NIU Journal of Legal Studies Copyright©2026
Nexus International University ISSN: *3007-1860;* 12(1): 39-49

Security-Driven Identification and Data Privacy: Lessons from Nigeria and India

OGHOMWEN RITA OHIRO
University of Benin, Benin City, Nigeria

Abstract. As mobile phones have become an integral part of socio-technical participation, states have made it imperative to collect biometric data in exchange for access to a network for the purpose of ensuring national security. This paper examines the conflict between national security interests and the right to privacy in Nigeria and India in the context of the obligation of registration of SIMs and linkage to identity through a biometric system. Through a doctrinal research methodology and comparative approach, it examines the legal frameworks in Nigeria and India, including the Registration of Telephone Subscribers Regulations 2011 in Nigeria and the Telecommunications Act 2023 in India. It also examines the legal systems in both countries through the lens of the New Social Contract theory. This article finds that the security benefits in Nigeria and India are uncertain due to poor implementation practices, such as the black market for pre-registered SIM cards and marginalisation through digital exclusion. In addition, there is a lack of independent oversight, which poses threats of mass surveillance. The existing policies on mandatory SIM registration embody a coercive social contract as opposed to a consensual one, reflecting an asymmetrical transfer of power to the state with no corresponding obligation regarding the right to privacy. There is a need to ensure that the legal frameworks in both countries comply with international standards of necessity and data minimisation. The creation of separate supervisory structures and judicial authority in the security-privacy trade-off in Nigeria and India is important in the rebuilding of democratic legitimacy.

Keywords: SIM Registration, National Security, Right to Privacy, New Social Contract Theory, Biometric Data, Nigeria, India, Data Minimisation, Mass Surveillance, Digital Exclusion

1. Introduction

Mobile phones are now socio-technical infrastructure, they are not mere tools of communication but are necessary for banking, welfare distribution, digital identification, political participation and everyday social interaction.[174] In response to threats to national security such as terrorism, kidnapping, cybercrime and digital fraud, governments have turned to mandatory SIM registration as a solution.[175] In Nigeria and India for example, SIM card registration is a mandatory process for all mobile phone users, requiring them to register their SIM cards with their respective Mobile Network Operators (MNOs) by providing proof of identification, personal data and biometric data to gain

174 M. Schomerus and A. S. Rigterink, *"And Then He Switched off the Phone": Mobile Phones, Participation and Political Accountability in South Sudan's Western Equatoria State*, *Stability: International Journal of Security & Development*, 4(1), Art. 10 (2015), 2, https://doi.org/10.5334/sta.ew

175 Majumdar, P. (2025). Implementing Aadhaar-linked biometric re-authentication can prevent terrorist misuse of India's mobile networks. *American Journal of Information Science and Technology, 9*(2), 129. https://doi.org/10.11648/j.ajist.20250902.11

access to voice and data services.[176] Governments enforce these measures by imposing strict deadlines, requiring subscribers to comply within the stipulated period or risk disconnection.[177] Similar security rationales exist in India.

While SIM registration and identity verification mechanisms have been set up by these countries, regulation, identity infrastructure and data governance frameworks lag behind.[178] This makes the assumption that each SIM card corresponds to a single, verifiable individual unrealistic. Studies show that because of the challenges associated with SIM registration process in many countries, users resorted to practices such as third party registration, shared SIM ownership within households, and the emergence of informal and black markets for re-registered SIM cards.[179] The reality therefore, is that the SIM registration and linkage to identity has informal and illegal practices have affected anonymity, hereby undermining both the effectiveness and legitimacy of security-oriented regulation.

The justification is that SIM registration and linkage to identity is a crime prevention strategy that is effective for the enforcement of law and national security, however, many studies reveal that this claim remains inconclusive.[180] In fact, Salami and Oloyede argue that despite the implementation of such regulations, including SIM-NIN linkage in Nigeria for over two years, crime rates have not shown a significant decrease attributable to these measures.[181] Criminals have shown the ability to circumvent these regulations by accessing and using illegally registered SIM cards through black markets, revealing a persistent challenge in effectively combating crime through mandatory SIM registration alone.[182] This raises the obvious question: if SIM registration cannot reduce crime, how then can its intrusion on privacy and anonymity be justified solely on the basis of speculative security gains?

The use of biometric ID in mandatory SIM registration has serious implications for privacy and data protection.[183] These risks include, data leaks, exclusion due to poor quality data, among others.[184] As will be discussed below, these SIM cards are linked to biometric national identity systems without clear limits on data access, retention, secondary use or sharing across agencies. In Nigeria and India, biometric data are collected and stored within fragmented databases managed by different bodies, creating risks of misuse, breach and function creep.[185] Several problems have been found in Nigeria's verification process, including insufficient supervision. In some instances, the biometric and

176 India. (2023). *Telecommunications Act, No. 44 of 2023*, s. 3(7).

177 Robert, T., & Oloyede, R. (2022, May 5). Why millions of Africans are right to resist mobile SIM card registration. Institute of Development Studies. 5 https://www.ids.ac.uk/opinions/why-millions-of-africans-are-rightto-resist-mobile-sim-card-registration/

178 Majumdar, 2025, 129

179 Luhanga, E., et al. (2023). User experiences with third-party SIM cards and ID registration in Kenya and Tanzania. arXiv:2311.00830 [cs.HC], 1. https://doi.org/10.1145/nnnnnnn.nnnnnnn

180 Tumang, B. (2025). The SIM registration legislation in enhancing mobile security against cyber threats. *International Journal of Multidisciplinary: Applied Business and Education Research*. https://doi.org/10.11594/ijmaber.06.02.17; Salami, A. O., & Oloyede, R. (2024). Digital identity, surveillance, and data protection in Africa. In R. A. Akongburo et al. (Eds.), *African data protection laws* (p. 138). Walter de Gruyter GmBH & Co KG Jentzsch, N. (2012). Implications of mandatory registration of mobile phone users in Africa. *Telecommunications Policy, 36*(8). https://www.sciencedirect.com/science/article/abs/pii/S0308596112000511; GSMA. (2024, February 23). The mandatory registration of prepaid SIM card users: Addressing challenges through best practice. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

181 Salami and Oloyede, 2024, p138.

182 Salami and Oloyede, 2024, p138.

183 Sesan, G., & Roberts, T. (2025). Digital-ID in Africa: Assessing progress and challenges to date. In G. Sesan & T. Roberts (Eds.), *Biometric digital-ID in Africa: Progress and challenges to date – Ten country case studies* (pp. 19–27). Institute of Development Studies.

184 Sesan and Roberts, 2025, p25.

185 Sesan and Roberts, 2025, p25.

personal data collected are not thoroughly checked, which results in errors in the database.[186] Other issues are the risks are associated with mandatory SIM registration, including implications for data privacy, state surveillance, and the exclusion of marginalised groups.[187] Linking SIM cards to biometric national identity systems is said to increase the surveillance capacity of governments, sometimes without adequate safeguards or oversight mechanisms.[188]

This paper adopts the New Social Contract Theory as propounded by Chesterman as its theoretical framework. Chesterman argues that citizens of a society, in order to enjoy the benefits of securities and the conveniences of modern life, may legitimately trade some aspects of informational autonomy to the state.[189] Ideally, these trade offs are governed by the rule of law, constrained by the principle of transparency and proportionality, and subject to robust oversight and accountability.[190] This theory provides a normative lens for assessing when security-driven data practices remain democratically legitimate and when they amount to unjustifiable rights infringements.

This paper critically analyses the legitimacy, governance designs and accountability structures in the SIM registration regimes in Nigeria and India, focusing on how security driven data practices are authorised and implemented. The primary aim is to shift the focus from security outcomes to legitimacy by tackling questions of consent, reciprocity, oversight and accountability which are important in democratic governance but easily affected by security narratives. This paper argues that the mandatory SIM card registration and linkage to national identity framework in some countries appears to be a coercive rather than a consensual form of the New Social Contract by which citizens surrender informational autonomy for promised security benefits. There are no guarantees of transparency, proportionality, oversight and accountability required to ensure that the state does not abuse the process. The process of registration and linkage to identity is usually justified as counter-terrorism, crime and kidnapping prevention tool, however, a comparative analysis of Nigeria and India reveals that there is little evidence that this has been effective. On the other hand, the level of privacy intrusions is evident. The argument of this study there is need to shift the focus from mere identification which increases the chances of state surveillance, data misuse and exclusion to a framework that aligns with the principles of necessity, proportionality, data minimisation, independent oversight, and meaningful consent.

2. Research Methodology

In this paper, the doctrinal research methodology and the comparative approach are used to examine mandatory SIM card registration regimes in Nigeria and India. This analysis strictly focuses on the examination of the legitimacy governance design and accountability structures in these regimes. It does not include an empirical analysis of the effectiveness of SIM registration in reducing crime. Primary sources of law such as the Data Protection Acts in the countries, telecommunications statutes, SIM registration regulations, data protection laws, policy documents, and judicial decisions are analysed. The essence of the analysis is to determine how law authorises data collection, structures surveillance powers, and provides safeguards for privacy and accountability. These countries were selected because they share similar structural features, rapid mobile penetration, heavy reliance on mobile connectivity, and security-driven justifications for mandatory SIM registration. These are often linked to national identity systems and biometric data collection. However, there are some notable differences in data protection frameworks and oversight mechanisms, allowing meaningful comparison. This paper compares the quality of the legal and normative bargain between the state and citizens, using legality, proportionality, oversight and accountability as indicators of whether SIM registration constitutes a legitimate or coercive security–privacy trade-off. The analysis of each country adopts a uniform framework addressing the state's security rationale, the governing legal regime, data protection and surveillance safeguards, and the

186 Aragba-Akpor, S. (2024). Nigeria's SIM card registration: Global trend with broader implications. *Science Nigeria*, 2563. https://sciencenigeria.com/nigerias-sim-card-registration-global-trend-with-broader-implications/

187 Robert and Oloyede, 2024.

188 Privacy International, *Africa: SIM card registration only increases monitoring and exclusion* (5 August 2019), https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion.

189 Chesterman, S. (2011). *One nation under surveillance: A new social contract to defend freedom without sacrificing liberty* (pp. 250). OUP Oxford.

190 Chesterman, 2011, p250.

broader social consequences, ultimately assessed through the lens of the New Social Contract Theory.

3. Theoretical Framework

The social contract theory views modern governance as an exchange where individuals consent to limitations on autonomy in return for collective goods such as security, order, and welfare.[191] In the context of mandatory SIM card registration, the surrender of anonymity and personal data is part of an implicit security bargain between the state and citizens. Citizens agreeing to share their personal information with the state or private entities in exchange for perceived benefits like security and the convenience of living in a modern world is a social contract.[192]

Chesterman argues that in giving up a degree of anonymity for security or other benefits, there must be consent on the part of the citizens, to ensure legitimacy.[193] In light of modern threats to many nations, extensive data collection is inevitable, it is not practical to ban collection, but laws should focus on strict rules for use, oversight and accountability of intelligence. This gives rise to a social contract where citizens accept more data access by the state in exchange for security and convenience, but under publicly debated, transparent laws that prevent abuse. For instance, in India, the decision in *Justice K.S. Puttaswamy v. Union of India*[194], arguably introduces a constitutional social contract, which restricts the state's power to collect data, the power is not absolute but a conditional grant from the people, subject to the fundamental right to privacy in Article 21 of the Constitution.[195]

Chesterman highlights several features that set this new contract apart from the traditional concept of social contract, including the possibility to some extent of opting out.[196] Firstly, individuals can attempt to minimise their digital footprint by avoiding certain technologies or online platforms.[197] It is important to state that mandatory policies such as SIM card registration and linking them to biometric IDs complicate this notion of opting out..Under the New Social Contract Theory, data collection must be based on consent, but in most countries, this consent is affected by the state's control over essential services.[198] In order to maintain a certain level of individual autonomy, citizens should be able to minimise their digital footprints. In sub-Saharan Africa and some parts of Asia, where mobile phones are necessary for banking, communication and identity, disconnection is not a personal choice but is necessary for survival in the absence of reliable physical infrastructure.[199] In September 2024, the NCC of Nigeria disconnected over 20 million SIM cards that were not linked to National Identity Numbers (NIN), stating that the SIM cards will be reactivated once the subscribers provide their NIN.[200]

In India, there is the Aadhaar, which is a document containing a 12digit unique identification number and the personal details(name, address, date of birth) of an individual.[201] It also contains the biometric data of an

191 Chesterman, 2011, p250.
192 Chesterman, 2011, p250.
193 Chesterman, 2011, p250.
194 **(2017) 10 SCC 1.**
195 1950 (adopted Nov 26, 1949, effective Jan 26, 1950).
196 Chesterman, 2011, p251.
197 Chesterman, 2011, p251.
198 Mohanty, S. (2025). Data, ethics, and power: Reimagining the social contract in the digital age. *International Journal for Research in Applied Science & Engineering Technology, 13*(X), 1629.
199 Edmund, E. (2017). Implementing customer-identity management to combat SIM-card fraud: A security framework for emerging market telcos. *International Journal of Computer Applications Technology and Research, 6*(12), 533.; Jain, A. K., Ross, A., & Nandakumar, K. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1). https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf
200 Okonji, E. (2024, February 28). Nigeria: Telcos begin total disconnection of unregistered SIM cards on Wednesday. ARISENEWS. https://www.arise.tv/nigeria-telcos-begin-total-disconnection-of-unregistered-sim-cards-on-wednesday/
201 Sadhya, D., & Sahu, T. (2024). A critical survey of the security and privacy aspects of the Aadhaar framework. *Computer & Security, 140.* https://doi.org/10.1016/j.cose.2024.103782

individual, including, fingerprints, facial images and iris scans.[202] The data contained in the Aadhaar is used for authentication while registering SIM cards, accessing government services, opening bank accounts among others.[203] This collection is undoubtedly highly intrusive, and there is no opt-out alternative that is not as intrusive. The transfer of personal information under this new social contract is no longer centralised but distributed among a wide range of actors.[204] In Nigeria, for example, there is decentralized handling of personal data across telecom and financial sectors.[205] This decentralization of data handling increases the complexity of protecting privacy and ensuring accountability, as individuals must navigate a fragmented system where their information is shared across various entities with differing levels of oversight and security measures.

Accountability is an important indicator of legitimacy, trust and proper functioning of ID systems.[206] The principle of accountability means that government must be answerable to the people for misuse of data.[207] This can be done by embedding principles designed to ensure proper regulation and oversight in the framework.[208] Accountability mechanisms include ensuring that there are consequences of actions that causes breach of data for instance or outright illegal invasion of privacy by the state, or other actions relating to the use, retention, and dissemination of collected information.[209] Transparency is also important to prevent misuse or overreach.[210] The question now is not whether data collection by the state should be bound but whether this process is legitimate or coercive based on the principles of legality, necessity, proportionality, independent oversight, and effective remedies. It goes without saying that where these elements are absent or underdeveloped, the social contract cannot be said to be a balanced social contract but an asymmetrical transfer of power to the state, with significant implications for privacy, surveillance, and digital citizenship. There are several instruments that seek to strike a balance between the rights of individuals and national security concerns, which form the international legal framework for data protection and surveillance.[211]

4. Legal Framework for SIM Registration in Nigeria

The legal framework for SIM registration in Nigeria includes the Nigerian Communications Act[212] and the Nigerian Communications Commission (NCC) Regulations on the Registration of Telephone Subscribers[213] which provide that all SIM cards to be registered and linked to verified subscriber information, increasingly through integration with the National Identity Number (NIN) system. In Nigeria, the telecommunications sector is primarily overseen by the Nigerian Communications Commission (NCC), which holds the authority to establish secondary

202 Sadhya, & Sahu,, 2024.
203 Sadhya, & Sahu,, 2024.
204 Chesterman, 2011, p252.
205 National Identity Management Commission (NIMC), Nigerian Communications Commission (NCC), Central Bank of Nigeria (CBN) and Financial Institutions - Bank Verification Number (BVN), The Nigerian Immigration Service (NIS) among others.
206 Sesan and Roberts, 2025, p27.
207 Mohanty, 2025.
208 Sesan and Roberts, 2025, p27.
209 Sesan and Roberts, 2025, p27.
210 Sesan and Roberts, 2025, p27.
211 European Union's General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1; the United Nations' Declaration of Human Rights United Nations General Assembly. (1948), art 12; United Nations General Assembly. (1966, December 16). *International Covenant on Civil and Political Rights*, vol. 999, 171. https://www.refworld.org/docid/3ae6b3aa0.html; African Union. (2014, June 27). *African Union Convention on Cyber Security and Personal Data Protection* (EX.CL/846(XXV)). Adopted at the 23rd Ordinary Session of the Assembly, Malabo, Equatorial Guinea. African Union. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf
212 Federal Republic of Nigeria. (2003). *Official Gazette No. 62 Lagos - 19th August, 2003 Vol. 90 Government Notice No. 115.* https://ncc.gov.ng/sites/default/files/2024-12/Legislation-Nigerian_Communications_Act_2003.pdf
213 Nigerian Communications Commission. (2011). *Registration of Telephone Subscribers Regulations 2011.* Federal Republic of Nigeria Official Gazette No.101 Vol. 98.

legislation for sector regulation.[214] The Registration of Telephone Subscribers Regulations 2011,[215] Regulation 4 mandates the NCC to establish and manage a database referred to as "the Central Database," which houses all information on registered subscribers.

Under Regulation 8 of the 2011 Registration of Telephone Subscribers Regulations, security agencies can access subscriber information in the database. To do so, a formal written request must be submitted to the NCC by an official from the requesting agency that holds at least the rank of Assistant Commissioner of Police or an equivalent position in other security organisations. The centralised identity-linked data and the fact that it is accessible to security agents, lowers the legal threshold for surveillance, enabling profiling, tracking and retrospective monitoring without interception safeguards.

This Regulation achieves its narrow goals, which include identity validation and national security surveillance. However, when assessed in light of international standards on data protection and state surveillance, it falls short in some areas relating to data subject rights, proportionality, transparency, retention policies, and ethical governance.
The Regulation contains some safeguards, for instance, it provides that subscriber information must not be disclosed to a licensee, security agency, or any other entity if such disclosure would violate the Constitution or any other law.[216] Additionally, mobile phone users are required to consent to the collection and registration of their fingerprints and facial biometric data, which are subsequently stored in the central database.[217] The central databases connected to SIM card registration may facilitate mass communication surveillance. There are serious vulnerabilities where people could be randomly monitored without due process.[218]

A key issue is whether there are adequate safeguards in the Regulation to ensure protection of subscriber information in the database and to prevent overreach by the state. Firstly, the database is owned by the state and managed by the NCC which is a government body.[219] There is no provision for independent oversight in respect of how the database is managed or used and no provisions for the applicability of the principles of necessity and proportionality. Under international instruments, to justifiably restrict an individual's right to privacy, the following must be considered:

- Is the restriction necessary to achieve a legitimate aim?[220]
- Is the restriction proportionate to the aim sought to be achieved?[221]
- Whether the restriction is authorised by law and whether these laws are made publicly available and established with sufficient precision to enable a person to guide his or her conduct suitably.[222]
- Any legislation that permits monitoring must also have clear and practical procedural remedies for anyone whose rights may have been violated.[223]
- The existence of effective procedural safeguards such as institutions of oversight with sufficient mandate to implement these legal standards relating to data processing for national security purposes.

The participation of both the executive and legislative branches of government, as well as that of an independent civilian oversight body, is vital to guarantee the effective preservation of the law.[224] In

214 Nigerian Communications Commission Act 2003, ss 3(1), 70

215 Nigerian Communications Commission. (2011). *Registration of telephone subscribers regulations 2011*

216 Registration of Telephone Subscribers Regulations 2011, reg. 10 (2).

217 Registration of Telephone Subscribers Regulations 2011reg. 11.

218 Registration of Telephone Subscribers Regulations 2011reg. 11.

219 Registration of Telephone Subscribers Regulations 2011, reg 5 (2).

220 ECHR, art. 8; African Commission on Human and Peoples' Rights. (2019). Declaration of Principles on Freedom of Expression and Access to Information in Africa, art. 41(1). https://achpr.au.int/en/node/902

221 International Principles on the Application of Human Rights to Communications Surveillance; the United Nations Draft Legal Instrument on Government-led Surveillance and Privacy, art 3(4).

222 International Principles on the Application of Human Rights to Communications Surveillance; the United Nations Draft Legal Instrument on Government-led Surveillance and Privacy, art 3(4).

223 The United Nations Draft Legal Instrument on Government-led Surveillance and Privacy, art.3(11).

224 The Declaration of Principles on Freedom of Expression and Access to Information in

the absence of oversight of databases in Nigeria, the state and its agents, can access subscriber data without judicial oversight. To safeguard the right to privacy, international law requires states to conduct a Data Protection Impact Assessment (DPIA) before implementing any surveillance system.[225] There is no information on whether a DPIA was done before this database was established.

The Regulation falls short of enforcing data subjects' rights in several ways, there are no provisions for informed consent, right to erasure or objection. Some rights are narrowly framed.[226] The NDPA 2023 provides for the right to object to processing, correction and erasure in Section 34. The regulation does not allow subscribers to request that their data be deleted. This can be compared with Article 17 GDPR, which provides the right to be forgotten: the right to delete data without undue delay under certain conditions. This policy ensures data confidentiality and data security.[227] This policy will not only ensure that irrelevant data are deleted within stated periods; it will reduce the risks of data accumulation, privacy breaches and unauthorised disclosures.[228]
In terms of access to the database, it is submitted that 'a formal written request submitted to the NCC by an official of the requesting agency holding a rank no lower than Assistant Commissioner of Police or an equivalent position in other security agencies' may not be sufficient to prevent unnecessary access to sensitive data. The Regulation does not contain provisions on pseudonymisation and anonymisation, which are essential ethical considerations for database management.[229] Pseudonymisation involve replacing direct identifiers (such as names and addresses) with pseudonyms, which could help to reduce the risk of identifying individuals while anonymization could involve stripping the data of all identifying information, making it impossible to link the data back to any individual.[230] Without these techniques in the database, any access poses a risk of data misuse.

Apart from these shortcomings of the Regulation, there are other issues with the mandatory SIM registration policy. Nigeria's mandatory linkage of SIM cards to national digital IDs was introduced as a measure to combat the country's alarming rise in kidnappings. However, it may be argued that this policy has yet to achieve its intended outcomes.[231] This failure is not as a result of the policy itself but to its flawed implementation and enforcement.[232]

The National Identity Management Commission (NIMC) faces several challenges such as bribery, corruption and bureaucratic inefficiencies which have affected its ability to effectively manage the registration.[233] These inefficiencies also affect SIM card registration and NIN linkage in Nigeria. Due to access barrier, many persons in mostly in rural areas, find it difficult to obtain a NIN, as a result many are left without any form of national identity.[234] There are cases of fraudulent registration, third-party SIM use and weak data verification which technically increase security risks.[235] There are also difficulties in modifying information; in fact, media reports indicate that many agents deliberately refuse to correct

Africa 2019, art 41(3); International Principles on the Application of Human Rights to Communications Surveillance; United Nations Human Rights Office of the High Commissioner 'The Right to Privacy in the Digital Age' para. 37.

225 The United Nations Draft Legal Instrument on Government-led Surveillance and Privacy, art 5(1) (a).

226 Registration of Telephone Subscribers Regulations 2011, reg 9 (1).

227 Pina, E., et al. (2024). Data privacy and ethical considerations in database management. *Journal of Cybersecurity and Privacy, 4*(3), 497.

228 Pina, 2024, p497.

229 Pina, 2024, p501.

230 Pina, 2024, p501; Vovk, O., et al. (2023). Methods and tools for healthcare data anonymization: A literature review. *International Journal of General Systems, 52*, 326–342.

231 Burt, C. (2024, January 19). Nigeria struggles to utilize biometric SIM registration to ID criminals: Mozambique begins pilot with similar goals. *Biometric Update.com.* https://www.biometricupdate.com/202401/nigeria-struggles-to-utilize-biometric-sim-registration-to-id-criminals

232 Burt, 2024.

233 Orji, M. U., & Ekemezie, N. C. (2024). Evaluating the operational effectiveness of the Nigerian National Identity Management Commission (NIMC). *Academic Journal of Academic Research in Business and Social Science, 14*(6), 147.

234 Inclusion for All. *Link between poverty and NIN ownership.* https://inclusion-for-all.org/wp-content/uploads/2024/02/02Poverty-SnapshotV2.pdf

235 Luhanga, et al. (2023) p1.

errors.[236] This coupled with the vulnerabilities in the identification system raise concerns about data integrity. A fact that has earned it the position of the second most vulnerable in Africa.[237]

Based on the New Social Contract theory, Nigeria's SIM registration regime does reflect an asymmetric exchange where citizens are forced to surrender personal and biometric data in the name of security, and the state, on the other hand, offers few reciprocal guarantees of transparency, proportionality or accountability. This questions the legitimacy of the security–privacy bargain underpinning the system.

5. Legal Framework for SIM Registration in India

Like Nigeria, India justifies SIM registration on the basis of national security threats such as cross-border terrorism and internal insurgency and the need to stop unauthorised use of the nation's telecom systems.[238] The legal framework in India is shaped by distinct judicial interventions. India's Supreme Court decided in the case of *Justice K. S. Puttaswamy (Retd.) v. Union of India*[239] that the Constitution guarantees the right to privacy under Article 21. The Court held that to satisfy the test of proportionality, any limitation of fundamental rights must: it must be for a proper purpose, the limitation must be connected to the fulfillment of the purpose, there are no less intrusive measures and the importance of achieving the aim and limiting the right must be directly related.[240] The Court then held that the decision to link Aadhaar SIM cards to national identity was neither valid nor constitutional.'[241] The court recognised the great danger linking SIM cards with biometric data has on personal autonomy and held that the practice must be invalidated, it ordered all such data to be deleted and should not be used for purpose whatsoever.[242]

The legal framework governing SIM registration in India is governed by the Telecommunications Act (2023).[243] This law operates through the Know Your Customer (KYC) mandates issued by the Department of Telecommunications (DoT) which links telephone identity and biometric information. Section 3(7) of the Telecommunications Act provides that telecommunications operators may be required to identify their customers through the use of any verifiable biometric based identification. The Act also contains penalties for fraudulent acquisition of SIM cards.[244] Users are also obligated to provide accurate information at the point of registering their SIM and are not to suppress material information or impersonate anyone.[245] Section 20 of the Act provides that in cases of public emergencies and in the interest of public safety, the government can intercept or detain messages but must record the reasons in writing.[246] It is also provided in the Section that the interception and detention of the message will only occur if it is considered necessary or appropriate by the state to protect India's sovereignty and integrity, ensure national defence and security, maintain friendly relations with other countries, preserve public order in India, or prevent the encouragement of criminal activity.[247] These powers cannot be exercised indefinitely; the Act provides that it shall be for such duration as prescribed.[248]

There are some gaps in the Section in terms of compliance with the international best practices and standards on government surveillance. For instance, there is no provision for parliamentary oversight. It is nowhere stated that interception and suspension orders should be subject to parliament, making democratic check over such powers impossible. There is also no provision for judicial or independent oversight. There is no definition of 'public emergency' and 'public safety' in the Act; this leaves room for subjective interpretations that may lead to abuse of power. Another issue identified in India is that once the SIM is active, there is no way to determine if the person

236 Elebeke, E. (2019, April 17). NCC decry continued fraudulent SIM registrations. *Vanguard News.* https://www.vanguardngr.com/2019/04/ncc-decry-continued-fraudulent-sim-registrations/

237 MacDonald, A. (2024, December 10). Nigerian NIN holders struggle with modification, vulnerability issues. *Biometric News.* https://www.biometricupdate.com/202412/nigeria-nin-holders-struggle-with-modification-vulnerability-issues

238 Majumdar, 2025, p129.

239 [Writ Petition No. 494/ 2012].

240 [Writ Petition No. 494/ 2012, para 432.

241 [Writ Petition No. 494/ 2012, para 284.

242 [Writ Petition No. 494/ 2012, para 284.

243 *Telecommunications Act, 2023* (India). https://egazette.gov.in/WriteReadData/2023/250880.pdf

244 Telecommunications Act, 2023, s. 42.

245 Telecommunications Act, 2023, s. 29.

246 Telecommunications Act, 2023, s. 20(2).

247 Telecommunications Act 2023, 20(2).

248 Telecommunications Act, 2023, s. 20(4).

who registered it is the one using it.[249] This lack of continuous identity assurance presents a significant gap in the legal system.[250]

The Digital Personal Data Protection (DPDP) Act, 2023 regulates the processing of personal data in India.[251] Indian telecom companies are classified as data fiduciaries with significant obligations regarding data accuracy and security.[252] The Act contains stringent financial penalties up to INR 250 crore (approx. $30 million USD) for data breaches, providing a more robust deterrent against breaches.[253] Section 17 of the Act exempts government agencies from complying with standard rules of data protection such as obtaining consent, giving notice, erasure of data when they process data for national security, public order and foreign relations.[254] The data subject rights of citizens are rendered unenforceable in this context.

India also faces similar challenges as Nigeria with respect to decentralization of data handling and the distributed range of actors. These include Aadhaar/central identities data repository, national and state e-governance platforms (such as the India Stack, BHIM, UMANG) which handle financial, welfare, service-use data tied to Aadhaar,[255] the health and contact-tracing datasets created during the COVID-19 pandemic[256] among others. Concerns have been raised that due to the fact that the Data Protection Board established under Section 18 is not independent, it may find it difficult to enforce the Act against state actors. This Board enforces the Act, but its chairman and members are appointed by the Central government.[257] There is no form of independence, this, coupled with broad exemptions granted to national security agencies have led to warnings that the law could 'turn India into an Orwellian State.'[258]

Like the situation in Nigeria, the Aadhaar of India has also faced criticism of excluding marginalised populations who lack valid digital identity documentation.[259] Most users lack cannot give informed consent due to lack of information in indigenous language during registration.[260] Others, due to several factors such as age, labour or health challenges cannot provide biometric identification and they are left with no alternative.[261] Apart from this, research argues that the Aadhaar has shifted from a tool of identity to a tool of mass identification and surveillance.[262] Those who choose not to participate in this system do not have any other option than to lose access to essential digital and financial services. For instance, since the mobile number is used for OTP authentication for bank accounts and welfare, the suspension of a SIM under Section 20 of the Telecom Act has two consequences, it cuts off communication and a person's access to their own money and food rations.[263]

Applying the New Social Contract theory to India shows that while the nation has a strong judicial check which other countries can learn from, it is lacking with respect to the principle of accountability to the public concerning surveillance. There is no parliamentary oversight or independent oversight which is important safeguards in preventing abuse by the state. Accountability in a sense also means that the state should be responsible for any failure in its system, therefore, where a citizen's fingerprint cannot be identified due to reasons mentioned above, and the citizen is denied access to SIM registration or food, is the state not failing in its primary contract obligation? However, it is conceded that the mandatory SIM registration in India constitutes a moderated security-privacy bargain due to the constitutional and judicial

249 Majumdar, 2025, p132.
250 Majumdar, 2025, p132.
251 *Digital Personal Data Protection Act, 2023*, No. 22 of 2023 (India). https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
252 DPDPA 2023, s. 2(h) (I).
253 DPDPA 2023, s 33(1).
254 DPDPA 2023, s 17(2) (a).
255 Dattani, K. (2020). "Governtrepreneurism" for good governance: The case of Aadhaar and the IndiaStack. *Area*, *52*(4), 741–748.
256 Dar, M., & Wani, S. (2022). COVID-19, personal data protection and privacy in India. *Asian Bioethics Review*, *15*(2), 125–141. doi: 10.1007/s41649-022-00227-0
257 DPPA, 2023, s 27.
258 Tewari, S. (2020, February 10). India's data protection bill, 2019 – The beginning of an Orwellian era. *Penn Carey Law. https://www.law.upenn.edu/live/news/9748-indias-data-protection-bill-2019-the-beginning-of*
259 Panigrahi, S. (2021). Marginalized Aadhaar: How the world's largest digital identification programme led to the exclusion of marginalized communities. *Culture Area Studies E Journal, 7*(28), 4–16. https://ssrn.com/abstract=3971724
260 Panigrahi, 2021, p9.
261 Panigrahi, 2021, p15 and 16.
262 Panigrahi, 2021, p5.
263 Panigrahi, 2021 p4.

oversight as evidenced in the *Justice K.S. Puttaswamy v Union of India case.*

6. Reforming the Security-Privacy Contract

Analysis has revealed that in Nigeria and India, mandatory SIM registration is justified for national security purposes. This is a common objective across the states, but the legal limitations imposed on state power are not as similar. India, for instance, stands out for its judicial enforcement of proportionality, a principle that regulates the security-privacy trade-off. The other states: Nigeria has weaker oversight mechanisms and inadequate safeguards generally.

However, viewed collectively through the New Social Contract theory, these regimes represent an asymmetrical transfer of power to the state. Reforming these regimes toward rights-respecting governance entails:

To ensure that telecommunications operators, security agencies and other actors are accountable, clear limits must be established on their roles, responsibilities and powers. The extent and purpose of collection of data for SIM registration must be clearly established by law. There must be sufficient provisions on the permissible scope of data collection, data retention periods, and penalties for misuse.[264] There may also be need to resolve the issue of fragmented governance of subscriber data, where citizens' data is collected, stored and accessed by telecommunications operators, regulatory authorities, national identity agencies, and security institutions operating under overlapping and sometimes unclear and unlimited mandates. Secondly, providing adequate safeguards and remedies for unauthorised surveillance or data breaches. There must be greater sensitivity to socio-economic issues such as the risks of digital exclusion and marginalisation. There is also need to improve the existing oversight mechanisms across the states. The establishment of independent supervisory bodies, judicial oversight and regular audits of the process are necessary to mitigate the risks involved in the use of personal data by the state.

7. Conclusion

No doubt, mandatory SIM registration in the Nigeria and India offers security benefits with attendant risks. There are however, issues such as inefficient regulatory oversight, privacy concerns, weak data protection frameworks, and bureaucratic inefficiencies which continue to undermine its effectiveness. This raises concerns about digital exclusion, identity fraud, third party registration and the potential for mass surveillance. This study argues that the principles of the New Social Contract Theory can guide SIM card registration regimes in the countries discussed above in ensuring that while governments have the right to impose rules for ensuring national security, they also uphold citizens' rights to privacy and data protection.

References

Aragba-Akpor, S. (2024). Nigeria's SIM card registration: Global trend with broader implications. *Science Nigeria*. Retrieved October 30, 2024, from https://sciencenigeria.com/nigerias-sim-card-registration-global-trend-with-broader-implications/

Chesterman, S. (2011). *One nation under surveillance: A new social contract to defend freedom without sacrificing liberty*. OUP Oxford.

Dar, M., & Wani, S. (2022). COVID-19, personal data protection and privacy in India. *Asian Bioethics Review, 15*, 125.

Dattani, K. (2026). "Governtrepreneurism" for good governance: The case of Aadhaar and the India Stack. *Area*. https://doi.org/10.1111/area.12579

Edmund, E. (2017). Implementing customer-identity management to combat SIM-card fraud: A security framework for emerging market telcos. *International Journal of Computer Applications Technology and Research, 6*(12), 533.

Elebeke, E. (2019, April 17). NCC decry continued fraudulent SIM registrations. *Vanguard News*. Retrieved January 15, 2026, from https://www.vanguardngr.com/2019/04/ncc-decry-continued-fraudulent-sim-registrations/

Jain, A. K., Ross, A., & Nandakumar, K. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1). https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Luhanga, E., et al. (2023). User experiences with third-party SIM cards and ID registration in Kenya and Tanzania. *arXiv:2311.00830 [cs.HC]*. https://doi.org/10.1145/nnnnnnn.nnnnnnn

[264] Federal Ministry of Communications and Digital Economy. (2021). *Revised national identity policy for SIM card registration*. https://nimc.gov.ng/docs/revised_national_digital_identity_policy_on_sim.pdf

MacDonald, A. (2024, December 10). Nigerian NIN holders struggle with modification, vulnerability issues. *Biometric News*. Retrieved February 2, 2025, from https://www.biometricupdate.com/202412/nigeria-nin-holders-struggle-with-modification-vulnerability-issues#:~:text=Those%20affected%20by%20the%20modification,mobile%20app%20for%20NIN%20modification

Majumdar, P. (2025). Implementing Aadhaar-linked biometric re-authentication can prevent terrorist misuse of India's mobile networks. *American Journal of Information Science and Technology, 9*(2), 129.

Mohanty, S. (2025). Data, ethics, and power: Reimagining the social contract in the digital age. *International Journal for Research in Applied Science & Engineering Technology, 13*(X), 1629.

Okonji, E. (2024, February 28). Nigeria: Telcos begin total disconnection of unregistered SIM cards on Wednesday. *ARISENEWS*. Retrieved January 10, 2026, from https://www.arise.tv/nigeria-telcos-begin-total-disconnection-of-unregistered-sim-cards-on-wednesday/

Orji, M. U., & Ekemezie, N. C. (2024). Evaluating the operational effectiveness of the Nigerian National Identity Management Commission (NIMC). *Academic Journal of Academic Research in Business and Social Science, 14*(6), 147.

Panigrahi, S. (2021). Marginalized Aadhaar: How the world's largest digital identification programme led to the exclusion of marginalized communities. *Culture Area Studies E Journal, 7*(28). https://ssrn.com/abstract=3971724

Pina, E., et al. (2024). Data privacy and ethical considerations in database management. *Journal of Cybersecurity and Privacy, 4*(3), 497–501.

Robert, T., & Oloyede, R. (2022, May 5). Why millions of Africans are right to resist mobile SIM card registration. Institute of Development Studies. Retrieved November 2, 2024, from https://www.ids.ac.uk/opinions/why-millions-of-africans-are-rightto-resist-mobile-sim-card-registration/

Salami, A. O., & Oloyede, R. (2024). Digital identity, surveillance, and data protection in Africa. In R. A. Akongburo et al. (Eds.), *African data protection laws* (p. 138). Walter de Gruyter GmBH & Co KG.

Sadhya, D., & Sahu, T. (2024). A critical survey of the security and privacy aspects of the Aadhaar framework. *Computer & Security, 140*. https://doi.org/10.1016/j.cose.2024.103782

Sesan, G., & Roberts, T. (2025). Digital-ID in Africa: Assessing progress and challenges to date. In G. Sesan & T. Roberts (Eds.), *Biometric digital-ID in Africa: Progress and challenges to date – Ten country case studies* (19–27). Institute of Development Studies.

Tewari, S. (2020, February 10). India's data protection bill, 2019 – The beginning of an Orwellian era. Retrieved January 10, 2026, from https://www.law.upenn.edu/live/news/9748-indias-data-protection-bill-2019-the-beginning-of

Tumang, B. (2025). The SIM registration legislation in enhancing mobile security against cyber threats. *International Journal of Multidisciplinary: Applied Business and Education Research.* https://doi.org/10.11594/ijmaber.06.02.17

Vovk, O., et al. (2023). Methods and tools for healthcare data anonymization: A literature review. *International Journal of General Systems, 52*, 326–342.