



DIGITAL RIGHTS AND PRIVACY IN NIGERIA

By Adeboye Adegoke



PARADIGM
INITIATIVE

The Author

Adeboye Adegoke is Senior Program Manager at Paradigm Initiative (PIN). He leads the organisation's Digital Rights Programs in Africa, which include advocating for rights-respecting digital policies in Africa through policy interventions, stakeholder engagements, capacity building, strategic litigations, coalition building, and media campaigns. He also led advocacy for the passage of the Digital Rights and Freedom Bill by Nigeria's parliament.

Adeboye is an alumnus of the African School on Internet Governance. He has written several articles and authored many reports. He is a co-author of the Digital Rights in Africa report by Paradigm Initiative. Adeboye has strong legislative engagement and policy influencing experience, having worked and influenced many legislations and policies in Africa. He is a member of the Freedom Online Advisory Network and sits on Twitter's Truth and Safety Advisory Council.

Published by: The Paradigm Initiative

Release date: July 2020

License: Creative Commons (CC BY-NC-ND 4.0)

CONTENTS

1	Introduction	4
2	Collection of Personal Data by the Nigerian State	6
3	Private Sector Threats to Privacy	7
4	Between Political Participation and Repression	9
5	Review of the Legal and Regulatory Environment	12
6	The Regulations in Practice	16
7	Towards Protecting Digital and Privacy Rights	20
8	Conclusion and Recommendations	22

1 Introduction

This report explores the state of digital rights and data privacy in Nigeria. It outlines how personal data is collected and retained, and how privacy can be breached by both private and state actors; the legal and regulatory framework, and how this functions in practice; and ongoing efforts and recommendations to better protect Nigerians' digital rights and privacy.¹

Over the past two decades, internet use has exploded in Africa's largest economy. At the beginning of 2001, a paltry 200 000 Nigerians used the internet. By 2020, that figure had increased to over 126 million – a factor of almost 630 – with a 61.2 percent penetration of the population.² In 2018, 98 percent of the adult population used some type of mobile phone (56% smartphones) to access the internet, while computers and tablets were used by only 23 percent and 9 percent, respectively.³

This growth has been economically significant as well. In the second quarter of 2019, the information and communication sector's 13.8 percent contribution to nominal GDP surpassed that of oil and gas (8.8%).

The Nigerian government has officially acknowledged the connection between digital rights and human rights. A 2012 United Nations resolution affirmed that the civil, political, economic, and social rights that people enjoy offline must also be protected online. In July 2016, Nigeria joined 52 other countries, including the United States, Germany, France, and the United Kingdom, to co-sponsor an updated reaffirmation of the 2012 resolution.⁵

Nigerians' right to privacy is derived from Chapter 4 of the 1999 Constitution of the Federal Republic of Nigeria, which recognises privacy and free expression as fundamental rights. Section 37 provides that the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected", while Section 39(1) asserts that "every person shall be entitled to freedom of expression, including the freedom to hold opinions and to receive and impart ideas and information without interference".⁶

¹“Digital rights” here refers to human and legal rights as related to digital media and technologies. “Data privacy” is concerned with individuals' control over personal information, freedom from surveillance, and protection from any third-party interception of private communications or unauthorised access to private data.

²Africa Internet Statistics, Africa 2020 Population and Internet Users Statistics, accessed 12 June 2020, <https://internetworldstats.com/stats1.htm>

³Simon Kemp, Digital 2019: Nigeria, slide 18, 31 January 2019, <https://datareportal.com/reports/digital-2019-nigeria?rq=nigeria>

⁴National Bureau of Statistics, Nigerian Gross Domestic Product Report (Q2), p. 43, [https://nigerianstat.gov.ng/elibrary/queries/search\]=Q2%202019](https://nigerianstat.gov.ng/elibrary/queries/search]=Q2%202019)

⁵UN Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet: Resolution Adopted by the Human Rights Council, 18 July 2016, A/HRC/RES/32/13, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

⁶Constitution of the Federal Republic of Nigeria, Act No. 24, 5 May 1999, <https://constitution.lawnigeria.com/2018/03/26/1999-constitution-with-amendments-nigerian-constitution-hub/>

The rights to privacy and freedom of expression are two sides of the same coin. For example, a free and open press is at risk if journalists' phones are under surveillance. At the same time, policymakers face a difficult trade-off between privacy rights and security and commercial concerns.

However, Nigeria's political trends do raise a number of red flags concerning people's vulnerability to data-related abuse by state and private-sector actors.

The rights to privacy and freedom of expression are two sides of the same coin. For example, a free and open press is at risk if journalists' phones are under surveillance.



2 Collection of Personal Data by the Nigerian State

The collection and storage of personal data pervade all spheres of life in Nigeria. This raises important questions about privacy standards in the digital age, starting with the state's handling of personal data.

One of the key objectives of Nigeria's regulatory structure is to assist law enforcement agencies combat fraud and other criminal activity.⁷ Because of this, mobile phone users are required to register their biometric credentials with their telecoms service provider, linking the ownership of SIM cards and phone numbers with their fingerprints and identity details.

In 2014, the Central Bank of Nigeria introduced a biometrically-registered bank verification number into the financial system.⁸ Nigerians have to go through similar processes with the Independent National Electoral Commission to register to vote, the Federal Road Safety Commission to get a driver's license, the Nigeria Immigration Service to get a passport, and many other public and private institutions.

A 2018 report co-authored by Privacy International and Paradigm Initiative was highly critical of Nigeria's lack of protection for privacy rights. It observed that the mandatory registration of SIM cards, the establishment of a central database containing information about mobile phone users, and compulsory data-retention by internet service providers all contravene international human rights standards because they are neither necessary to achieve a legitimate aim nor proportionate to the aim pursued.⁹

In September 2018 – and in the absence of a data protection framework – Nigeria's federal executive council announced the immediate implementation of a “digital identity ecosystem”.¹⁰ Later investigations revealed that the USSD codes people were given to access their personal national identity number lacked appropriate protocols and could be compromised by anyone who had the date of birth and surname of their target. When the ecosystem was found to be porous, the National Identity Management Commission was urged to suspend the implementation,¹¹ but it took a court intervention for them to act.¹² This incident shows just how vulnerable Nigerians can be to data-privacy breaches.

⁷ Frederick Ehiagwina, Managing Insecurity with Biometric Engineering: An Overview of the Nigerian Experience, Conference on Globalization and Contemporary Issues: Opportunities for Sub-Sahara African Transformation & Development, University of Ilorin, Kwara State, Volume 3, 2015, DOI: 10.13140/RG.2.1.4229.6086

⁸ Victor Olabode Munis, CBN Introduces Bank Verification Numbers, 27 June 2014, http://www.trlplaw.com/wp-content/uploads/2015/04/CBN_introduces_bank_verification_numbers-1.pdf

⁹ Paradigm Initiative and Privacy International, Stakeholder Report Universal Periodic Review 31st Session, March 2018, https://privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf

¹⁰ National Identity Management Commission, FEC Approves Implementation of Strategic Roadmap for Digital Identity Ecosystem in Nigeria, 27 Jun 2014, <https://www.nimc.gov.ng/fec-approves-implementation-of-strategic-roadmap-for-digital-identity-ecosystem-in-nigeria/>

¹¹ Peter Oluka, Reasons Paradigm Initiative Wants NIMC to Suspend NIN Enforcement activities, Tech Economy, 9 Jan 2019, <https://techeconomy.ng/2019/01/09/reasons-paradigm-initiative-wants-nimc-to-suspend-nin-enforcement-activities/>

¹² Andersen Tax, Federal High Court Affirms the Data Privacy Rights of Nigerian Citizens, 30 August 2019, <https://andersentax.ng/federal-high-court-affirms-the-data-privacy-rights-of-nigerian-citizens/>

3 Private Sector Threats to Privacy

In addition to the poor standards of data handling by the state, data-related cyber-attacks such as identity theft, fraudulent electronic transactions, and privacy invasions are rampant in Nigeria. Deloitte's 2019 Cybersecurity Outlook reported a high incidence of phishing attacks, malicious software embedded at payment interfaces, and ransomware. Although these attacks did not receive heavy media coverage, billions of naira were lost.¹³

On the dark web – which exists on overlay networks that use the internet but require specific software, configurations, or authorisation to access – stolen private data is up for grabs. As cybersecurity expert and ethical hacker Emmanuel Olaniyi confirmed for this report, the dark web contains the credit card details of many Nigerians who have been hacked. In October 2018, for example, it was discovered that thousands of customers flying Arik Air, one of Nigeria's foremost airlines, may have had their data leaked.¹⁴

The commercial use of private data is also widespread and the data is easy to obtain. A simple search on Nigeria's popular discussion platform Nairaland delivers offers of lists of valid and active private phone numbers that are available for rent or purchase.¹⁵

“

On the dark web – which exists on overlay networks that use the internet but require specific software, configurations, or authorisation to access – stolen private data is up for grabs. As cybersecurity expert and ethical hacker Emmanuel Olaniyi confirmed for this report, the dark web contains the credit card details of many Nigerians who have been hacked.

”

¹³ Tope Aladenusi, Deloitte, Nigeria Cyber Security Outlook 2019, <https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2019.html>

¹⁴ Oladeinde Olawoyin, Massive Data Leak Affecting Arik Air Customers; Company Slow to Respond: Paine, Data Breaches, 31 Oct 2018, <https://www.databreaches.net/massive-data-leak-affecting-arik-air-customers-company-slow-to-respond-paine/>

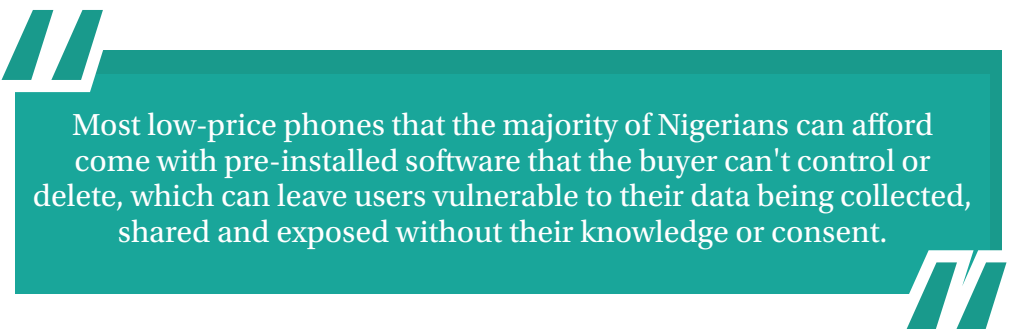
¹⁵ Nairaland Forum, Buy Nigerian Phone Numbers for Your Business, 12 June 2020, <https://www.nairaland.com/3719301/buy-nigerian-phone-numbers-business>

The most common way to secure phone numbers for commercial use is through a bulk SMS platform. These usually offer a database of active phone numbers that can, to put it plainly, be bought and spammed. As one platform boasts, “One of the advantages of bulk SMS service is access to a phone number database of target demographics for your SMS marketing campaigns, advertisements, customer survey, market research and analysis, including academic research and data collection.”¹⁶ That is, you can buy phone numbers for your preferred geographic area, gender, or network service. These blatantly illegal practices have raised few public outcries or enforcement efforts by the relevant government agencies.

Some companies use a financial lure to lead Nigerians into data-privacy breaches. People have voluntarily sold their privacy for \$20 a month by taking up offers from Facebook Research, or its testing services Applause, BetaBound and uTest, to install a VPN that spies on their phone and web activities. According to one tech journalist, “It’s unclear exactly what data Facebook is concerned with, but it gets nearly limitless access to a user’s device once they install the app.”¹⁷

Other vulnerabilities are built into mobile phone technology. The huge demand for smartphones in Nigeria is largely supplied by refurbished secondhand phones. These phones, which may have been imported from the United Kingdom, the United States or China, are often locked to the network provider of the original owner. The common “jailbreaking” processes used to unlock this setting also turn off some security features, which again jeopardises the privacy of data on the phone.

Most low-price phones that the majority of Nigerians can afford come with pre-installed software that the buyer can’t control or delete. In a January 2020 open letter to Google, a global coalition of data-privacy advocates called for action against such pre-installed Android apps, “which can leave users vulnerable to their data being collected, shared and exposed without their knowledge or consent.”¹⁸



Most low-price phones that the majority of Nigerians can afford come with pre-installed software that the buyer can’t control or delete, which can leave users vulnerable to their data being collected, shared and exposed without their knowledge or consent.

¹⁶ Ebulksms.com, Sending Bulk SMS in Nigeria, 10 June 2020, <https://www.ebulksms.com/blog/page/2>

¹⁷ Josh Constine, Facebook Pays Teens to Install VPN that Spies on Them, TechCrunch, 30 January 2019, <https://techcrunch.com/2019/01/29/facebook-project-atlas/>

¹⁸ Privacy International, Open Letter to Google, 8 Jan 2020, <https://privacyinternational.org/advocacy/3320/open-letter-google>

4 Between Political Participation and Repression

Increased access to the internet and social networking platforms has also stimulated socio-political conversations and influenced civic action. The hashtags #OccupyNigeria,¹⁹ #BringBackOurGirls,²⁰ #NotTooYoungToRun²¹ and #CitizensSolutionToEndTerrorism²² signify some of the most notable citizen-driven advocacy campaigns of recent years in Nigeria. Yet the freedom of digital advocacy in Nigeria is on shaky terrain and has been for a while.

The annual Freedom on the Net Report is produced by the US-based thinktank Freedom House. It measures obstacles to internet access, limits to content, and violations of users' rights.²³ Countries are scored on a scale of 0 to 100, with less than 39 considered as “not free”, 40–69 as “partly free” and 70+ as “free”. With marks in the 60s, Nigeria has received a “partly free” status every year since 2011. In 2019, the country scored a 64, with 17 out of 25 points (68%) for obstacles, 26 out of 35 (74%) for limits; and 21 out of 40 (52%) for violations.

There is no publicly available data on the government's takedown requests to telecommunications companies related to moderation and censorship, but there are a few indications. A leaked memo from the Nigerian Communications Commission ordered the blocking of about 21 pro-Biafran websites in 2017. According to the Commission, the websites “threatened national security”.²⁴ Another source of information is Facebook's Transparency Report, which registers government requests to the company for user data. Between July and December 2019, they received 12 requests (11 through “legal process” and one “emergency” request) related to 28 users/accounts from the Nigerian government.²⁵ While there have been no nationwide disruptions of internet service, there have also been claims that signals are jammed in areas where the president visits.

“

There is no publicly available data on the government's takedown requests to telecommunications companies related to moderation and censorship, but there are a few indications.

”

¹⁹ Wikipedia, Occupy Nigeria, last edited 27 May 2020, https://en.wikipedia.org/wiki/Occupy_Nigeria

²⁰ Wikipedia, Chibok Schoolgirls Kidnapping, last edited 8 June 2020, https://en.wikipedia.org/wiki/Chibok_schoolgirls_kidnapping

²¹ Wikipedia, Not Too Young to Run, last edited 21 April 2020, https://en.wikipedia.org/wiki/Not_Too_Young_To_Run

²² Cordelia Hebblethwaite, Lessons from Nigeria on Social Media Activism, BBC, 15 April 2014, <https://www.bbc.com/news/blogs-trending-27026755>

²³ Freedom House, Freedom on the Net, accessed 10 June 2020, <https://freedomhouse.org/report/freedom-net>

²⁴ Sunday Tribune, FG Begins Clamp Down on Online Newspapers, Others, 6 November 2017, <https://thecitizenng.com/fq-begins-clamp-down-on-online-newspapers-others/>

²⁵ Facebook Transparency Report, Nigeria, Jul–Dec 2019, <https://transparency.facebook.com/government-data-requests/country/NG/jul-dec-2019>

The Internal Security and Enforcement Law, for example, was enacted as an anti-kidnapping measure in Akwa Ibom State in 2009, but it has since been used to suppress government critics. Section 6(1), which talks vaguely about “public disturbance”, has been used to jail government critics.

While Nigerians are largely able to express themselves and share information on the internet, an Amnesty International report on freedom of expression noted that 50 journalists and bloggers had been arrested in the five years since the introduction of the 2015 Cybercrime Act, and profiled several cases of those who suffered intimidation, arrest and even torture.²⁶ Cases like these create a climate of fear and self-censorship. A 2018 poll conducted by Paradigm Initiative found that about 40 percent of respondents did not feel free to express themselves online.²⁷

In addition to journalists and bloggers, opposition politicians, civil society activists, protesters and critics are all vulnerable to privacy breaches by those in power. Nigeria's state and federal governments have a history of questionable applications of the law to act against dissent groups in the guise of national security.

For example, the Internal Security and Enforcement Law was enacted as an anti-kidnapping measure in Akwa Ibom State in 2009, but it has since been used to suppress government critics. Section 6(1), which talks vaguely about “public disturbance”, has been used to jail government critics. In 2014, a newspaper editor was secretly abducted and then charged under this law for publishing stories critical of the then state governor, Godswill Akpabio.²⁸ In another incident in November 2019, a bank official was illegally detained for publishing “annoying” Facebook posts against the current governor, Udom Gabriel Emmanuel.²⁹ In Abia State, police arrested Obinna D. Norman, the founder and editor of the online Realm News in March 2019. Accused of defaming and harassing a state senator, he was charged with cyber-stalking under state anti-terrorism and kidnapping laws and the federal Cybercrime Act.³⁰

The government has also made legal and illegal use of surveillance technology. As far back as 2013, Lanre Ajayi, the president of the Association of Telecommunications Companies of Nigeria, claimed that the Nigerian government, in collaboration with the security agencies and telecoms providers, had been secretly invading citizens' privacy. According

²⁶ Amnesty International, *Endangered Voices: Attack on Freedom of Expression in Nigeria*, p 6,

<https://www.amnesty.org/download/Documents/AFR4495042019ENGLISH.PDF>

²⁷ Paradigm Initiative & OONI, *Status of Internet Freedom in Nigeria*, 2018 <https://ooni.torproject.org/documents/nigeria-report.pdf>

²⁸ Daily Trust, *Akwa Ibom Secretly Arraigns Abducted Editor for Publishing Story Critical of Gov Akpabio*, 6 Jul 2014,

<https://www.dailytrust.com.ng/akwa-ibom-secretly-arraigns-abducted-editor-for-publishing-story-critical-of-gov-akpabio.html>

²⁹ Cletus Ukpogon, *Court Grants Bail to Bank Official Who Published “Annoying” Facebook Posts Against Nigerian Governor*, Premium Times, 19 Dec 2019, <https://www.premiumtimesng.com/regional/south-south-regional/368994-court-grants-bail-to-bank-official-who-published-annoying-facebook-posts-against-nigerian-governor.html>

³⁰ Media Foundation for West Africa, *FOE Situation in West Africa: Assaults, Detentions Blight March 2019*, 9 April 2019,

<https://www.mfwa.org/foe-situation-in-west-africa-assaults-detentions-blight-march-2019/>

³¹ Technology Times, *SSS, MTN Nigeria, Others, Already Spying on Nigerians*, JACITAD Forum Told, 15 May 2013, <https://technologytimes.ng/sss-mtn-nigeria-spying-nigerians/>

to him, the Dutch firm DigiVox listed the Nigerian State Security Service and the four major Nigerian mobile communication firms as customers of their communications-interception technology.³¹

Also in 2013, the Nigerian government secretly, and in contravention of contract procedures, awarded a \$40 million tender to the Israeli firm Elbit Systems for technology that would enable the state to intercept all internet activity and invade users' privacy at will.³² In 2015, a newspaper investigation revealed that the governors of four states in the Niger Delta region were illegally using cutting-edge devices to spy on residents, especially politically active opponents. A follow-up two years later suggested that those operations still continued.³³

According to a 2018 report by the New York-based Committee to Protect Journalists, the Nigerian police unlawfully arraigned journalist Samuel Ogundipe and tried to force him to reveal his source for a published article about the inspector-general of police. The police had a file with Ogundipe's bank statement and call history, which were obtained from his bank and his telecommunication service provider.³⁴

High-ranking government officials have called for legislation to clamp down on social media commentary that is critical of the government,³⁵ and the head of the military has admitted that social media is being monitored by “strategic media centres.”³⁶ Noting that the Nigerian government spent at least 127 billion naira on surveillance and security equipment between 2014 and 2017, the Committee to Protect Journalists reported that the Nigerian military has used digital forensic technologies to extract information from phones and computers to spy on ordinary Nigerians and the press.³⁷

Budgetary allocations for the Office of the National Security Adviser and Department of State Services have included such cryptic items as the “Stravinsky Project” and the “All-Eye” surveillance project.³⁸ The national budget reveals that the government plans to spend five billion naira on surveillance-related technologies in 2020 alone, and the procurement of surveillance technology has become a permanent feature of the annual budget.

“

Budgetary allocations for the Office of the National Security Adviser and Department of State Services have included such cryptic items as the “Stravinsky Project” and the “All Eye” surveillance project. The national budget reveals that the government plans to spend five billion naira on surveillance-related technologies in 2020 alone.

”

³² Ogala Emmanuel, Exclusive: Jonathan Awards \$40 Million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians, Premium Times, 25 April 2013, <https://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-to-israeli-company-to-monitor-computer-internet-communication-by-nigerians.html>

³³ Samuel Ogundipe, Investigation: Two Years After, Niger Delta States Continue Controversial Spying Programmes, Premium Times, 30 June 2017, <https://www.premiumtimesng.com/news/headlines/235396-investigation-two-years-after-niger-delta-states-continue-controversial-spying-programmes.html>

³⁴ Committee to Protect Journalists, Nigerian Journalist Jailed for Refusing to Reveal Source, 16 Aug 2018, <https://cpj.org/2018/08/nigerian-journalist-jailed-for-refusing-to-reveal-phil>

³⁵ Freedom House, Freedom on the Net 2019: Nigeria, n. 40, https://freedomhouse.org/country/nigeria/freedom-net/2019#footnote2_lxr4xi2

³⁶ Punch, Military Monitoring Social Media for Hate Speech – Enenche, 23 Aug 2017, <https://punchng.com/military-monitoring-social-media-for-hate-speech-enenche/>

³⁷ Jonathan Rozen, Nigerian Military Targeted Journalists' Phones, Computers with “Forensic Search” for Sources, Committee to Protect Journalists, 22 Oct 2019, <https://cpj.org/blog/2019/10/nigerian-military-target-journalists-phones-forensic-search.php>

³⁸ The Nation: Presidency Votes N3.6b for BMW Cars in Budget 2016, 30 Dec 2015, <https://www.thenewsnigeria.com.ng/2015/12/office-of-nsa-votes-n9b-for-project-stravinsky-in-2016/>

5 Review of the Legal and Regulatory Environment

As noted above, the 1999 Constitution recognises privacy and freedom of expression as fundamental rights. However, digital privacy rights are yet to receive dedicated attention from policymakers, and the current policy environment can best be described as patchy. The legislation and regulations reviewed in this section have provisions that coincide with digital-rights and data-privacy objectives, but these are incidental to their main focus. There is as yet no act that explicitly addresses the subject of digital rights and data privacy. Nigeria did not have any legal framework for the interception of communications until January 2019, when the Lawful Interception of Communications Regulations was gazetted under the Nigerian Communications Act, 2003.

Most policies that touch on surveillance have been drafted over the years in reaction to national security threats or other issues with grave economic implications. Cybercrime is a good example. In 2012, Nigerian consumers lost an estimated N2.15 trillion (more than US\$13 billion) to cybercrime.³⁹ It was also a huge threat to foreign investment and the country's international image.⁴⁰ Given these mounting pressures, the government eventually felt compelled to act, which resulted in the Cybercrimes (Prohibition, Prevention, etc) Act, 2015.

At the heart of the existing policy framework is the **Nigerian Communications Act, 2003**,⁴¹ which established the Nigerian Communications Commission (NCC) as the regulatory body. The Act vests the NCC with the power to create and provide a regulatory framework for the Nigerian communications industry and other related matters.

Sections 146–149 address “national interest matters”. Section 146(1) mandates licensees to endeavour to prevent the use of their facilities or service to commit any offence under any law in operation in Nigeria. Section 146(2) obliges licensees, “upon written request by the Commission or any other authority, to assist as far as reasonably necessary in preventing an offence ... or otherwise in enforcing the laws of Nigeria, including the ... preservation of national security”, and subsection 3 protects licensees from any liability while carrying out this duty. Under Section 147, the NCC “may determine that a licensee or class of licensee ... implement the capability to allow authorised interception of communications”. In the event of “a public emergency or in the interest of public safety”,

³⁹ Gbenga Sesan, Babatope Soremi & Bankole Oluwafemi, *Economic Cost of Cybercrime in Nigeria*, 2013, https://www.opennetafrika.org/?wpfb_dl=7

⁴⁰ Nigeria Communications Commission, *Effects of Cybercrime of Foreign Direct Investment and National Development*, pp. 93–94, <https://www.ncc.gov.ng/documents/735-nmis-effects-cybercrime-foreign-direct-investment/file>

⁴¹ Federal Republic of Nigeria Official Gazette, *Nigerian Communications Act, 2003*, http://www.uspf.gov.ng/files/Nigerian_Communications_Act_2003.pdf

Section 148 allows the Commission to suspend licenses; take temporary control of services or networks; order the disclosure, interception or prevention of specified communications; or take possession of “network facilities, service, or customer equipment”. The Act uses the terms “national interest” and “national security” fluidly and does not attempt to define them in its interpretation section, thereby leaving them open to abuse.

Since its establishment, the NCC has issued the following regulations relevant to this report:

- The Consumer General Code of Practice, 2007
- The Registration of Telephone Subscribers Regulations, 2011
- The Nigerian Communications (Enforcement Process, etc.) Regulations, 2019
- The Lawful Interception of Communication Regulations, 2019.



The **Consumer General Code of Practice, 2007**⁴² requires “any licensee that collects information on individual Consumers” to “adopt and implement a policy regarding the proper collection, use and protection of information they collect” (Section 36).

It also mandates them to ensure that those with whom they share or exchange this information have adopted similar measures. Section 37(2) of the Code further states that the policy “shall state clearly what information is being collected; the use of such information; possible third party exchange or disclosure of such information; and the choices available to the Consumer regarding collection, use and disclosure of the collected information”.

However, there are no stipulated penalties for contraventions of the consumer codes: the Commission is to be “guided” by a shopping list of considerations for “administrative fines” under the Nigerian Communications (Enforcement Processes etc.) Regulations, 2019. It is not clear how these provisions provide consumers with adequate protection from the real dangers of data breaches.

The **Registration of Telephone Subscribers Regulations, 2011**⁴³ mandates licensees to capture subscriber information and to transmit this information to a central database established and maintained by the Commission. It also enables security agencies to access that database “provided that a prior written request is received by the Commission from an official of the requesting security agency who is not below the rank of an Assistant Commissioner of Police or a coordinate rank in any other Security Agency” (Section 8(1)). Section 10 does open the possibility for the regulator to issue guidelines about releasing personal information to security agencies, but this remains a grey area that can be used to either strengthen or limit privacy rights. The NCC seemingly prefers for this to remain this way. Given the human rights record and disposition to the rule of law in Nigeria, a further limitation of privacy rights is not unlikely.

More recently, the Commission released the **Nigerian Communications (Enforcement Process, etc.) Regulations, 2019**.⁴⁴ Section 8 mandates every licensee to keep records of

The Registration of Telephone Subscribers Regulations, 2011 mandates licensees to capture subscriber information and to transmit this information to a central database established and maintained by the NCC.

⁴²Federal Republic of Nigeria Official Gazette, Consumer Code of Practice Regulations, 2007, <https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/102-consumer-code-of-practice-regulations-1/file>

⁴³Federal Republic of Nigeria Official Gazette, Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011, <https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file>

⁴⁴Federal Republic of Nigeria Official Gazette, Nigerian Communications (Enforcement Process, etc) Regulations, 2019, <https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/840-enforcement-processes-regulations-1/file>

call data in accordance with the Cybercrime Act and the Consumer Code Regulations. Regulation 8 (2)(a,b) directs every licensee to make available “basic” and “non-basic” information that “may be required by any relevant authority pursuant to Section 146 of the Nigerian Communications Act”. The release of basic information requires only a written request from the authority, signed by a police officer at or above the rank of assistant commissioner, or the equivalent in another agency, while non-basic information requires a court order.

The **Lawful Interception of Communication Regulations, 2019**,⁴⁵ which also falls under the ambit of the Nigerian Communications Act, sets out the conditions in which communications in Nigeria may be intercepted, collected and disclosed. The Regulations make it an offence to intercept any communication in Nigeria except by an authorised agency. The Department of State Security and the Office of the National Security Advisor are authorised to intercept communications subject to a court warrant. The authorised agencies are obliged to submit an annual report of all concluded interception cases to the attorney general.

These three sets of regulations collectively set out the legal limitations on privacy rights in Nigeria.

“The Department of State Security and the Office of the National Security Advisor are authorised to intercept communications subject to a court warrant. The authorised agencies are obliged to submit an annual report of all concluded interception cases to the attorney general.”

⁴⁵Federal Republic of Nigeria Official Gazette, Lawful Interception of Communication Regulations, 2019, 23 Jan 2019, <https://www.ncc.gov.ng/accessible/documents/839-lawful-interception-of-communications-regulations-1/file>


6 The Regulations in Practice

The constitutional right to privacy under Section 37 is not absolute. It is limited by Section 45, which provides that nothing in Section 37 “shall invalidate any law that is reasonably justifiable in a democratic society – (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedoms of other persons”.⁴⁶

However, the NCC's regulations for the derogation of digital privacy rights have often been utilised with little regard to “reasonable justification” and without embracing the principles of necessity and proportionality that keep the deviation in check.

The regulations themselves also fall short of the mark of protecting the digital rights of Nigerians. For example, official requests to access the private information of individuals have to be signed by a law enforcement or security agent at or above the police rank of assistant commissioner. This is prone to abuse: authorisation should come with a court warrant issued by a judge. It is for the court – and not a law enforcement or security agency – to determine whether such a request is, firstly, reasonable and justifiable in a constitutional democracy, and, secondly, whether it is made in terms of the interests or purposes set out under Section 45 of the Constitution.

The Lawful Interception of Communication Regulations does call for court warrants, but the NCC has failed to create effective systems of accountability around these processes. For example, the agencies authorised to intercept communications must submit a comprehensive annual report to the attorney general, but this disregards the fact that the Office of the Attorney General is not separated from that of the minister of justice, and that its role has increasingly been defined by the politics of regime preservation as opposed to the rule of law.



Official requests to access the private information of individuals have to be signed by a law enforcement or security agent at or above the police rank of assistant commissioner. This is prone to abuse: authorisation should come with a court warrant issued by a judge.

⁴⁶ Constitution of the Federal Republic of Nigeria, Act No. 24, 5 May 1999, <https://constitution.lawnigeria.com/2018/03/26/1999-constitution-with-amendments-nigerian-constitution-hub/>

“

The Lawful Interception of Communication Regulations does call for court warrants, but the NCC has failed to create effective systems of accountability around these processes... In the Nigerian context, reporting on data interception to the attorney general creates a conflict of interest to the extent that the legal oversight authority does not have the necessary political independence from the sitting government as a potential offender.

”

In the Nigerian context, reporting on data interception to the attorney general creates a conflict of interest to the extent that the legal oversight authority does not have the necessary political independence from the sitting government as a potential offender.

The Cybercrime Act is also prone to abuse and has been used in a plethora of situations to improperly breach digital and data privacy rights. Section 24(1)(a) states that “any person who knowingly or intentionally sends a message or other matter by means of a computer system or network that is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent”⁴⁷ has committed an offence under the Act and shall be liable for punishment.

However, 24(1)(b) makes it an offence to similarly sending messages or other matter “for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another.”⁴⁸ This provision has been used to quash freedom of expression since it was enacted. Its imprecise language makes it easy to target journalists, bloggers and media practitioners with inconvenient views. Many Nigerians have been harassed, intimidated, arbitrarily arrested and detained, and unfairly prosecuted for expressing views perceived to be critical of the government, whether at the federal or state level.

The Act also sets criteria for the law enforcement and security agencies who request and use private data information. For example, section 38, which directs service providers to retain all traffic data and prescribed subscriber information for two years, and to comply with official requests, states that the requested data must only be used for “legitimate purposes”, and with “due regard to the individual's constitutional right to privacy”, and taking “appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement”.

Section 6 of the Act criminalises unauthorised access to computer systems, regardless of

⁴⁷ Cybercrime (Prohibition, Prevention, Etc) Act, 2015, https://cert.gov.ng/ngcert/resources/CyberCrime_Prohibition_Prevention_etc_Act_2015.pdf

⁴⁸ Cybercrime Act, 2015

the motivation. This presents a huge challenge for “ethical hackers” who possess the skills to identify gaps in an organisation's system and who may be privy to sensitive private information that has been dumped on the dark web. It is difficult for them to communicate this to the affected institution or individuals, as the messenger might be accused and arrested. Under this provision, hackers can be fined up to 5 million Naira or sentenced to up to five years of imprisonment. The Act should recognise ethical hacking as a legitimate profession and possibly mandate organisations holding sensitive data to employ their services to discover vulnerabilities.

Several other government institutions have regulations that address privacy within their specific mandate. Many of these regulations also permit derogations from the right to privacy, opening the potential of abuse. While not necessarily problematic, they are in line with the general system of privacy rights in Nigeria: the rights are first acknowledged and then constrained with broadly general language around law enforcement or national security.

The **National Identity Management Commission (NIMC) Act, 2007**,⁴⁹ in Section 26, forbids the disclosure of registered information and restricts access to the data or information contained in the NIMC's database with respect to a registered individual entry. However, access to an individual's information can be permitted, with the authorisation of the Commission, if an application is made by, or with the authority of that individual, or if that individual otherwise consents to the provision of that information.

Information can be given without the individual's consent if it is “in the interest of National Security; necessary for purposes connected with the prevention or detection of crime; or for any other purpose as may be specified by the Commission in a regulation” (26(3)).

The 2016 **Central Bank of Nigeria (CBN) Consumer Protection Framework**⁵⁰ states that a bank customer has the right to confidentiality and that their information “must be protected unauthorised access and disclosure” (3.1). Financial institutions shall not reveal customers information to a third party except with the express permission of the customer. There are, however, exceptions where the bank can make disclosure: “as required by the CBN and other regulatory bodies; where there is a court order; in pursuance of public duty/interest” (2.6.2 (2a)).

Still in the financial sector, the **Credit Reporting Act, 2017**⁵¹ provides that all data

⁴⁹ https://www.nimc.gov.ng/docs/reports/nimc_act.pdf

⁵⁰ [https://www.cbn.gov.ng/Out/2016/CFPD/Consumer%20Protection%20Framework%20\(Final\).pdf](https://www.cbn.gov.ng/Out/2016/CFPD/Consumer%20Protection%20Framework%20(Final).pdf)

subjects shall have the right to privacy, confidentiality, and protection of their credit information, and where such information needs to be shared, it shall be done with the consent of the data subject.

Also, when the subject gives consent, it is only valid for the specific purpose for which it was granted and shall lapse immediately after the purpose is satisfied. However, credit information providers may disclose credit information of the data subject without consent for purposes relating to processing, reviewing, approving and recovery of credits or in compliance with a court order or regulatory requirement.

The Child Rights Act, 2003⁵² addresses the privacy of children. Section 8(1) guarantees the right of every child to “privacy, family life, home, correspondence, telephone conversations and telegraphic communications, except as provided in subsection (3)”, which makes provision for derogation to the extent of parents' or legal guardians' rights to exercise reasonable supervision of their children or wards.

The National Health Act, 2014⁵³ provides a legal framework for the regulation, development, and management of Nigeria's healthcare system. Sections 26–30 make information relating to a healthcare user confidential and set out the conditions for disclosure of such information, the measures required to safeguard information, and the offences related to changing, deleting or copying health records.

Lastly, the **Freedom of Information Act 2011**⁵⁴ was enacted to “make public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and the protection of personal privacy, protect serving public officers from adverse consequences of disclosing certain kinds of official information without authorisation and establish procedures for the achievement of those purposes”. Section 14(1(a)–(e)) of the Act requires every government or public institution to deny applications for any personal information that it retains unless the individual concerned grants consent or the information is already publicly available.

The provision under the Cybercrime Act 24(1)(b) has been used to quash freedom of expression since it was enacted. Its imprecise language makes it easy to target journalists, bloggers and media practitioners with inconvenient views. Many Nigerians have been harassed, intimidated, arbitrarily arrested and detained, and unfairly prosecuted for expressing views perceived to be critical of the government, whether at the federal or state level.

⁵¹ <https://lawyersonline.ng/lfn/lfn/credit-reporting-act-2017/>

⁵² <https://www.lawyard.ng/wp-content/uploads/2016/01/CHILD%E2%80%99S-RIGHT-ACT.pdf>

⁵³ <https://www.publihealth.com.ng/wp-content/uploads/2017/10/The-Official-Gazette-of-the-National-Health-Act.pdf>

⁵⁴ <https://www.cbn.gov.ng/F01/Freedom%20of%20Information%20Act.pdf>

7 Towards Protecting Digital and Privacy Rights

Despite this inadequate record of protecting digital rights, a number of legislative efforts have the potential to strengthen the ecosystem for data privacy and digital rights in Nigeria.

In April 2015, the Net Rights Africa Coalition of civil society organisations, led by the Paradigm Initiative among others, presented a Digital Rights and Freedom Bill to the Nigerian public.⁵⁵ The Bill addressed the broad issue of digital rights, including data privacy, freedoms of online expression, opinion and information, the right to peaceful online assembly and association, and safeguarding human rights regarding surveillance and interception of communication.⁵⁶ In April 2019, after the Bill was passed by both houses of the National Assembly, President Muhammadu Buhari declined to sign it into law. Explaining his refusal, the president suggested that “the scope of the bill should be limited to the protection of human rights within the digital environment to reduce the challenge of duplication and legislative conflict in the future”.

The civil society coalition intensified its advocacy work by redrafting the Bill and presenting it to the legislature. The revised version accommodated the president's concern by unbundling data protection and provisions concerning surveillance, monitoring and interception while focusing on human rights within the digital environment. The revised version passed first reading in the House of Representatives in July 2019 and has been lingering since.⁵⁹

In April 2015, the Net Rights Africa Coalition of civil society organisations, led by the Paradigm Initiative among others, presented a Digital Rights and Freedom Bill to the Nigerian public. The Bill addressed the broad issue of digital rights, including data privacy, freedoms of online expression, opinion and information, the right to peaceful online assembly and association, and safeguarding human rights regarding surveillance and interception of communication.

⁵⁵ Paradigm Initiative Nigeria, Press Release: Presentation of Digital Rights and Freedom Bill, 23 April 2015, <https://paradigmhq.org/pin-and-netrightsnig-coalition-presents-digital-rights-and-freedom-bill/>

⁵⁶ Policy and Legal Advocacy Centre, Digital Rights and Freedom Bill Analysis, 2016, <http://placbillstrack.org/view.php?getid=1801>

⁵⁷ Kemi Busari, Buhari Declines Assent to Digital Rights Bill, Four Others, Premium Times, 20 Mar 2019, <https://www.premiumtimesng.com/news/headlines/321189-buhari-declines-assent-to-digital-rights-bill-four-others.html>

⁵⁸ Solomon Fowowe, Buhari Declines Assent to Digital Rights Bill, Four Others, The Guardian Nigeria, 20 Mar 2019, <https://guardian.ng/news/buhari-declines-assent-to-digital-rights-and-freedom-bill-four-others/>

⁵⁹ Ugo Onwuaso, Digital Rights Bill Passes First Reading at the House of Representatives, Nigeria Communications Week, 27 Jul 2019, <https://nigeriacommunicationsweek.com.ng/digital-rights-bill-passes-first-reading-at-the-house-of-representatives/>

The **Data Protection Bill, 2016**, which was first introduced in the 7th National Assembly (2011–2015), was another important attempt to protect data privacy in Nigeria. However, it failed to pass the required legislative hurdles.

A **Personal Information and Data Protection Bill**⁶⁰ that covered various aspects of personal data protection was prepared by the National Identity Management Commission and sent to the House of Representatives. Another bill on the **Protection of Personal Information** was introduced at the Senate. These similar draft bills were harmonised along with other relevant regulations and reintroduced in the 8th National Assembly (2015–2019).⁶¹ The Data Protection Bill, 2019 was passed and sent to the president for assent, but it has not been signed into law.

In January 2019, the National Information Technology Development Agency (NITDA), the agency statutorily mandated to develop regulations for electronic governance and the monitoring of the use of information technology and electronic data, released the **Nigerian Data Protection Regulation (NDPR)**. Its stated objectives are “to safeguard the rights of natural persons to data privacy; to foster safe conduct for transactions involving the exchange of personal data; to prevent manipulation of personal data; and to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice”(1.1). The regulation, however, has not had any effect apart from the licensing “data protection organisations” to provide training, auditing, consulting, and compliance services to data controllers.⁶³

Although the regulation came into effect in January 2019, it is yet to be published in the Official Gazette of the Federal Republic of Nigeria, and NITDA has had to respond to questions about whether it is legally empowered to make such regulations.⁶⁴ Even if it passes all these hurdles, the regulation is still only a secondary legislation and does not address the need for Nigeria to enact a data protection law that establishes an independent data protection authority, ensuring data protection from a human rights' perspective.

“

In April 2019, after the Digital Rights and Freedom Bill was passed by both houses of the National Assembly, President Muhammadu Buhari declined to sign it into law. Explaining his refusal, the president suggested that “the scope of the bill should be limited to the protection of human rights within the digital environment to reduce the challenge of duplication and legislative conflict in the future.

”

⁶⁰ National Identity Management Commission, Personal Information and Data Protection Bill, https://www.nimc.gov.ng/docs/reports/personal_info_bill.pdf

⁶¹ Adebayo Adegoke: Where is Nigeria's Data Protection Law?, LiveTimes, 26 September 2019, <https://livelimesng.com/where-is-nigerias-data-protection-law-by-adebayo-adeoke/>

⁶² National Information Technology Development Agency: Nigeria Data Protection Regulation, 2019, <https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf>

⁶³ Na'ankwat Dariem, NITDA Grants Licences to 11 Data Protection Organisations, Voice of Nigeria, 20 Oct 2019, <https://www.von.gov.ng/nitda-grants-licences-to-11-data-protection-organisations-2/>

⁶⁴ ITEdgeNews, Nigeria Data Protection Regulation Not in Conflict with NCC's Role, Says NITDA, 22 October 2019, <https://itedgenews.ng/2019/10/22/nigeria-data-protection-regulation-not-in-conflict-with-nccs-role-says-nitda/>

8 Conclusion and Recommendations

This report explored the state of digital rights in Nigeria with a primary focus on the right to digital privacy. It exposed vulnerabilities to privacy breaches and a generally weak regulatory framework for the protection of data privacy and digital rights.

The right to privacy is central to the protection of human dignity; it also supports and reinforces other rights, such as the freedom of expression, information, and association. To freely form and impart their political, religious or ethical beliefs, people need a private personal space free from interference by the state, the private sector or other citizens in the forms of physical or online surveillance, monitoring of communications or activities, or intrusion into private, family or home affairs.

Surveillance without judicial and democratic oversight must be reined in and illegal arrests and prosecutions for online activities must stop. The right to privacy and freedom of expression as guaranteed for every Nigerian by the Constitution must be preserved. Law enforcement agencies must respect the rule of law in the discharge of their duties. Those with dissenting voices must not be silenced.

According to the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, adopted by the African Commission on Human and Peoples' Rights, states should ensure that safeguards are provided for the right to privacy for any law that authorises targeted communication surveillance, "including:

- a. the prior authorisation of an independent and impartial judicial authority;
- b. due process safeguards;
- c. specific limitation on the time, manner, place and scope of the surveillance;
- d. notification of the decision authorising surveillance within a reasonable time of the conclusion of such surveillance;
- e. proactive transparency on the nature and scope of its use; and
- f. effective monitoring and regular review by an independent oversight mechanism.”⁶⁵

Surveillance without judicial and democratic oversight must be reined in and illegal arrests and prosecutions for online activities must stop.

⁶⁵ African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, <https://www.achpr.org/legalinstruments/detail?id=69>

“

According to the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, adopted by the African Commission on Human and Peoples' Rights, states should ensure that safeguards are provided for the right to privacy for any law that authorises targeted communication surveillance.

”

In order to establish an effective regulatory framework that can protect the digital rights of Nigerians and create a system of accountability to ensure, among other things, that every organisation (private or public) that collects citizens' private information is accountable for how the information is retained and used, the following recommendations are made:

- The Digital Rights and Freedom Bill should be passed and signed into law;
- The Cybercrime Act 2015 should be repealed and re-enacted after a review of the sections that have been abused to stifle the rights of Nigerian citizens;
- The NCC regulations should be reviewed to enforce judicial oversight and to accommodate a mandatory annual report that will be publicly accessible;
- The Nigerian Data Protection Regulation (NDPR) should be officially gazetted and put to work to improve the data protection practices of companies and institutions and to protect the rights of Nigerian citizens. The NDPR's prescribed penalties for violations must be applied as a deterrence;
- Given the poor public awareness of data privacy, public education about the privacy implications of applications and the internet must be intensified, so as to build a community of self-aware citizens who understand their digital rights and can demand them from companies, institutions and the government;
- Most importantly, Nigeria's data protection law should authorise an independent data-protection institution that will balance the state's need to gather and keep information about individuals with the rights of those individuals to be protected from unwarranted invasion of their privacy through the collection, maintenance, use, and disclosure of personal information.



The Digital Rights and Freedom Bill should be passed and signed into law.



The Cybercrime Act 2015 should be repealed and re-enacted after a review of the sections that have been abused to stifle the rights of Nigerian citizens.



The NCC regulations should be reviewed to enforce judicial oversight and to accommodate a mandatory annual report that will be publicly accessible.



The Nigerian Data Protection Regulation (NDPR) should be officially gazetted and put to work to improve the data protection practices of companies and institutions and to protect the rights of Nigerian citizens.



Public education about the privacy implications of applications and the internet must be intensified, so as to build a community of self-aware citizens who understand their digital rights and can demand them from companies, institutions and the government.



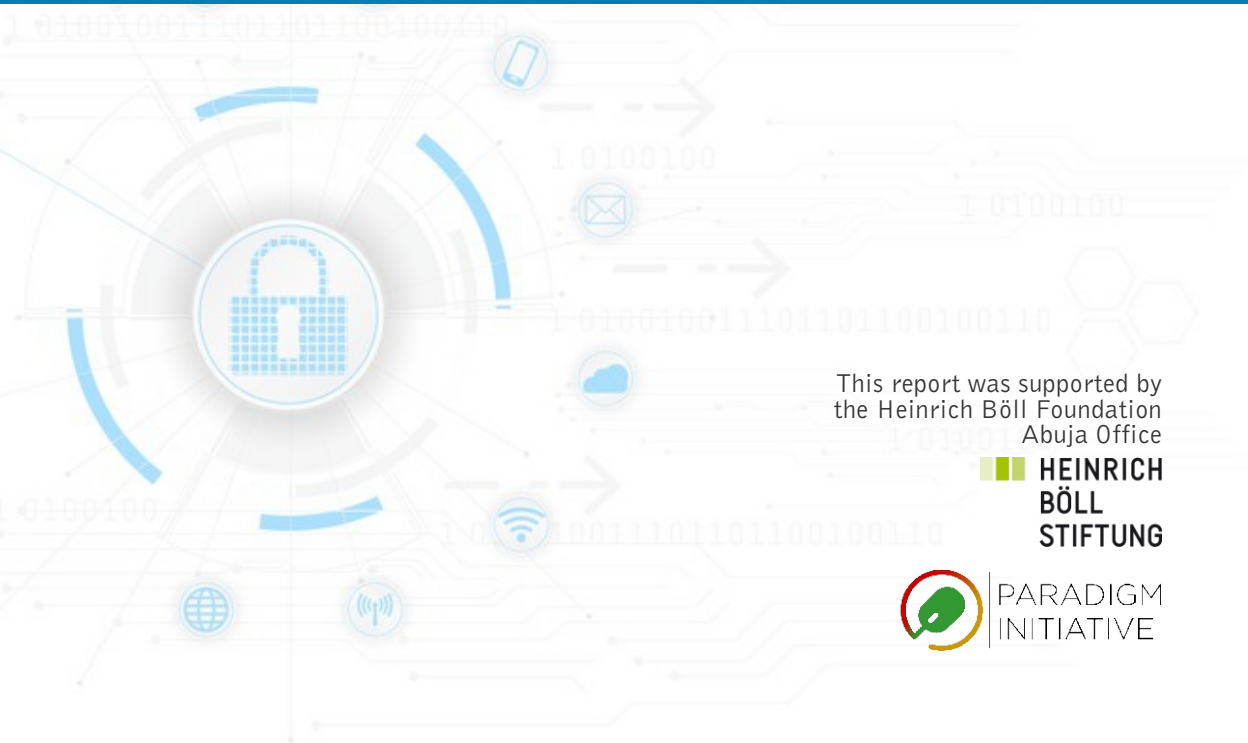
Nigeria's data protection law should authorise an independent data-protection institution that will balance the state's need to gather and keep information about individuals with the rights of those individuals to be protected from unwarranted invasion of their privacy through the collection, maintenance, use, and disclosure of personal information.

NOTES

[illegible]

NOTES

[illegible]



This report was supported by
the Heinrich Böll Foundation
Abuja Office

 **HEINRICH
BÖLL
STIFTUNG**

 **PARADIGM
INITIATIVE**