accountabilitylab NIGERIA

Towards the Implementation of Data Protection Measures to Safeguard Against Surveillance Abuse in Nigeria

POLICYBRIEF

2024

SPACES FOR CHANGE | S4C

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

Luminate

Policy Brief

Towards the Implementation of Data Protection Measures to Safeguard Against Surveillance Abuse in Nigeria

By
Jake Okechukwu Effoduh
(Assistant Professor, Lincoln Alexander School of Law)

January 2024

Edited by:
Odeh Friday Odeh
(Country Director, Accountability Lab Nigeria)

Design by:
Ifeayolu N. Hyacinth, Stears Consul LTD.

This policy brief considers how implementing data protection laws in Nigeria can safeguard against surveillance abuse in Nigeria. It establishes evidence of the use of mass surveillance tools in Nigeria by providing a breakdown of the surveillance expenditures of some key security institutions in the last decade. This is followed by a discussion on the legality of surveillance in Nigeria and otherwise, and then some propositions on how Nigeria's Data Protection regime may be used to protect against surveillance abuse and safeguard the rights of Nigerian citizens.

Towards the Implementation of Data Protection Measures to Safeguard Against Surveillance Abuse in Nigeria

01

Background

The enactment of the Nigeria Data Protection Act 2023 (the "NDPA")[1] marked Nigeria's entry into the realm of data protection-conscious countries. The law, expected to be as effective as the European General Data Protection Regulations (GDPR),[2] introduced a fully-fledged data protection regime in the country. While it may be too early to call, it is not difficult to see that the NDPA faces an uphill task: enforcing data protection in a country with a surveillance/privacy infraction problem.

Indeed, surveillance,[3] enabled by growing digitalization, is a global challenge. On the one hand, private citizens must stave off surveillance from non-state entities (individuals, corporations, and other individuals) keen to gather individuals' data for various broad intentions. On the other hand, citizens must grapple with the expanding scope of government monitoring. Nigeria is ranked the 8th most terrorized country in the world on the Global Terrorism Index (GTI) 2023, an index that assesses the impact of terrorism in 163 countries.[4] In response, several key security agencies whose functions include intelligence gathering and internal security have increasingly spent significant monies acquiring advanced surveillance capabilities. These surveillance tools range from spyware, CCTV cameras, data warehousing, and interception systems, to name a few.

While it is usually possible to detect where surveillance by non-state actors is unlawful, the same cannot be said where the surveillance is from the government. This is because surveillance by the government is often justified by the principle of necessity. Thus, like most governments, Nigeria citesintelligence gathering and crime prevention as the basis for mass surveillance. In that way, various laws in Nigeria grant certain agencies of the government limited powers to carry out lawful surveillance and surveillance that may violate laws, but for which no repercussions will accrue.[5] Surveillance necessarily raises privacy and data protection issues since it can interfere with an individual's right to privacy.[6] Thus, it goes without saying that the deliberate implementation of data protection measures enshrined in Nigeria's data protection laws will, if not eliminate, reduce the spate of mass surveillance in the country. Alternatively, it could ensure that where lawful surveillance is carried out, the rights of citizens are protected and guaranteed.

Like most African countries, Nigeria has remarkably sustained a reputation for being at the

1 The NDPA was enacted to provide a comprehensive framework for protecting personal information and to establish the Nigeria Data Protection Commission for regulating and processing personal information. The NDPA was signed into law by Nigerian President Bola Ahmed Tinubu on June 12, 2023.

2 The GDPR was put into effect on May 25, 2018, and it addresses the transfer of personal data even outside the European Union (EU) and the European Economic Areas (EEA).

3 Surveillance, as used here, refers to the monitoring of individuals' digital and physical actions and communications by an entity, lawfully, but many times, unlawfully. These could take several forms which may include physical observation, electronic monitoring, video recording, data collection and analysis. Electronic surveillance, also known as wiretapping, refers to the surveillance of email, fax, social media, and the internet of a target.

4 Funmilayo Babatunde, 'Why Nigeria is listed among 10 countries mostly impacted by terrorism' (Dataphyte, 18 July 2023) https://www.dataphyte.com/latest-reports/why-nigeria-is-listed-among-10-countries-mostly-impacted-by-terrorism/

5 Some of these laws include the Cybercrimes Act, the National Information Technology Development Agency (NITDA) Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries and Conditions for Operating in Nigeria, the Nigerian Communications Commission's Lawful Interception Regulations, amongst others. (This will be more extensively discussed under the heading, 'When is Surveillance (Il)Legal?'.

6 The right to privacy, simply put, is the right of a person to be left alone, to be free from unwarranted publicity and to live without unwarranted interference.(Stimmel, Stimmel & Roeser, ;The Legal Right to Privacy' Accessible here: https://www.stimmel-law.com/en/articles/legal-right-privacy).

Nigeria’s Increasing Records of State Surveillance

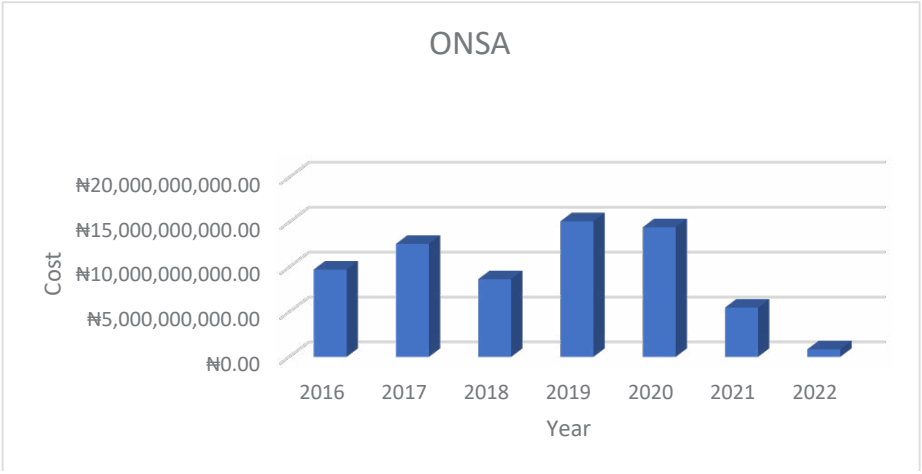
02

Key findings

From 2014 to 2023, the Office of the National Security Adviser (ONSA), the State Security Service (SSS), the National Intelligence Agency (NIA), and the Defense Intelligence Agency (DIA) cumulatively spent N73,736,607,928 on the following surveillance-related equipment, amongst other security-related capital expenditures. All four agencies are set up via the National Security Agencies Act 1986. This Act sets up the DIA, NIA, and SSS with distinct responsibilities while establishing the ONSA as the coordinator of the intelligence activities of these agencies. This position is reaffirmed by Section 2 of the Terrorism (Prevention) (Amendment) Act 2013.

A. ONSA

i. Develop All Eye Project (2016) – N8,721,364,000
ii. Construct Stravinsky Project (2016) – N1,004,200,000
iii. Security Equipment Systems (Stravisky Project) (2017) – N5,470,995,994
iv. Stravisky Project 2 (2017) – N7,121,364,000
v. Stravisky Project 2 (2018) – N4,000,000,000
vi. All Eye Project (Counter Terrorism Centre) (2018) N4,650,000,000
vii. Stranvinsky Project 2 (2019) – N4,000,000,000
viii. Counter Terrorism Centre (All Eyes Project) (2019) – N11,109,000,000
ix. Falcon Eye Project (2020) – N10,000,000,000
x. Stranvisky Project 2 (2020) – N1,429,229,600
xi. Counter Terrorism Centre (All Eye Project) (2020) – N3,009,000,000
xii. Counter Terrorism Centre (All Eye Project) (2021) – N5,489,20Aance system, implementation at Department of State Services (2022) – N850,000,000
TOTAL – N58,204, 362,598



B. SSS

i. Polaris Mass Location and Wireless Tracking System (2014) – N425,600,000
ii. Acquisition of Data Retention System (2014) – N415,000,000
iii. Acquisition of Data Retention System (2015) – N330,867,783
iv. Procurement of GSM Passive Off-the-Air Interception System (2014) – N359,000,500
v. Procurement of surveillance equipment for the service's commands across the nation (2016) – N1,000,000,000
vi. Create Intel Profiling Equipment (2016) – N1,004,200,000
vii. Purchase of Digital Audio Jammer (2017) – N22,000,000
viii. Upgrade and expansion of DSS CCTV Surveillance Project (Phase 1) (2017) – N850,400,000
ix. Purchase of Finfisher Equipment (2017) – N70,400,000
x. Social Media Mining Suite (2018) – N1,013,456,360
xi. Surveillance Drone with Precision Camera with $1MSI Payload capabilities (2018) – N1,006,200,000
xii. Mobile Surveillance Facilities (2018) – N239,855,000
xiii. Social Media Mining Suite (2019) – N990,689,907
xiv. Surveillance Drone with Precision Camera $MSI Payload Capabilities (2019) – N199,786,908
xv. Procurement of Extract-Transform Load (ETL) Technology (2019) – N229,809,879
xvi. Surveillance Drone with Precision Camera with $1MSI Payload capabilities (2020) – N199,786,908
xvii. Procurement of Extract-Transform Load (ETL) Technology (2020) – N229,809,879
xviii. Procurement of Extract-Transform Load (ETL) Technology (2021) – N129,941,287
xix. Expansion of Lawful Interception Centres to high-threat zones including annual maintenance charge (2021) – N140,846,896
xx. Procurement of surveillance equipment (MG-EYES) (2021) – N139,437,846
xxi. Expansion of lawful interception centres to high-threat zones, including annual maintenance charges (2022) – N150,000,000
xxii. Procurement of surveillance equipment (MG-EYES) (2022) – N308,935,000
xxiii. Installation of integrated crisis management surveillance system and implementation (2022) – N300,250,000
xxiv. Expansion of lawful interception centres to high-threat zones, including annual maintenance charge (2023) – N492,445,863
xxv. Procurement of surveillance equipment (MG-EYES) (2023) – N153,113,314
xxvi. Installation of integrated crisis management surveillance system (2023) -N1,000,000,000

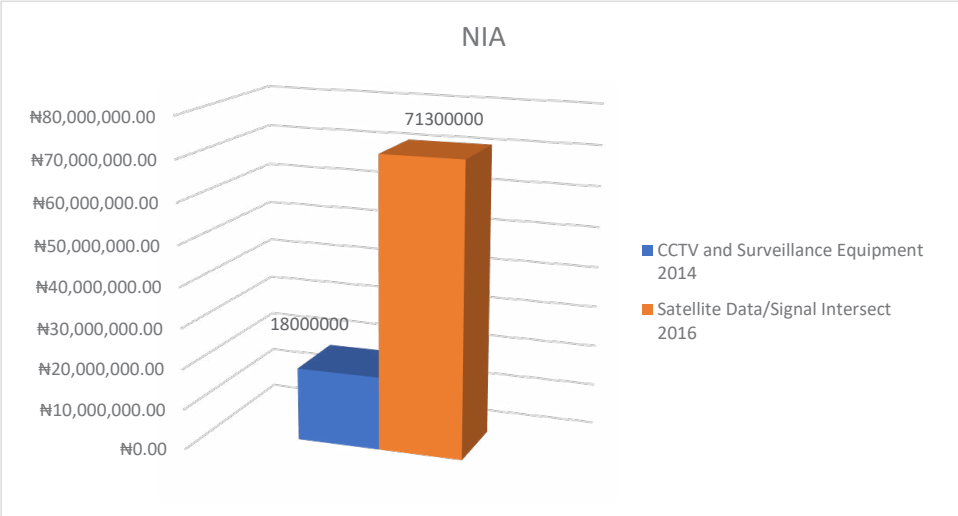
TOTAL – N11, 401,833,33

C. NIA

i. CCTV and Surveillance Equipment (2014) – N18,000,000

ii. Satellite Data/Signal Intersect (2016) – N71,300,000

TOTAL – N89,300,000



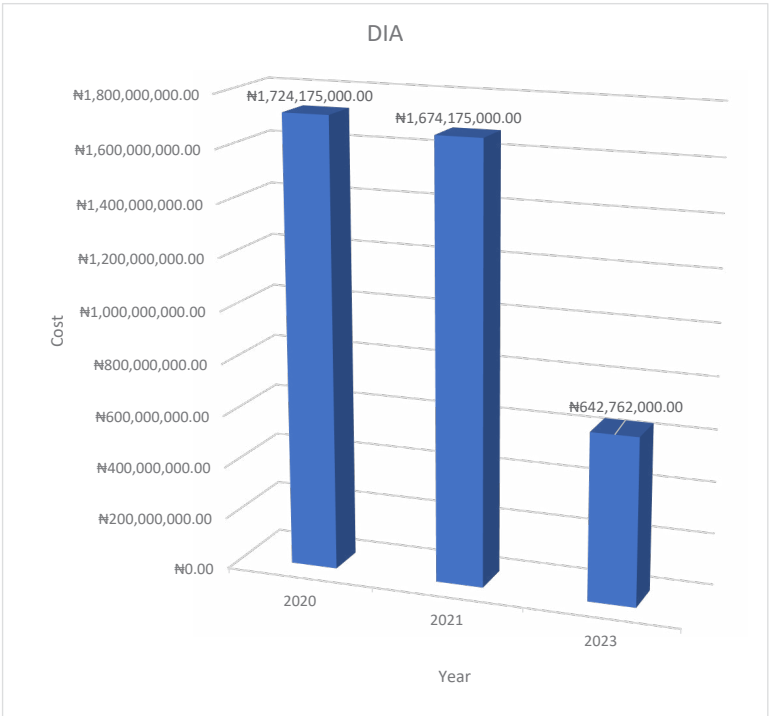
D. DIA

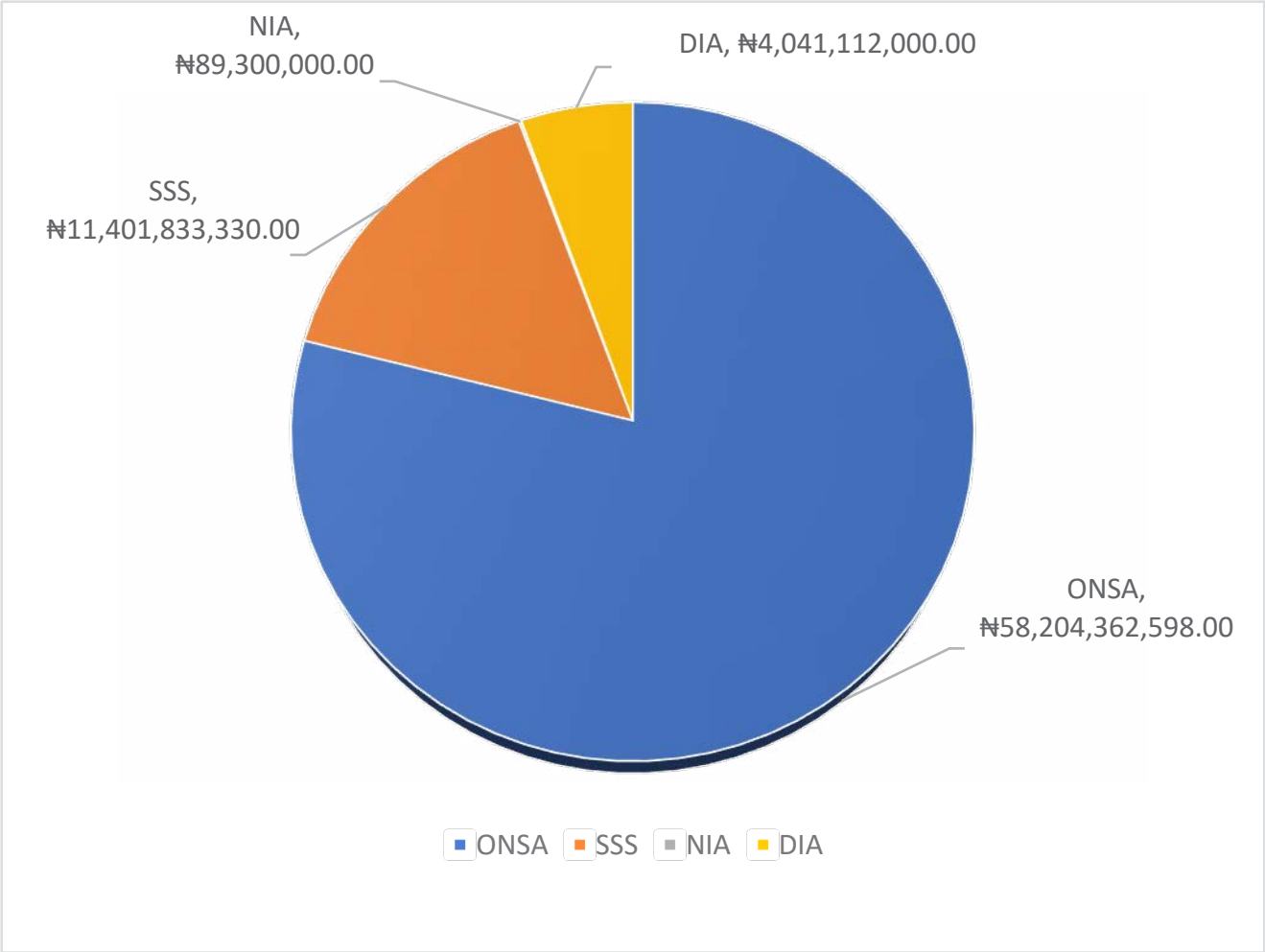
i. Purchase of OSINT software (2020) – N1,724,175,000

ii. Purchase of OSINT software (2021) – N1,674,175,000

iii. Renewal of license for lawful intercept equipment and other platforms (2023) – N642,762,000

TOTAL – N4,041,112,000





forefront of (unlawful) surveillance of citizens. [7] In September 2023, research released by the Institute of Development Studies and the African Digital Network revealed that Nigeria is the largest customer of digital surveillance companies, with at least US$2.7 billion spent on known contracts with China, US, Israel, Australia, EU, and UK-based companies, in a decade-long surveillance spending spree. The report revealed that the Nigerian government shone across the five surveillance technologies available – internet interception, mobile interception, social media monitoring, safe city/ intelligent city, and Biometric ID. [8] The report comes as no surprise, seeing that over time, even though the Nigerian military refuses to make its spending public, the data that has made its way to the public regarding the amount the government spends on surveillance, is revealing.

For instance, in 2019, Paradigm Initiative, a Nigerian-based human rights group, revealed that between 2014 and 2017, the Nigerian government spent at least 127 billion Naira on surveillance and security equipment. [9]Likewise, in 2021, it became known that the National Assembly approved a supplementary budget of 7.46 billion Naira (N7,459,373,304) for Nigeria's Defence Intelligence Agency (DIA) to launch a purported "independent lawful interception platform – voice and advanced data monitoring."

7 A 2020 report from the Africa Center revealed that no less than 15 African countries have deployed surveillance systems in various forms over the years. The rise was attributed to the ease of accessibility of these devices from countries such as China. (Bulelani Jili, 'The Spread of Surveillance Technology in Africa Stirs Security Concerns' (11 December 2020) Accessible here: https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/).

8 Ibid.

9 Paradigm Initiative, 'State of Surveillance in Nigeria: Refocusing the Search Beams' Accessible here: https://paradigmhq.org/wp-content/uploads/2021/04/Policy-Brief-009-Status-of-Surveillance-in-Nigeria.pdf

This was besides the 30.82 billion Naira earlier approved for the agency in the 2021 actual budget. [10] In several cases, the Nigerian government had created pathways for the mass gathering data or surveillance, raising questions of legality, data protection, and threats of surveillance abuse. For example, in 2014, the Nigerian Central Bank introduced the Bank Verification Number (BVN), a biometric identification system that creates a unique identity for each bank customer. However, during the registration processes for citizens to obtain a BVN, they are forced to provide numerous amounts of personal information, some of which are extraneous, and stored by the government permanently. [11]

More so, in 2014, Premium Times, a Nigerian investigative tabloid, ran an expose on a Nigerian spy program installed by the Israeli Elbit Security. [12] The report revealed that the spying system had "unlimited capability to intercept and retrieve any data transmitted over the internet and traditional telecom channels… phone calls, read text messages and hack into computers, mobile phones and any internet ready device."[13] The Premium Times report was preceded by a report by Citizen Lab, an academic research lab at the University of Toronto's Munk School of Global Affairs, which found evidence of the presence of two foreign surveillance systems, the US-based Blue Coat Systems and the UK Gamma International, in Nigeria.[14] The government did not provide context for the rationale and scope of using these systems.

Similarly, in 2017, the Nigerian Director of Defense Information revealed that the activities of Nigerians on social media were being monitored to combat misinformation and to cull anti-government, anti-military or anti-security rhetoric specifically.[15] Information was also not given on the scope and extent of the data being monitored . In the same year, it was revealed that social media user data requests to tech companies from African governments accelerated between 2013 and 2017. [16] Data provided explicitly to Nigeria by Facebook showed that Nigeria requested more information than any other African government (requesting data regarding 119 Facebook user accounts).[17] Again, information from these exercises seems to have been classified.

In 2018, the Nigerian Communications Commission (NCC)[18] revealed that it was sharing citizens' private information with the Nigerian Security Adviser, the country's top intelligence chief accused of spying on Nigerians at various times. [19] In what generated collective

10 Ode Uduu, 'Lawful Interception: NASS Approves N7.46bn for DIA to Intercept Voice Calls and Internet Communications of Nigerians' (July 15 2021) Accessible here: https://www.dataphyte.com/latest-reports/development/lawful-interception-nass-approves-n7-46-bn-for-dia-to-intercept-voice-calls-and-internet-communications-of-nigerians/

11 Adeboye Adegoke, 'Digital Rights and Privacy in Nigeria' (July 2020) Accessible here: https://ng.boell.org/sites/default/files/2020-08/Digital%20Rights%20and%20Privacy%20in%20Nigeria_0.pdf

12 Ogala Emmanuel, 'US Spy Program Reforms Spotlight Nigeria's Expanding Surveillance Program' (February 10 2014) Accessible here: https://www.premiumtimesng.com/news/154931-u-s-spy-program-reforms-spotlight-nigerias-expanding-surveillance-program.html?tztc=1

13 Ibid.

14 Morgan Marquis-Boire, 'The Commercialization of Digital Spying' (May 1, 2013) Accessible here: https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

15 'We Now Monitor Social Media for Anti-Government and Anti-Military Information – Military' (August 23 2017) Accessible from: https://www.channelstv.com/2017/08/23/now-monitor-social-media-anti-government-anti-military-information-military/

16 Yomi Kazeem, 'African Governments are Requesting More User Data from Facebook, Google and Twitter More Than Ever' (August 29, 2017) Accessible here: https://qz.com/africa/1064168/african-governments-user-data-requests-from-facebook-google-and-twitter-hits-historic-level

17 Ibid.

18 The NCC is Nigeria's premier regulatory authority for the telecommunications sector in Nigeria. Established by the NCC Act 2003, it has the functions of regulating the supply of telecommunications services and facilities, promoting competition, and setting performance standards for telephone services in Nigeria.

19 Idris Abubakar, 'Nigerian Government is Spying on Your Phone Calls' (March 7 2018) Accessible: https://technext24.

outrage, the NCC stated that private information provided by citizens during the national SIM card registration was shared with Nigerian security authorities, ostensibly, in a bid to fight crime.[20]

Aside from mass surveillance for state activities, in 2019, the then-president signed the Federal Mutual Assistance in Criminal Matters Bill into law.[21] In what may be likened to self-espionage on behalf of other countries, the law fosters mutual assistance in the prosecution of crime and the location of alleged criminals, through means such as "interception of telecommunications and conversion of electronic surveillance".[22]

Information was not given on the scope and extent of the data being monitored.

Recently, in October 2023, the Minister of Information and National Orientation,[23] revealed the plans by the government to expand the regulation of social media in Nigeria. [24] The proposed route to achieve the regulation would be an amendment of the National Broadcasting Commission (NBC) Act 2004,[25] which currently does not give the commission the power to regulate social media. The extent of this new "regulation" is not evident yet as the amendment is not available for public perusal. However, there may be concerns that the amendment will further give broad monitoring powers to the NBC to keep tabs on all aspects of citizen's use of social media. If this happens, the NBC Act may become yet another law that could concern data protection in Nigeria.

com/2018/03/07/nigerian-government-spying-phone-records-ncc/

20 'SIM Card: ONSA, NCC Partner to Track, Apprehend Criminals' (March 7 2018) Accessible: https://www.nigeriacommunicationsweek.com.ng/confirmed-fg-now-monitors-calls-in-nigeria/

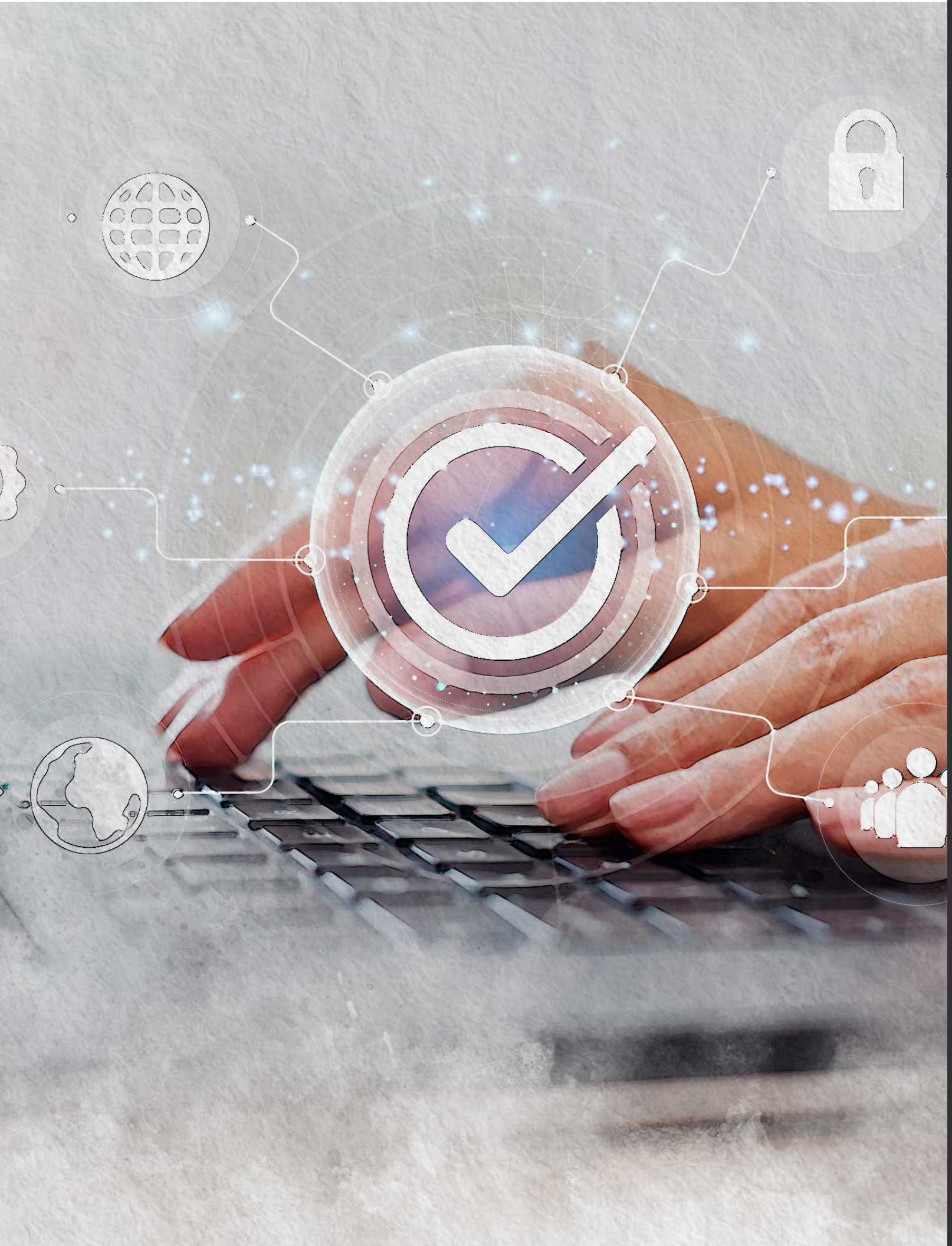
21 Tony Ailemen. 'Buhari Signs Bill on Mutual Assistance in Criminal Matters Act 2019' (June 21 2019) Accessible here: https://businessday.ng/uncategorized/article/updated-buhari-signs-bill-on-mutual-assistance-on-criminal-matters-act-2019/

22 Ibid.

23 The Federal Ministry of Information and National Orientation serves as the Federal outfit responsible for the dissemination of essential and vital information which will enhance and facilitate democratic governance of Nigeria as a Federal Republic. (See the ministry's website here: https://fmino.gov.ng/about-us/).

24 Dyepkazah Shibayan, 'We've Sent Social Media Regulation Bill to the National Assembly' (October 11 2023) Accessible here: https://www.thecable.ng/nbc-weve-sent-bill-seeking-to-regulate-social-media-to-nassembly

25 The NBC Act primarily sets up the NBC as the regulator for the broadcasting industry in Nigeria. To this end, the NBC's functions and powers include receiving, processing, and considering applications for the establishment, ownership or operation of radio and television stations, recommending applications through the Minister to the President, for the grant of radio and television licences, promoting Nigerian indigenous cultures, moral and community life through broadcasting, etc.



National Security or Mass Surveillance: When is Surveillance Legal?

03

Key findings

Section 3(2)(c) of the Nigeria Data Protection Act 2023 exempts data controllers or data processors if the processing of personal data is carried out by a competent authority, as is necessary for national security, from the obligations set out under Part V of the Act, except those relating to the principles of data processing, lawful basis of processing, appointment of data protection officers, and reporting personal data breaches. The implication is that these security agencies, in their adoption of surveillance technologies, are under no obligation to obtain consent for processing, and are not required to provide information to data subjects about processing activity. They are also not required to conduct data privacy impact assessments, which would ordinarily serve to balance and identify the risks and impacts of the processing activity, its proportionality to the intended purposes of the processing, the risks to data subject rights and freedoms, and the presence of mechanisms to address these risks.

The implication is that these security agencies, in their adoption of surveillance technologies, are under no obligation to obtain consent for processing

Arguably, security agencies in Nigeria are not obligated to implement technical and organizational measures to ensure the security and confidentiality of personal data. Relatedly, they are also not subject to any restrictions that come with processing sensitive personal data, children's data, or persons lacking the legal capacity to grant consent. They, therefore, do not fall under any obligation to conduct annual data protection compliance audits, which, in practice, may have allowed for a third-party review of their data management activities and perhaps make recommendations for improvement.

The absence of robust legal safeguards to protect the data and privacy of citizens in this area may legitimize a trend of state surveillance in Nigeria,

The absence of robust legal safeguards to protect the data and privacy of citizens in this area may legitimize a trend of state surveillance in Nigeria, where there seems to be a lack of transparency and justification for the expenditure on certain recurring items across the annual budgets of these agencies. Details are not available on the exact nature of every surveillance-related expenditure in their budgets, and some of them are shrouded in the mystery of code names (e.g., "Develop All Eye", "Stranvisky"). In some instances, budgetary items were only described as "purchase of security equipment," making it impossible to ascertain if the equipment in question was surveillance-related and the extent of its use and scope. However, these vague descriptions were approved, calling into question the level of scrutiny by both chambers of the

National Assembly and their security-related committees.[26] Simply put, all surveillance is (potentially) illegal except in the limited instances where the law allows it. Thus, surveillance that does not require any kind of permission, e.g., listening to someone make a call on a public bus, could be considered legal since no laws, especially privacy, are broken. Thus, even security forces can use this sort of surveillance without breaking the law. However, all surveillance that impacts citizens' privacy rights without any legal justification are proscribed. For example, under Nigerian laws, there are limited instances where surveillance is permitted. Even under the Constitution, the right to privacy can be derogated from in limited circumstances, specifically in the interest of defence, public safety, public order, public morality, or public health, or to protect the rights and freedom of other persons. [27]

Similarly, the NCC has the power to allow authorized interception of communications on the system of third parties it has licensed during a public emergency or in the interest of public safety. [28] Under the Cybercrimes Act, a judge could order a service provider or a law enforcement agent to collect, record, permit, or assist competent authorities with the collection or recording of content data and/ or traffic data associated with specified communications transmitted through a computer system.[29]

Moreso, the National Information Technology Development Agency (NITDA), released a Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries and Conditions for Operating in Nigeria (the "NITDA Code"). Internet Intermediaries[30] and Interactive Computer Service Platforms[31] are, as per the Code, mandated to provide information, including personal data, under their domain or any assistance to any authorized government agencies regarding content put on a platform to carry out an investigation, combat cybercrimes, or prosecuting an offence.[32]

The NDPA likewise exempts data processing from compliance with lawful processing requirements in certain limited circumstances. One such is where data processing is carried out by a competent authority for the prevention, investigation, detection, etc., of a criminal offence; or carried out for prevention or control of a national public health emergency; or carried out by a competent authority for national security, etc.[33] It then means that where surveillance is carried out by a competent authority for the afore-mentioned reasons, no violation of the NDPA would have occurred.

26 However, some budgetary items are described by their proper name, making obtaining an overview of their workings easier on the open internet. The Polaris Mass Location and Wireless Tracking System under the SSS budget of 2014 is used to 'enable government agencies… locate and track suspected criminals and terrorists'. It also offers tracking, geo-fencing, and analytics. A GSM passive off-the-air interception system under the SSS budget of 2014, can be used to 'passively and covertly cellular traffic in an area and analyze it in real-time to identify potential targets, identify suspicious communication patterns using a wide range of analysis tools (location, speech recognition, link analysis, text matching)'. The Finfisher equipment in the 2017 SSS budget may refer to the FinSpy malware, which can infect iOS, Android, Linux, and Windows devices, recording and transmiting all it hears, the keystrokes of the user, transmitting images and screenshots of user activity, intercepting emails, calls, and files on the device. ETL technology under the 2017, 2019, and 2021 budgets of the SSS is used for combining data from multiple sources into a central repository, from where it can be analyzed and machine learning algorithms can be applied to derive insights.

27 Section 45 of the Constitution of the Federal Republic of Nigeria 1999 (as amended).

28 Section 147 and 148 of the NCC Act 2003.

29 Section 39 of the Cybercrimes Act.

30 Under the NITDA Code, Internet Intermediaries are defined to include social media operators, websites, blogs, media sharing websites, online discussion forums, streaming Platform, and other similar oriented intermediaries where services are either enabled or provided and transactions are conducted and where users can create, read, engage, upload, share, disseminate, modify, or access information.

31 Under the NITDA Code, Interactive Computer Service Platforms refer to any electronic medium or site where services are provided by means of a computer resource and on-demand and where users create, upload, share, disseminate, modify, or access information, including websites that provide reviews, gaming Platform, online sites for conducting commercial transactions.

32 Sections 1 & 2 of Part 1 of the NITDA Code.

33 See section 3 of the NDPA.

However, one of the most critical pieces of legislation that vests the government with unfettered power to monitor citizens' communications is the Lawful Interception of Communications Regulations 2019 (the "Regulations") released by the NCC. The Regulations provide the basis, process, and framework for the interception of communications and divulgence of the same communications[34] by an authorized agency[35] in Nigeria. Agencies recognized under the Regulations are empowered to intercept communications where the interception is related to the use of a communications service provided by licensees[36] to persons either in or outside Nigeria [37], either upon the grant of a warrant by a judge or, in limited instances, without a warrant. There is a concerning provision for lawful interception of communications without a court warrant, even by private individuals where "in the ordinary course of business, it is required to record or monitor such communication."[38]

The primary reason often offered by the government for state surveillance is to ensure national security, combat terrorism, and prevent crime. However, these practices raise significant privacy, ethical, and legal concerns, leading to debates and challenges regarding their acceptability, regulation, and oversight. This "national security" rhetoric gained prominence following the rise of the terroristic activities in late 2002. Surveillance, it appeared, was the only way the security forces could gather enough intel to dismantle groups like Boko Haram. Hence, the required expansion of surveillance was treated as a trade-off for continued security. [39] However, globally, sanctioned surveillance is always to happen within the bounds of the law, emphasizing necessity, proportionality, transparency, and data protection. The Paradigm Initiative Report earlier cited reveals that of the vast government resources expended on surveillance systems between 2014 and 2017, there was little or no evidence to show that the expenditures were spent on cyber protection or engaging in national security protection. Instead, the evidence showed that the surveillance could have been used mainly for political influences. [40]

with the vast government resources expended on surveillance systems between 2014 and 2017, there was little or no evidence to show that the expenditures were spent on cyber protection or engaging in nationalsecurity protection.

34 See Regulations 4, 6, 7, 9, 10 and 12, Lawful Interception of Communications Regulations 2019.

35 Authorized agency refers to the Office of the National Security Adviser represented by the National Security Adviser or his assignee, or the State Security Services represented by the director. (Section 12(1) of the Lawful Interception of Communications Regulations 2019.

36 In this context, a licensee means any person, body or organization that provides communications services in accordance with the license issued to such a person by the NCC.

37 Regulations 4(a) & (b) of the Lawful Interception of Communications Regulations 2019.

38 Regulation 8 of the Lawful Interception of Communications Regulations 2019.

39 Ibid (n 9).

40 Paradigm Initiative, 'Status of Surveillance in Nigeria: Refocusing the Search Beams' (Accessible here: https://paradigmhq.org/wp-content/uploads/2021/04/Policy-Brief-009-Status-of-Surveillance-in-Nigeria.pdf)


E
R
S
F
X
C

Data Protection Laws Against Surveillance Abuse

04

Nigeria has a wealth of laws providing for the sanctity of the private lives of citizens and thus prohibiting surveillance outside the limited confines of the law. This lineup is led by the Constitution of the Federal Republic of Nigeria, which guarantees that the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications are protected.[41] This constitutional provision forms the springboard[42] for other legislations that directly or peripherally provides data protection. For instance, under the Cybercrimes (Prohibitions, Prevention, etc.) Act 2015. It is an offence for any person to intercept, by technical means, non-public transmissions of computer data, content, or traffic data.[43]

However, the first instrument to centre data privacy at its core is the Nigeria Data Protection Regulations 2019 (the "NDPR").[44] After the NDPR's enactment, the Nigeria Data Protection Regulations Implementation Framework 2020 (the "NDPR Implementation Framework") was released to expatiate the relevant provisions of the NDPR. The NDPR served as the precursor to the NDPA which is currently the primary instrument regulating data protection in Nigeria. The NDPA expressly provides that the NDPR will continue to exist complementarily with the NDPA, until the NDPA makes any regulations eliminate the NDPR.

the NDPR will continue to exist complementarily with the NDPA, Until the NDPC makes any regulations to eliminate the NDPR.

The NDPA applies to the processing[45] of personal data[46] of a data subject, [47] whether by automated means or not, by a broad category of entities referred to as data controllers [48] or data processors.[49] The NDPA provides for what qualifies as lawful processing of personal data, which essentially refers to the instances where the processing of personal data is permitted. [50] Asides from the principle of lawful

41 Section 37 & 39 of the Constitution of the Federal Republic of Nigeria 1999(as amended).

42 Notably, the provisions of the Constitution which guarantee the privacy of citizens make no mention of data. However, the Court of Appeal has given rulings to the effect that information on homes, correspondences and telephone conversations are captured in the definition of personal data. Hence, the Constitution can rightly be relied upon to ground an action in data protection. (See Emerging Market Telecommunication Services (EMTS) v Barr Godfrey Nya Eneye [2018] LPELR-46193.)

43 Section 12 of the Cybercrime Act.

44 The NDPR was released by the National Information Technology Development Agency (NITDA) in 2019, to achieve the following objectives: to safeguard the rights of natural persons to data privacy; foster safe conduct for transactions involving the exchange of Personal Data; tprevent manipulation of Personal Data; and ensure that Nigerian businesses remain competitive in international trade, amongst others.

45 The NDPA defines "Processing" as any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and does not include the mere transit of data originating outside Nigeria.

46 The NDPA defines "Personal Data" as any information relating to an individual, who can be identified or is identifiable, directly, or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.

47 The NDPA defines a "Data Subject" as an individual to whom personal data relates.

48 The NDPA defines a "Data Controller" as as an individual, private entity, public Commission or agency, or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

49 The NDPA defines a "Data Processor" as an individual, private entity, public authority, or any other body who or which processes personal data on behalf of or at the direction of a data controller or another data processor.

50 Section 25 of the NDPA provides for lawful basis for the processing of data of data subjects. They include: (a) where the Data Subject has given and not withdrawn consent for the specific purpose or purposes for which Personal Data is to be processed. (b) where processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; (c) where processing is necessary for compliance with a legal obligation to which the Data Controller or Data Processor is subject; (d) where processing

processing, data processors/controllers are mandated to collect data for specified, explicit and legitimate purposes (the "Purpose" principle), [51] collected data is to be adequate, relevant and limited to the minimum necessary for the purposes for which the personal data was collected or further processed (the "Data Minimization" principle),[52] retained for the period mandated by law (the "Retention" principle"),[53] and processed data is protected against unauthorized or unlawful processing, including implementing technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession.[54] Where consent is obtained as the basis for lawful processing, such consent must be freely given, specific, informed and unambiguous. Further to these principles, a data subject has a slew of rights relating to the processing of their data. These include the rights of access to data/copies of data, right to rectification of errors, right to deletion of data, right to object to processing, right to restrict processing, right to data portability, and right to withdraw consent.[55]

To underscore the public sector's non-exemption from the data protection laws, NITDA released the Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020 (the "Guidelines"). The Guidelines specifically guide public officers on handling and managing personal information in compliance with the NDPR (and, by extension now, the NDPA), acknowledging that governments at all levels are the biggest processors of personal data of Nigerians and in Nigeria. [56] The Guidelines apply to public institutions in Nigeria, including ministries, departments, agencies, public corporations, publicly funded ventures, and incorporated entities with government shareholding, either at the federal, state or local levels.

In the broader African context, the "Malabo Convention," more formally known as the African Union Convention on Cyber Security and Personal Data Protection, was adopted by the African Union in 2014 to strengthen cybersecurity and data protection standards among member states. While enough countries have not yet ratified the convention to enter into force, its emphasis on protecting personal data obliges state parties to legislate measures that safeguard personal data, adhering to principles concerning collecting, processing, and securing such data. These provisions are meant to protect individuals against the unlawful collection and processing of personal information, which can include unjustified surveillance activities. The convention promotes a legal framework that defines and prohibits unlawful activities conducted in cyberspace. Setting these standards implicitly mandates the state parties to ensure that their digital surveillance activities do not breach individuals' and organizations' lawful rights and data security.

Expectedly, some international treaties have laid the foundation for modern-day state legislation on

---

is necessary in order to protect the vital interests of the Data Subject or of another natural person; where processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the Data Controller; or (e) where processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or Data Processor, or by a third party to whom the data is disclosed.

51 Section 24 (1) b of the NDPA.

52 Section 24 (1) c of the NDPA.

53 Section 8.2 of the NDPR Implementation Framework provides for the retention periods for personal data as follows: (a) three years after the last active use of a digital platform; (b) six years after the last transaction in a contractual agreement; (c) upon the presentation of evidence of death by a deceased's relative, the Data Controller and/or Processor must immediately delete the Personal Data of the deceased Data Subject unless there is a legal obligation imposed on the Data Controller to continue to store the Personal Data; (e) immediately upon a request by the Data Subject or his/her legal guardian where: (i) no statutory provision provides otherwise, and (ii) the Data Subject is not the subject of an investigation or suit that may require the Personal Data sought to be deleted.

54 Sections 24 (1) f and 39(1) of the NDPA.

55 Sections 34, 36, 47 of the NDPA.

56 Section 1.2 of the Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020.

privacy and anti-surveillance.[57] Article 12 of the Universal Declaration of Human Rights provides that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. The International Covenant on Civil and Political Rights (ICCPR)[58] , which Nigeria is a signatory to, provides that no one shall be subject to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor unlawful attacks on his honour and reputation. [59] Specifically, the convention provides that "everyone has the right to the protection of the law against such interference or attacks ." [60]

Everyone has the right to protection under the law against interference with their privacy or attack on their reputation.

57 According to the United Nations, 137 out of 194 countries have legislations in place to secure the protection of data and privacy. (Source: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide).

58 The International Covenant on Civil and Political Rights was adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 and formally entered into force on 23 March 1976.

59 Article 17 (1), the ICCPR.

60 Article 17 (2), the ICCPR.-

Policy Propositions: Implementation of Data Protection Measures Against Surveillance Abuse in Nigeria

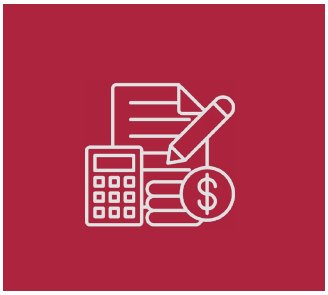
05

Key takeaways

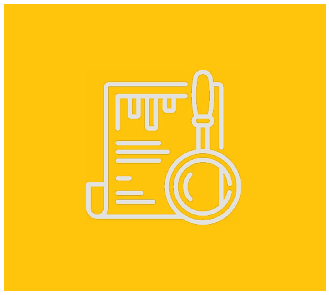
Nigeria has increasingly enacted comprehensive data protection laws since introducing the Nigeria Data Protection Regulation (NDPR) 2019 until the Nigeria Data Protection Act (NDPA) 2023. However, exemption clauses in these laws limit the enforceability of these laws. Barring an amendment to the NDPA to reduce the scope of exemptions or the issuance of tailored regulations that put in place data protection parameters for the adoption of surveillance technologies, there is a need for greater engagement at the constituency level towards the presentation of the 2024 budget and beyond.

This engagement should be aimed at enlightening constituents on the real-world application of these surveillance tools and their implications for their right to privacy. This will also be supported by engagement with parliamentarians in both houses of the National Assembly, prioritizing their security-related committees.

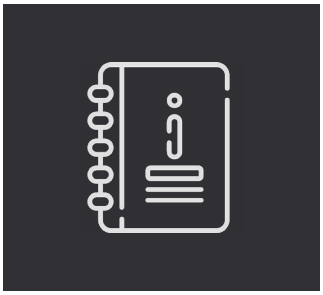
The objectives of this engagement will include, but are not limited to:



Demanding explicit description of all items in the budgets of agencies covered by the National Security Agencies Act 1986.



Report on utilizing previously approved funds for surveillance equipment, the impact on overall security, and safety measures implemented in their real-world deployment. Emphasis should be placed on those items that recurred more than once in previous budgets.

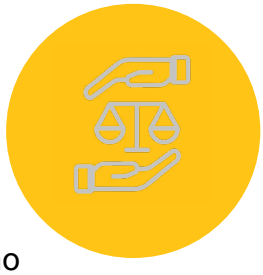


Achieving consensus on the position that continued approval of funds will be contingent upon the issuance of data protection guidelines from the ONSA, binding on itself and agencies under its supervision, in their use of surveillance.

A For Government

The discretion granted to certain government officials to intercept communications weakens the effectiveness of the data protection laws in Nigeria. For instance, a warrant for interception of communications can be issued in vague instances, such as in the interest of national security, to prevent or investigate a crime, to protect and safeguard the economic well-being of Nigerians, in the interest of public emergency or safety, or to give effect to any international mutual assistance agreements to which Nigeria is a party. [61] In fact, the authorized agency can obtain a warrant after the fact in the event of immediate danger of death or severe injury to any person, activities that threaten national security, or activities that have the characteristics of organized crime.[62] Given the wide latitude of the preceding, virtually any surveillance carried out by the NSA or DSS can be justified. Thus, there must be a balance between data protection laws and the need to safeguard citizens. To balance the requirements of data protection laws and lawful interception, the following should be implemented:

1. Stronger Enforcement: The challenge is not a lack of principles and laws to prevent a violation of privacy through surveillance or otherwise. Hence, where unsanctioned surveillance exists, it is a pointer to the fact that there is an enforcement gap. The NDPC,[63] the entity empowered to enforce the provisions of the NDPA, lacks the will and capacity to enforce the data protection laws' provisions, especially concerning data privacy violations by public institutions and government agencies. It is telling that in the wake of the multitude of data privacy violations that the Nigerian government has been accused of, enforcement actions have not been taken.



2. Operationalizing Penalties: An indication of a robust enforcement mechanism is the imposition of penalties, where appropriate. Generally, penalties under the data protection laws include fines, with the monetary limits varying for a Data Controller/Processor of Major Importance[64] ("DCMI/DPMI") , [65] and a regular data controller. [66] Additionally, a data subject who suffers injury, loss, or harm due to a violation of the NDPA may also recover damages from the data controller or processor who caused the damage in a civil proceeding.[67] The courts may order forfeiture against a

61 Regulations 7 (3) of the Lawful Interception of Communications Regulations 2019.

62 Regulations 12 (4) of the Lawful Interception of Communications Regulations 2019.

63 Prior to the enactment of the NDPA, data protection enforcement in Nigeria was enforced under the auspices of the NITDA.

64 A DCMI/DPMI is defined under the NDPA as a data controller or data processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate

65 Such a defaulter will be liable to pay a fine of Ten Million Naira (N10,000,000) (approximately $12,860) or 2% of the controller/processor's annual gross revenue in the previous financial year, whichever is higher. (Section 44 of the NDPA).

66 Such a defaulter will be liable to pay a fine of Two Million Naira (N2,000,000) (approximately $2,570) or 2% of the controller/processor's annual gross revenue in the previous financial year, whichever is higher.

67 Section 51 of the NDPA.

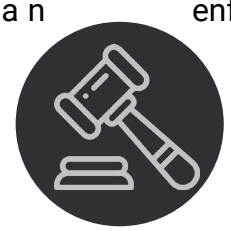
convicted data controller, data processor, or individual per the Proceeds of Crime (Recovery and Management) Act 2022.[68] It appears none of these penalties relates specifically or considers the peculiar situation of government agencies who are culpable in violating data privacy rights. This is because it is inconceivable that the NDPC can impose fines on a government entity like the NSA. Thus, there must be a review of the penalties provided in the various data protection laws.

3. Mandating Transparency: One of Nigeria's most significant challenges with mass surveillance is that it is shrouded in secrecy. The opacity that trails surveillance hinders robust conversations around the subject, creates an easy avenue for surveillance abuse, and ensures the infractions are hardly identified or addressed. A core principle of data protection laws is transparency. Data subjects are made aware of the nature, extent, and length of time their data is used. This data protection principle can be imported into surveillance. Transparency would mean ensuring that the legal requirement regarding surveillance is followed. Additionally, violations must be brought to light and penalized accordingly. The benefits of the Nigerian data protection regime will be most evident in an environment of transparency.

4. Paying Attention to Developing Technologies: As digitalization expands and new technologies are introduced, new surveillance opportunities and further data protection violation continue to emerge. For a jurisdiction like Nigeria, with low enforcement capabilities and inadequate ICT infrastructure, the deep information asymmetries between the private sector and regulatory agencies and the vast market power of these private agencies may empower companies to evade scrutiny and continue violating individual rights. To prevent the violation of rights by new technologies, every new technology must be subject to current data protection laws. New technologies have to be closely monitored to ensure that new capabilities can violate privacy rights through surveillance or otherwise meet data protection thresholds and stipulations. Contemporaneously, as new capabilities are discovered, the laws should be equally updated to cater to such lacunas and further prevent data processing.

B For Citizens

5. Sensitization: The first step in preventing privacy incursions is sensitization. Citizens need to know the laws on data privacy, the extent of the rights available to them, and the remedies. Knowledge of what the law is could prevent surveillance abuse in that citizens understand the extent of data obligations they have to comply with and thus limit the sharing of personal data to the barest minimum.
Additionally, knowledge of data privacy rights will aid enforcement efforts. A well-informed citizen can enforce their data privacy rights upon any breach.



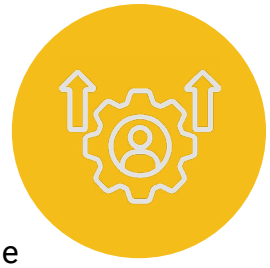
6. Participating in Legislative Processes: Citizens can influence laws made at their legislative houses by influencing their elected representatives at such forums. Hence, citizens should be active participants in the legislative process, engage in

68 Section 52 of the NDPA.

data privacy stakeholder conversations, and oppose legislation that either unduly restricts data privacy or grants extensive surveillance powers to the state and its authorities.

7. Prioritizing the Importance of Cybersecurity.: It is not the duty of a private citizen to prevent surveillance by the state. Also, surveillance is sometimes inevitable. Thus, it may behove each citizen to take active steps to prevent surveillance and encroachment on their privacy. One such way could be using apps and online tools that limit incursions to private digital spaces. For instance, using Virtual Private Networks, and encrypted apps can prevent privacy violations. This effort should be in addition to, and not an alternative to, enforcing data protection compliance.

C For Civil Society



8. Advocacy for the Lawful Processing of Data: Civil Society Organizations (CSOs) can advocate for the rights of data subjects in cases where surveillance abuse is evident, especially for the most vulnerable members of society who may be unable to ensure their data protection rights are protected actively. Some CSOs have the means and the muscle to reject extraneous personal data requests from the government and use these situations as grounds for challenging the government in court and elsewhere. At all times, CSOs support the rights of citizens to data protection, even if it means going up against the government.

9. Lobbying and Stakeholder Engagements: CSOs can lobby for more effective laws and policies to respect data protection rights and constrain the Nigerian government's seemingly limitless surveillance powers. Stakeholder engagements with media institutions, academia, and even data privacy experts can help foster collaboration and partnerships toward a data protection regime that will counteract surveillance abuse. The relationships, networks, and tools CSOs have at their disposal (both at home and abroad) could be leveraged to put pressure on the government and the surveillance tech industry.

10. Aiding Enforcement: Some CSOs occupy a unique position where they can assist individuals in enforcing data privacy rights breached by the government, corporations, or fellow citizens. By providing technical know-how, they can help institute strategic data protection litigation or class action suits, advise in challenging the status quo of surveillance abuse through FOI requests, act as amicus curiae in courts, etc. As mass surveillance tools are sometimes classified or shrouded in secrecy, investigations may need to be carried out, and even mass education campaigns to ensure that data privacy laws are duly enforced, and citizens are protected from mass surveillance.

D For Media

11. As a watchdog, the media is responsible for raising awareness about the importance of data privacy, reporting on breaches, and holding both government and private sector entities accountable for surveillance overreach. By investigating and spotlighting the implications of inadequate data protection and the risks of surveillance abuse, various media outfits (traditional media, social media, new media, etc.), must play their role in educating the public and catalyzing citizen engagement. This should include prompting demand for more vital legislation and enforcement. Additionally, the media in Nigeria can serve as a platform for experts to discuss best practices and for advocacy groups to campaign for citizens' rights, thus playing a central role in shaping a culture of privacy and the discourse around data protection policies in Nigeria.

E For Private Sector

12. Adoption of Robust Privacy Frameworks: Companies can lead by example by implementing comprehensive data protection policies and practices within their operations. This includes complying with the NDPA and NDPR and adopting global best practices such as the GDPR framework, and the various UN guidelines for businesses to comply with human rights principles. Businesses must ensure that personal data is collected, processed, stored, and shared securely and lawfully. The private sector can set high standards for data stewardship, demonstrating the viability and benefits of strong data protection measures, and encouraging broader industry compliance.

13. Innovation in Data Security Technologies: The private sector, particularly technology companies and start-ups, is well-positioned to drive innovation in data security solutions. By investing in research and development of advanced security products and services, such as encryption technologies, secure data management systems, and privacy-enhancing tools, companies can offer solutions that help mitigate the risk of surveillance abuse. These technological advancements can be made available not just within the private sector, but also as part of public-private partnerships to strengthen the overall data protection ecosystem in Nigeria.

accountabilitylab
NIGERIA