes depend on reliable identification of beneficiaries across agencies. Where databases conflict or cannot be cross-referenced, targeting becomes imprecise, exclusion errors increase, and programme efficiency declines. The state's practical ability to reach specific populations, particularly those in greatest need of services, is directly constrained by the unreliability of identification across systems. This is the core sense in which fragmentation limits administrative reach: not in principle, but in the institutional capacity to consistently identify, locate, and serve individuals across agencies.

Enforcement and Regulatory Coordination Gaps

Fragmented identification creates structural limitations for regulatory and law-enforcement agencies. When institutions cannot reliably match individuals across databases, compliance monitoring, investigation, and record-keeping become more difficult. Individuals may appear under different identifiers in separate systems, complicating financial regulation, administrative enforcement, and legal administration. This is an institutional coordination problem rather than primarily a security technology problem: verification depends on which database is consulted rather than a consistent cross-agency identification framework.

Nigeria's regulatory agencies, including the Economic and Financial Crimes Commission and the Nigeria Police Force, face impediments in sharing information across databases even where statutory authority exists. Without integrated systems, connections between records held in different agencies may only be discovered through labour-intensive manual investigation. This may limit the capacity for cross-system analysis that could support more effective compliance monitoring and regulatory coordination. It should be noted, however, that these effects are inferred from the structural features of fragmented architectures and from international comparative experience; direct empirical measurement of their magnitude in Nigeria falls outside the scope of this study.

Erosion of Public Trust

A less immediately quantifiable but institutionally significant finding concerns citizen confidence in government digital initiatives. Each additional registration requirement imposes procedural complexity and time costs. Where citizens experience these requirements as redundant or poorly coordinated, compliance motivation may weaken, and disengagement from formal systems may increase in favour of informal alternatives. Public trust, once eroded, is difficult to rebuild and creates headwinds for subsequent digital governance initiatives regardless of their technical or policy merit. While this effect cannot be directly measured from the evidence available to this study, it is a consistent

theme in comparative research on identification systems in developing states (Gelb and Metz, 2018; World Bank, 2018).

International Comparative Evidence

International cases indicate that harmonised identification architectures are technically achievable and institutionally beneficial at a comparable scale. India's Aadhaar system, administered by the Unique Identification Authority of India (UIDAI), provides a single 12-digit identifier to over one billion residents and serves as the reference point for banking through e-KYC processes, telecommunications registration, employment verification, and social welfare delivery. The architecture establishes a common verification platform while allowing sector-specific agencies to link services through application programming interfaces. Official UIDAI reporting suggests that the system has been associated with simplified verification procedures and reduced duplication in enrolment (Unique Identification Authority of India, 2023), though the system has also generated ongoing debate about privacy and data protection that has required iterative legislative and judicial attention.

South Africa's 13-digit national identity number, issued by the Department of Home Affairs, functions as the primary identifier for voter registration, banking, employment, social security, and law enforcement across all agencies (Razzano, 2021). Its effectiveness derives from strong backend integration among government agencies, standardised verification protocols, legislative mandates for use across sectors, and data protection frameworks. The United Kingdom employs the National Insurance number across tax, employment, pension, and related government services, with departments accessing shared identity infrastructure through secure interfaces rather than maintaining separate registration systems (Hood and Margetts, 2007). The international cases reviewed here suggest that harmonised identification systems can support administrative efficiency, broaden access to services, improve verification reliability, and strengthen regulatory coordination when accompanied by appropriate legal safeguards, oversight mechanisms, and evolving institutional arrangements to manage privacy-related risks.

Taken together, these findings show that fragmentation affects more than identification accuracy alone. It shapes how citizens encounter the state, how agencies coordinate with one another, how efficiently services are delivered, and how reliably administrative authority can be exercised across sectors. The cumulative effect is to weaken the coherence of public administration by making identification contingent, duplicative, and uneven rather than consistent, portable, and system-wide.

DISCUSSION

The findings support the theoretical framework developed in Section 2 and extend it in several respects. Nigeria's identification fragmentation is primarily an institutional problem, the product of sequential, autonomous, sectoral development that was individually rational but collectively suboptimal. The mechanism through which fragmentation constrains state capacity is consistent across the findings: parallel databases without interoperability undermine the reliability of identification across agencies, which in turn limits administrative reach, increases transaction costs, constrains financial inclusion, and reduces regulatory coordination. This is the core process through which fragmentation attenuates what Mann (1984) terms infrastructural power.

The theoretical value of the infrastructural power framework here is that it reframes digital identification from a technology procurement question to a governance design question. A state's practical capacity to deliver services, regulate economic activity, and implement welfare programmes

depends on its ability to reliably identify and reach its population across agencies and geographies. Where identification is fragmented, this capacity is constrained not by lack of will or technology, but by institutional arrangements that do not support consistent cross-agency identification. Nigeria's case illustrates how technically capable individual systems can collectively produce an infrastructure that constrains rather than enables state capacity.

A further implication is that fragmentation may persist not only because integration is technically demanding, but also because separate systems confer institutional advantages on the agencies that control them. Standalone databases can reinforce bureaucratic autonomy, preserve control over budgets and procurement, and strengthen an agency's strategic relevance within government. In this sense, fragmentation is not merely an accidental by-product of administrative history; it can also become politically and organisationally self-reinforcing. Any serious reform strategy must therefore address not only technical integration and legal reform but also the incentive structure facing agencies that may perceive harmonisation as a loss of institutional control.

The international comparisons are instructive about the conditions under which harmonisation succeeds. Across the three cases examined, effective harmonisation required: legislative mandates establishing a primary identifier, inter-agency governance frameworks with decision-making authority, phased technical integration through API-based access rather than wholesale system replacement, data protection legislation, and sustained political commitment over multiple government cycles. None of these conditions currently exists in Nigeria at the requisite level. This analysis suggests that the principal obstacle to harmonisation is less technical feasibility than institutional politics, particularly where agencies have developed vested interests around independent data control.

A workable implementation sequence would begin with high-feasibility and high-impact integrations, particularly NIN linkage with BVN infrastructure, before extending progressively to telecommunications registration, voter registration, passport and immigration systems, driver licensing, and other government services.

The paper does not argue that a unified identification system is risk-free. Centralised identity infrastructure creates genuine concerns about government surveillance, data breaches, and potential misuse by state actors or officials. These risks are not hypothetical. However, the international evidence reviewed here indicates that they can be substantially mitigated through appropriate institutional design: access controls limiting who can query identity data and for what authorised purposes, comprehensive audit trails, independent oversight bodies with investigative authority, and transparent reporting mechanisms. The choice facing Nigerian policymakers is not between a risk-free fragmented system and a risky unified one; it is between the documented, compounding costs of fragmentation and the manageable, addressable risks of a well-designed integrated system with appropriate safeguards.

Implications for Research and Practice

Implications for Research

This study suggests several directions for further scholarly work on digital governance in developing states. First, it demonstrates the analytical value of applying infrastructural power theory to digital identity systems. Future research should develop this framework further, including consideration of how identification reliability might be operationalised as a measurable dimension of state capacity in comparative governance studies.

Second, the study highlights a gap in comparative research on identity system architectures. Existing comparisons tend to contrast countries with different systems without offering systematic frameworks for understanding how specific architectural choices produce specific administrative outcomes. A more systematic comparative study, applied across a wider sample of developing and emerging economies, would advance understanding of the conditions under which harmonisation improves governance.

Third, the mechanisms through which fragmentation affects public trust in digital governance deserve dedicated empirical investigation. Survey and experimental methods could test the relationship between registration burden, perceived redundancy, and compliance behaviour, a relationship that this study identifies theoretically from documentary evidence but does not measure directly.

Implications for Practice

For Nigerian policymakers, the findings point toward a harmonisation approach centred on the NIN as the universal identifier, pursued through phased backend integration rather than the creation of new systems. A workable implementation sequence would begin with high-feasibility and high-impact integrations, particularly NIN linkage with BVN infrastructure, before extending progressively to telecommunications registration, voter registration, passport and immigration systems, driver licensing, and other government services. First: NIN linkage with BVN infrastructure (which already shares biometric architecture), followed by telecommunications SIM registration, voter registration, passport and immigration systems, and driver's licences. Progressive integration of other government services could follow as technical and governance capacity matures.

The legislative and governance infrastructure required for harmonisation includes amendments establishing NIN as the primary identifier across government services; inter-agency coordination mechanisms with authority to resolve integration disputes; data sharing protocols specifying permitted uses and access controls; and independent oversight bodies with powers to audit access and investigate misuse. These arrangements are not novel; analogues exist in each of the reference cases, but they require sustained political commitment and executive-level sponsorship. The transition should be planned as a multi-year process with clear milestones, public communication, and mechanisms to manage service continuity for citizens holding existing credentials.

For other African governments facing analogous challenges of incremental identification proliferation, the Nigerian case offers a comparative illustration of the cumulative institutional costs of uncoordinated sectoral evolution. The evidence reviewed here suggests that early investment in interoperability standards and governance frameworks is substantially less costly than retrofitting integration onto mature, politically entrenched systems.

CONCLUSION

Nigeria's proliferation of uncoordinated identification systems represents a significant and underappreciated constraint on state capacity and administrative reach. This paper has argued that the core problem is not the absence of digital identification technology, but the lack of interoperability between systems that prevents the state from reliably identifying, reaching, and serving its population across agencies. This is an institutional problem, not a technical one, and it calls for an institutional response.

The theoretical contribution of this study is to situate digital identification within a framework of infrastructural power and administrative reach, linking the architecture of identification systems to the practical capacity of the state to govern. This framing moves the debate beyond technological reform discourse toward questions of institutional design, coordination, and governance, where the real obstacles and opportunities lie.

The practical contribution is an evidence-based case for NIN-centred harmonisation, grounded in international comparative experience and informed by an analysis of Nigeria's specific institutional conditions. The international cases reviewed here, India, South Africa, and the United Kingdom—suggest that harmonised identification systems can support administrative efficiency, broaden access to services, improve verification reliability, and strengthen regulatory coordination when accompanied by appropriate legal safeguards and oversight mechanisms.

The costs of continuing on the current fragmented trajectory grow with each new standalone system added to the ecosystem, each citizen excluded from services, and each agency unable to coordinate effectively with others. The case for reform is therefore not simply that harmonisation is technically desirable, but that fragmented identity architecture imposes cumulative administrative, economic, and governance costs that weaken the state's practical capacity to govern. Ultimately, the effectiveness of digital identification depends less on how many identifiers a state creates than on whether those identifiers operate as a coherent public administrative infrastructure.

Future Research

This study identifies several directions for future research. First, cost-benefit analysis of harmonisation approaches including quantification of administrative savings, inclusion gains, and transition costs, would strengthen the evidence base for investment decisions. Such analysis requires access to administrative microdata not available for this study.

Second, original empirical research on the citizen experience of identification fragmentation in Nigeria, using survey or qualitative methods, would provide the demand-side evidence that this study's documentary approach cannot supply. Participatory methods would also be valuable in capturing the experiences of populations most severely affected by exclusion from services.

Third, technical architecture studies examining specific protocols and standards for secure API-based integration between Nigeria's existing systems, including interoperability between NIN and BVN infrastructure, would translate the institutional arguments developed here into actionable specifications.

Fourth, political economy research on the distributional consequences of harmonisation, the interests of institutional stakeholders, and the conditions under which reform coalitions can be assembled to overcome agency resistance would address the implementation dynamics that this study, as an institutional and documentary analysis, treats mainly at the structural level.

Fifth, comparative studies of identification governance in other West African states facing analogous challenges of fragmented identification infrastructure would test the generalisability of the institutional framework developed here and generate regionally grounded policy learning.

REFERENCES

Breckenridge, K. (2014). Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present. Cambridge University Press.

Christensen, T., & Lægreid, P. (2007). The whole-of-government approach to public sector reform. Public Administration Review, 67(6), 1059–1066.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution. World Bank.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead: Long live digital-era governance. Journal of Public Administration Research and Theory, 16(3), 467–494.

Gelb, A., & Clark, J. (2013). Identification for development: The biometrics revolution (Working Paper No. 315). Center for Global Development.

Gelb, A., & Metz, A. D. (2018). Identification revolution: Can digital ID be harnessed for development? Center for Global Development.

Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-government: Impediments and benefits of information-sharing projects in the public sector. European Journal of Information Systems, 16(2), 121–133.

Hood, C., & Margetts, H. (2007). The tools of government in the digital age. Palgrave Macmillan.

Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance: Doing more with less. Government Information Quarterly, 30, S1–S8.

Levi, M., & Reuter, P. (2006). Money laundering. Crime and Justice, 34(1), 289–375.

Lyon, D. (2009). Identifying citizens: ID cards as surveillance. Polity Press.

Makulilo, A. B. (2016). African data privacy laws. Springer.

Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. European Journal of Sociology, 25(2), 185–213.

Matfess, H. (2017). Women and the war on Boko Haram: Wives, weapons, witnesses. Zed Books.

National Identity Management Commission. (2023). January 2023 enrolment report. https://nimc.gov.ng/nin/enrolment-report/jan-2023

Nyabola, N. (2018). Digital democracy, analogue politics: How the internet era is transforming Kenya. Zed Books.

Peters, B. G. (2015). Pursuing horizontal management: The politics of public sector coordination. University Press of Kansas.

Razzano, G. (2021). Digital identity in South Africa: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa. Research ICT Africa. https://researchictafrica.net/research/digital-identity-in-south-africa-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/

Unique Identification Authority of India. (2023). UIDAI annual report 2022–23. https://uidai.gov.in/images/UIDAI_Annual_Report-2022-23_English.pdf

World Bank. (2018). Principles on identification for sustainable development: Toward the digital age.

World Bank. (2022). The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19.

Zenn, J. (2021). Boko Haram's factional feuds: Internal extremism and external interventions. Terrorism and Political Violence, 33(3), 616–648.