Surveillance Law in Africa: a review of six countries

Nigeria country report

Ridwan Oloyede

DOI: 10.19088/IDS.2021.059

This report explores the surveillance landscape in Nigeria. It provides a concise review of the existing domestic laws, practices and jurisprudence relating to surveillance and privacy, while outlining the safeguards, checks and balances available and how they operate in practice. Surveillance is defined here as the 'monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future' (Electronic Frontier Foundation (EFF) 2014).

The report also examines surveillance cases that have played out in Nigerian courts and decides whether the existing surveillance practices are legal, necessary and proportionate. In addition, the report considers the efficacy of existing laws to protect privacy and limit surveillance. Nigerian surveillance law is then compared against international law, specifically against the UN Draft Legal Instrument on Government-led Surveillance and Privacy and the International Principles on the Application of Human Rights to Communications Surveillance (EFF 2014). Recommendations are then made based on the analysis of legislation, gaps in existing policies and practices, and the need to protect Nigerians' privacy rights adequately. Finally, the report closes with recommendations to different stakeholders on improving the quality of legislation, understanding prevalent practices and responsibly implementing the law.

Introduction

State surveillance on its own is 'not inherently unlawful, especially when governments have legitimate reasons to undertake surveillance that is not rooted in a desire to enforce political repression and limit individual 'freedoms' (Feldstein 2019: 11). However, governments must ensure that while protecting national security they take care to avoid infringing on the human rights of their people (Privacy International 2014). Historically, Nigeria has had a repressive colonial and military past that encouraged state surveillance. Unfortunately, it has continued to fester even during the democratic dispensation. As a result, information capture to monitor Nigerian citizens' activities has proliferated in recent years, despite the legal right to privacy.

Nigeria is the most populous country in Africa, with a population of over 180 million people. In the past decade, the country has witnessed an increase in violent incidents that are threatening national cohesion,[1] which the government has cited as the justification for surveillance. The government was reported in April 2013 to have procured surveillance technology from Elbit Systems Limited in Israel (Johnson 2013; Ogala 2013) to 'advance the internet and computer-based gathering of Nigerian citizens' personal data' (Advox 2013). The government ignored protests by concerned civil organisations and citizens, and the lack of enabling legislation for such procurement, and went ahead regardless. More research (Marquis-Boire *et al.* 2013) conducted in the same year also revealed the government's involvement with global spyware giant FinFisher (*ibid.*: 104). A report titled 'Running in Circles: Uncovering the Clients of Cyber-espionage Firm Circles' also revealed that 'a telecom surveillance company by the name of Firm Circles [had] been helping state security apparatuses across 25 countries, including Nigeria, to spy on the communications of opposition figures, journalists, and protesters' (Al Jazeera 2020). The Nigerian government spent close to 46 billion naira (US$127.6 million) in 2017 (Budget Office of the Federation 2021) and budgeted almost 9 billion naira (US$22.8 million) in 2020 (Adegoke 2021) for surveillance-related activities or equipment.

Multiple state agencies now require fingerprint, facial capturing or other biometric[2] data for identification. No less than six government agencies maintain different biometric data points on citizens and residents at federal

1 There is the notorious threat posed by militant Islamist group Boko Haram, which has been reported to be the cause of more than 300,000 deaths, with more than 2 million people displaced in the north-eastern part of the country since 2002 when the group started its operations. In the north-west, communities have witnessed killings and kidnappings by armed groups. There have also been military actions in the south and the south-east.

2 Biometrics is the measurement and statistical analysis of people's unique physical and behavioural characteristics.

level,[3] while some state governments have also adopted resident registration programmes (Ajayi 2021). Some states have adopted closed circuit television (CCTV) cameras in public for surveillance and security (TVC News 2020). The live feeds from the cameras are observed from a command centre, ensuring real-time updates to law enforcement agencies. The Lagos State Vehicle Inspection Service uses licence plate recognition of CCTV images to monitor traffic offenders and impose sanctions on erring vehicle owners (QED 2018). The fine ticket is sent to the address of the owner of the offending vehicle. Some law enforcement agents in Lagos state reportedly now wear body cameras (Guardian 2021).

The Nigerian Senate in July 2021 approved 4.8 billion naira (US$11 million) to the Nigerian Intelligence Agency for the purchase of WhatsApp Intercept Solution and Thuraya Interception Solution, 'a communications system used for monitoring voice calls, call-related information, short message service (SMS) and data traffic, among others'. The deployment of these tools will impact end-to-end encryption for 'communication' (Iroanusi 2021). In the past year, Nigerians have used virtual private networks (VPNs) to beat the 'government's blocking of access to micro-blogging site Twitter (Arise News 2021). In June 2021, the government suspended the operation of Twitter in Nigeria. Nigerians have also relied on the use of other privacy-preserving communication tools such as Signal and Telegram (The New York Times 2021). According to the Committee to Protect Journalists, it 'found at least two companies that produce digital forensics tools – Israel-based Cellebrite and U.S.-based AccessData – operating in Nigeria' (Rozen 2019). The tools are capable of extracting information from phones and computers.

One might argue that the government needs targeted surveillance, primarily because of the sad realities of the state of insecurity in the country. However, civil society organisations and citizens generally are concerned that surveillance could be normalised and abused by authorities, especially in the absence of adequate legal protection. This concern has been confirmed repeatedly by the incidence of surveillance abuse by governments the world over. For example, in the case of Nigeria, research has shown that the procurement of surveillance equipment by the government was simply for 'political reasons, especially by the then authorities in power to monitor their adversaries and political opponents' (Ekott 2013). At the same time, others consider the Nigerian government to have the capability to 'intercept all internet activity and to invade users' privacy at will' (Dada and Tafida 2014).

3 Independent National Electoral Commission (voter card); Central Bank of Nigeria (bank verification number); Nigeria Police Force (tint permit, which allows drivers to wear tinted glasses); Federal Road Safety Commission (driver's licence); Nigeria Immigration Commission (international passport and residential permit); and National Identity Management Commission.

Against this background, this report provides a country assessment of the Nigerian government's use of state surveillance on citizens. In addressing the research questions, this report will provide a concise review under several subheadings.

1. What reasons does the Nigerian government use to justify surveillance?

Due to its lengthy colonial and military history, surveillance of citizens, dissents and opposition has been a recurrent theme. Article 7(3) of the Lawful Interception of Communication Regulations (LICR) specifies as legitimate aims for surveillance in Nigeria: national security; preventing or investigating crime; protecting and safeguarding the economic wellbeing of Nigeria; public emergency or safety interests; and giving effect to any international agreement Nigeria is a party to. The rise in domestic terrorism has also fuelled the case for surveillance, leading to increased spending in this area. In addition, the outbreak of the Ebola virus in 2014 and the coronavirus (Covid-19) pandemic in 2020 provided public health and emergency as a premise for health surveillance. Visitors' personal information was documented for testing and tracing. The motive is evident in the enactment of the Covid-19 Regulations 2020, under the Quarantine Act (Cap Q2 LFN 2004).

2. Which international conventions protecting privacy has Nigeria adopted?

Nigeria has ratified or adopted into domestic law a range of international conventions that guarantee its citizens' right to privacy and freedom from unwarranted surveillance, including those listed below.

a. **African Charter on the Rights and Welfare of the Child**

Article 10 of the charter guarantees African 'children's right to privacy. Accordingly, children enjoy protection of the law in relation to their communications and correspondence, which cannot be unduly interfered with. Nigeria ratified the charter in 2001.

b. **Universal Declaration of Human Rights**

Article 12 provides that no one should be subjected to arbitrary interference in relation to their privacy and correspondence. Thus, all Nigerians should enjoy legal protection against such arbitrary interference.

c. **International Covenant on Civil and Political Rights**

Article 17 of the covenant provides that individuals should enjoy protection from arbitrary and unlawful interference in their communications and correspondence.

d. **Economic Community of West African States Supplementary Act on Personal Data Protection**

The act creates a legal framework for the protection of personal data in the West Africa sub-region. Nigeria is a signatory to the act.These international instruments have emerged as international human rights norms Nigeria is committed to uphold in relation to protection of privacy. According to section 12 of the Nigerian Constitution, these instruments take effect and have the force of law in Nigeria when enacted into law by the legislature.

3. Which domestic laws enable or limit permitted surveillance in Nigeria?

The most significant laws and draft bills enabling surveillance include those listed below.

a. **Constitution of the Federal Republic of Nigeria 1999**

Section 37 of the constitution guarantees the 'privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications'. However, section 45 restricts the application of rights 'in the interest of defence, public safety, public order, public morality or public health'. Nonetheless, such derogation must be 'reasonably justifiable in a democratic society'.

b. **Cybercrimes (Prohibition, Prevention, etc.) Act 2015**

Section 45(2) (e) and (f) permit law enforcement officers to apply to a judge *ex parte*[4] for a warrant to 'search any data contained in or available to any computer system or computer network' and to 'use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format'. These provisions provide one of the bases for the decryption of encrypted communication in Nigeria.

Similarly, section 38(1) of the act mandates service providers to retain traffic and content data for two years. Further, section 38(2) of the act allows law enforcement agents to request data from service providers, and they are mandated to comply. Section 38(4) prescribes that data obtained under the provision can only be used for a legitimate purpose. However, the act fails to define what constitutes a legitimate purpose. Section 45 of the act enables a law enforcement officer to apply to a judge to obtain electronic evidence in the investigation of crime without notifying the individual subject to the investigation. There is no publicly available repository or report to the legislature documenting such requests and approvals. Section 12 criminalises unlawful interception of communication with an imprisonment term of up to two years, a fine of 5 million naira (US$13,888) or both, which is consistent with the international principle on safeguards against illegitimate access. Finally, section 38(5)

4 *Ex parte* means a legal proceeding brought by one party in the absence of and without representation of or notification to another party.

prescribes that the exercise of the power must uphold the right to privacy guaranteed under the constitution.

c. **Mutual Assistance in Criminal Matters Act 2019**

Part V of the act provides for interception of telecommunications and postal items and surveillance, including covert electronic surveillance. Among other things, it allows for the exchange with other countries of: surveillance information relating to the identification and location of criminal offenders; obtaining evidence; securing the production of official or judicial records; interception of postal orders; interception of telecommunications; and conversion of electronic surveillance. An interception under the act is limited to criminal matters of a serious nature. In this regard, the government can be involved in the surveillance of citizens once it pursues a criminal investigation. The act further encourages transparency through the requirement that government requests for citizens' data should be published: such a request can only be made based on reasonable suspicion, and it must specify the purpose, the type of communication to be intercepted, the details of the recipient of the data and details of the authority concerned. The attorney general of Nigeria is designated as the central authority responsible for handling requests for mutual assistance between the countries.

d. **Terrorism Prevention Amendment Act 2013**

The act amends the Terrorism (Prevention) Act of 2011 (TPA). It gives the relevant law enforcement agency power to intercept communications to prevent terrorist acts and detect offences related to them. However, this is subject to getting the approval of the attorney general, inspector general of police and coordinator of national security. Section 29 of the act empowers the relevant law enforcement agency to conduct intelligence gathering 'for the prevention of terrorist acts or to enhance the detection of offences related to the preparation of a terrorist act or the prosecution of offenders under this Act.' The judge's order can permit the installation of a device to intercept communication. However, the order must specify the duration for the service provider to retain the communication data. Section 24 permits terrorism investigation with a judge's approval; the warrant request must specify the purpose and material relevance to the investigation. In contrast, section 25 allows an investigation without a warrant when there is a verifiable urgency, where life is threatened and when seeking the judge's approval would delay or be prejudicial to public safety. Such an officer cannot be less than the rank of the chief superintendent of police.

e. Nigeria Data Protection Regulation 2019

The National Information Technology Development Agency (NITDA) published the regulation in 2019. It creates a set of obligations for both public and private entities. The regulation provides for data protection rights, principles and lawful bases for processing personal data. Prominently, public interest exercised by public authority and lawful obligation is part of the lawful bases recognised under the regulation. The Data Protection Implementation Framework, which is an addendum to the regulation, includes processing carried out by public agencies to investigate crime, national interest and public safety as exceptions to the application of the Nigeria Data Protection Regulation (NDPR). Finally, individuals have the right to approach the court to seek redress for violation of their rights.

f. Nigerian Communications Commission Act 2003

The Nigeria Communications Commission (NCC) regulates internet service providers and mobile phone companies. The Nigerian Communications Act provides a 'regulatory framework for the Nigerian telecommunications industry'. Section 147 gives the NCC the power to determine that a licensee or class of licensee has 'the capability to allow authorised interception of communications'. Section 148 gives the NCC the power on the occurrence of 'a public emergency or in the interest of public safety' to: suspend operation licenses; take temporary control of services or network facilities; order the disclosure, interception or prevention of specified communications; withdraw services or network facilities; or order the possession of 'network facilities, service, or customer equipment' (section 148(1a–d)).

It is disturbing that the act refers to the preservation of 'national security' and dedicates sections 146–149 to 'national interest matters' but fails to provide a working definition of the terms. Section 157, which is the interpretation section, also categorically fails to spell out what qualifies as a public emergency and to define what constitutes public safety. All these provide gaps that could occasionally be abused by a future government, which could use this imprecision to curtail citizens' rights.

Outside the principal act, the NCC is empowered to issue secondary legislation to regulate the telecommunications sector. The NCC has exercised this power by issuing regulations, guidelines and a code of practice that impose an obligation on service providers to intercept communications, decrypt encrypted communication, disclose communications data to law enforcement agencies and potentially violate the right to privacy. Concerning surveillance, some of the related regulations issued by the NCC are listed below.

g. **Nigerian Communications Commission (Registration of Service Telephone Subscribers) Regulations 2011**

Part 2 of the regulation establishes the obligation to maintain a central database domiciled within the NCC for the central processing and storage of subscribers' information. Article 8 of the regulation provides for access to subscriber information on the central database by security agencies. However, it requires that a prior written request specifying the purpose of the request should be made to the NCC 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'.

h. **Nigerian Communications (Enforcement Process, etc.) Regulations 2019**

The regulation gives the NCC monitoring and enforcement powers. Regulation 8(1) prescribes that 'every licensee shall keep records of call data under the Cybercrimes Act and the consumer code of practice regulations'. It also requires every licensee to make available 'basic' and 'non-basic' information that may be required by law enforcement agency under section 146 of the Nigerian Communications Act (Regulation 8(2)(a, b)). It states that, concerning basic information, 'a written request from the relevant authority, duly signed by a police officer not below the rank of assistant commissioner of police or its equivalent' would suffice without any further assurance; while for non-basic information, a court order is necessary.

i. **Guideline for the Provision of Internet Service 2013**

The guidelines apply to all internet service providers (ISPs) in Nigeria. Paragraph 6 of the guidelines mandate ISPs to cooperate with 'all law enforcement and regulatory agencies investigating cybercrime or other illegal activity'. In addition, ISPs must provide investigating authorities with service-related information, information about users, and the content of their communication. Paragraph 8 of the guidelines mandates ISPs to retain user identification, content of user message and traffic data for twelve months. The power to intercept communication data is not subject to an independent oversight.

j. **Registration of Telephone Subscribers Regulation 2011**

The regulation makes it mandatory to for subscribers to register SIM cards with their biometric data and also establishes a central database of all registered subscribers in the country. The provision legitimises mandatory SIM registration in the country, which erodes anonymity. Article 9 of the regulation guarantees the privacy and confidentiality of subscriber information. However, the data can be accessed by security agencies if a request is made to the NCC by an officer not below the cadre of an

Assistant Commissioner of Police (art. 8). The request must specify the reason the information is required. In what appears to be a safeguard, article 10 of the regulation specifies that the release of subscribers' personal information to security agents must comply with existing law, and such a request can be refused if it constitutes a breach of the constitutional provision or any other law or is a threat to national security.

k. Lawful Interception of Communications Regulations 2019

The scope of the regulation includes the provision of a 'legal and regulatory framework for lawful interception of communications, collection and disclosure of intercepted communications in Nigeria'. It stipulates that only an authorised agency may affect the interception of communications. It gives these powers only to the Department of State Security, the Nigeria Police Force and the Office of the National Security Advisor, subject to obtaining a court warrant. The warrant to intercept can be granted when interception is the only way to access the communication data and if the 'facts alleged in the application are reasonable and persuasive enough' to provide sufficient evidence that the surveillance subject has or is about to threaten a legitimate aim (LICR art. 13(3)).

Article 9 gives the authorised agency the power to request protected or encrypted communications disclosure. Security officers have been enabled to intercept phone calls, text messages, chat messages or emails on this premise (Collins 2013). However, the authorised agency must submit an annual report of all concluded interception cases to the attorney general. The report is not made publicly available. It allows the authorised agency the liberty to store intercepted communications for the duration of its investigation. Article 10 mandates service providers to install interception capabilities that permit interception. Similarly, article 11 prohibits network providers from providing services that cannot be intercepted and monitored. An application for a warrant should include the duration, the grounds for the application, the identity of the subject of interception, and the investigating authority's identity. Article 5 makes it an offence to unlawfully intercept communication, which is consistent with the international principle of imposing safeguards against illegitimate access.

Article 7 provides for an interception with a warrant, while article 8 allows interception without a warrant. When interception is carried out without a warrant, the investigating authority must apply for a warrant to a judge of the Federal High Court within 48 hours after the interception has occurred. Where the application is not made, the interception shall terminate and be treated as unlawful. Similarly, article 13(2)(d) of the LICR provides that

where the judge rejects an application for the interception that has taken place, any information obtained before the refusal is invalid and not admissible for criminal persecution of the individual affected by it. The information extracted is valid for the investigation period and destroyed after the conclusion of the investigation. In addition, the information is confidential and can only be used for investigation and prosecution in a criminal proceeding. An interception order granted by a judge is valid for three months or a lesser period specified by the judge, after which the record can be archived for three years and destroyed afterwards.

Interestingly, article 20(1) of the LICR allows a network provider or any individual aggrieved about any interception activity to notify the NCC or make a formal application to the Federal High Court for judicial review. Unfortunately, it may be difficult for individuals to know they have been targeted for surveillance if they are not notified about it. Specifically, article 13(4) of the LICR provides that an application for a warrant shall be heard without placing the individual affected under notice.

Other laws and proposed bills

The National Security Agencies Act is another critical piece of legislation, which established the State Security Service, Defence Intelligence Agency and National Intelligence Agency, the government agencies responsible for intelligence gathering in different capacities in the country. There have also been legislative proposals to legitimise surveillance by the legislature. The Telecommunications Facilities (Lawful Interception of Information) Bill 2019 seeks to compel telecommunications service providers to enable law enforcement agents to intercept communications for national security purposes. Section 3 of the bill requires service providers to hand over intercepted communications to law enforcement agents. The provision also allows the decryption of communications. Section 13 mandates network providers to hand over subscribers' personal information to law enforcement agents. Any appeal over violation of the law goes to the minister of justice. The bill is currently at its first reading in the House of Representatives (lower federal legislature).

The Digital Rights and Freedom Bill 2019 provides for online privacy rights and defines the legal framework regarding surveillance. The bill outlines the provisions of lawful and authorised interception of communication within the digital environment. It grants the court more powers to perform oversight functions. Under the bill, surveillance is made subject to necessity and furtherance of a legitimate aim. In stemming the asymmetrical power dynamics between law enforcement and private citizens, the bill

proposes that private organisations make public the details of government requests for private citizens' data. The bill is currently awaiting the House of Representative committee report.

4. How does Nigerian surveillance law compare with that in other countries in Africa/US/EU/UK?

Some African countries have been reported to engage in arbitrary mass surveillance (Citizen Lab 2020). In addition, there are fears that several governments are procuring surveillance tools to monitor dissidents, political opponents, human rights defenders and journalists. Algeria, Botswana, Côte d'Ivoire, Egypt, Ghana, Malawi, Nigeria, Rwanda, South Africa, Tanzania, Uganda, Zambia and Zimbabwe were recently reported to have procured and deployed surveillance tools (Jili 2020). In July 2021, after a forensic investigation, the Guardian and other media outlets reported the use by some African countries such as Rwanda, Togo, and Morocco of Israeli company NSO Group's malware, Pegasus, which allows security agencies to listen to phone calls, intercept messages, and also to track individuals (Damien 2021). The malware has been reportedly used to spy on dissidents, opposition, journalists, and foreign leaders (Lynsey 2021). Although Rwandan and Moroccan governments have denied the claim (Kirchgaessner 2021, Shaquile 2021), in 2019, dissident and human rights activists from Rwanda and Morocco were privately warned by communication giant WhatsApp that they were victims of cyber-attacks designed to infiltrate their phones by an NSO Group malware (Kirchgaessner *et al.* 2019).

The pervasive practice appears to go unchallenged due to vague laws that are subject to abuse, codification of state power to conduct mass monitoring, the absence of independent oversight bodies, and weak legal frameworks and institutions. For example, in Uganda, facial recognition has been deployed to monitor protesters (Quartz Africa 2020b).

Nonetheless, there are examples of progressive practices on the continent. In South Africa, the Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA) is the primary law on surveillance. The RICA creates an oversight body and puts in place several safeguards contained under the International Principles. However, the law also omits some safeguards. The legal frameworks in South Africa and Nigeria lack safeguards on transparency. There is no statutory requirement to publish a public annual report, although in Nigeria a report is meant to be submitted to the attorney general. Both countries omit the obligation to notify individuals either before they are surveilled or at the conclusion of surveillance. Under Nigeria's Cybercrimes Act, investigating authorities can apply to the court to conduct surveillance without notifying the individual

being surveilled and there is no avenue to challenge the surveillance measure or appeal the decision. Both the RICA and LICR mandate the communication service provider to ensure their communication tools are capable of being intercepted, which is contrary to the international principle of integrity of communications and systems and could also open a floodgate for unregulated surveillance.

Both countries have a requirement to specify the category of offence before requesting a judicial directive. The TPA requires specifying the subject of surveillance in the application to the judge. There also appears to be a normative condition to establish a legitimate aim before surveillance. The South African law also has the benefit of being tested before the court. For example, in 2021 South Africa's Constitutional Court delivered a landmark judgment outlawing mass surveillance in the country. In *Amabhungane Centre for Investigative Journalism v Minister of Justice and Correctional Services (CCT 278/19)* the court held that the government should no longer conduct mass surveillance of citizens. The court also declared certain parts of the RICA unconstitutional (BusinessTech 2021). Notably, the court stated that the RICA fails to provide sufficient safeguards to preserve the right to privacy, the law did not provide adequate protection or relief for persons subjected to surveillance, and the law did not make provision for individuals subjected to surveillance to be notified after the fact, among other issues. Nevertheless, South Africa has a specific surveillance law, as recommended by the UN Draft Instrument, while in Nigeria legal surveillance provisions are located in different laws. This could be considered preferable to having contradictory legitimate aims and safeguards specified in different pieces of legislation, as in Nigeria. South Africa has a more explicit definition of tests for a judge to assess before issuing authorisation, which is not evident in all cases in the Nigerian framework. South Africa has an 'independent oversight board' as conceptualised under the International Principles. The law in South Africa also has the advantage of being challenged and tested in court by civil society in ways that have identified flaws, clarified provisions and provided enhanced privacy protections.

5. How does Nigerian surveillance law compare with the UN Draft Legal Instrument?

The UN Draft Legal Instrument on Government-led Surveillance and Privacy sets out principles and safeguards on the minimum requirements to conduct surveillance. Article 4 of the UN Draft Legal Instrument sets out the principles. A quick review of the Nigerian legal framework – including the Mutual Legal Assistance Act and the TPA – suggest appreciable adherence to the requirement for a legitimate aim, such as the interception for serious crimes. In addition, the Nigerian framework requires specifying the details to be intercepted in the application for warrant and only intercepting when there is a reasonable suspicion and interception is the only way to access the communication data, which suggests necessity. There are other additional safeguards. For example, under the LICR, the failure to obtain a warrant where it is required renders the evidence unlawful and unacceptable before the court.

An appraisal of existing Nigerian laws against other principles shows a contrasting picture for some parts. Nigeria's laws are noticeably lacking in sufficient procedural safeguards and an independent oversight mechanism of the activities of investigating authorities. The UN Draft Legal Instrument recommends that government or police officials should seek prior authorisation for surveillance from a court and that an oversight body independent of both the court and government or police be given the power to access all requests and authorisations to ensure that robust checks for the legality, necessity and proportionality of surveillance are implemented, and that notification is provided to the individuals under surveillance. Specifically, the LICR makes it mandatory not to notify the subjects of surveillance when the investigating authority is applying to the court for a warrant to intercept communication, which deprives the individuals concerned of the right to an effective remedy. Notification is essential to fight surveillance overreach. Although the LICR allows individuals who are subject to surveillance to approach the NCC or Federal High Court for judicial review if dissatisfied (LICR, art. 20), the mandatory requirement not to notify them robs them of the chance to be aware of the interception before or after the fact (LICR, art. 13(4)).

Both the TPA and LICR mandate network service providers to install tools that can enable interception capability, which is contrary to the principle of integrity of communications under the UN Draft Legal Instrument. The failure

to install the tool is punishable with a fine or withdrawal of operation license. Also, the LICR permits interception for 'investigation of crime' and fails to make a distinction or allow interception for the most severe crimes, which could allow the abuse of investigative powers. The Nigerian law also includes the notification to the regulator and the data subjects when there is a data breach.

Another principle of the UN Draft Legal Instrument is the requirement to ensure safeguards by law enforcement agencies. For example, the LICR and the Cybercrimes Act suggest that the application for a warrant should specify the subject of the interception and the grounds on which the application is being made, which is consistent with the requirement of reasonable suspicion. Under the LICR, the obligation to ensure the security of the transmission of data is placed on the network provider. The intercepting agency must ensure data are stored confidentially, which is consistent with the principle of ensuring confidentiality and integrity of communications data under the UN Draft Legal Instrument. Similarly, other laws, such as the NDPR, impose security obligations on public agencies.

Another requirement addresses intelligence sharing with other countries. The UN Draft Legal Instrument favours a regime where independent and cross-border data transfer rules are adequate. However, under the Mutual Legal Assistance Act, the attorney general, a political appointee of the government, is responsible for exercising this power in Nigeria. In addition, the LICR mandatory requirement for installation of surveillance capability and decryption of encrypted communication could pave the way for unregulated bulk data collection, contrary to one of the principles in the UN Draft Legal Instrument. Also, there are instances of the government deploying surveillance tools, as highlighted in the introduction of this report, but there is no record or evidence of a human rights impact assessment being conducted. None of the laws on surveillance in Nigeria makes it mandatory to conduct a human rights impact assessment. Finally, transparency about requests and authorisations through the publication of an annual report is only visible under the LICR. The report is meant to be submitted to the attorney general and it is not made public.

6. Does legislation provide adequate definitions of key legal terms?

Generally, not all laws define these phrases. The TPA sets out prevention of terrorism as its legitimate aim. Under some laws, such as the Mutual Legal Assistance Act and the TPA, it is a requirement to specify the purpose of interception. Similarly, these laws require that the application for an interception should include the scope and scale of communication data required. The provisions appear to prohibit mass surveillance. Also, section 45(3) of the Cybercrimes Act specifies that a warrant to decrypt data will only be issued where there is suspicion that the person named in the warrant is about to commit a crime. The exercise of the power is not reserved for the most severe crimes. The legitimate aim under the TPA is prevention of terrorism; whereas the Mutual Legal Assistance Act applies to the most severe crimes. The TPA allows intelligence gathering without a warrant where there is an emergency. However, it fails to define what constitutes an emergency and that imprecision could be abused.

Under the Implementation Framework to the NDPR, and the Nigerian constitution, the rights guaranteed can only be derogated in limited circumstances prescribed by law. The Supreme Court in the case of *Military Governor of Lagos State v. Ojukwu (2001) FWLR (Part 50) 1779,* held that:

> the Nigerian Constitution is founded on the rule of law, the primary meaning of which must be done according to the law. It also means that government should be conducted within the framework of recognised rules and principles which restricts discretionary powers.

The derogation to the right to privacy under section 45(1)(a) of the constitution specifies that it has to be 'reasonably justified in a democratic society'. Consequently, surveillance is not expected to be used arbitrarily.

7. How do legal safeguards, checks and balances, and independent oversight operate in practice?

Section 45 of the Cybercrimes Act and article 17 of the LICR require an interception application be made to a judge. However, there is no evidence to suggest if there is recourse to a court, considering that it is done without notifying the individual subject of surveillance. In many cases, the individual is only aware of surveillance if there is an arrest based on a request for communication data from a network provider or in a criminal prosecution if it becomes part of the evidence. In 2018, a journalist, Samuel Ogundipe, was arrested by the police using communication data obtained from a network service provider. Samuel's arrest is not an isolated case; the Committee to Protect Journalists profiled other cases where journalists were arrested by the police using records from their network provider (Jonathan 2020). There are also reported instances of journalists' phones, computers and other devices being seized by authorities to conduct forensic searches to establish their sources of information (Jonathan 2019). In another instance, a Twitter user that created a parody account in the name of former president Goodluck Jonathan was arrested by the police and detained for 54 days by obtaining call records from a network service provider (Sahara Reporters 2020). The pattern suggests surveillance is being used arbitrarily for just any crime at the behest of security agents, and there is a disregard for rule of law and legal safeguards.

The LICR and the Mutual Legal Assistance Act designate the attorney general as the central authority concerning international mutual assistance. The LICR specifies that surveillance data collected should not be kept longer than necessary and should be destroyed afterwards. The same regulation stipulates a limit of three years for the retention of data. Similarly, the Cybercrimes Act prescribes two years as the limit to retain traffic data, while the Guidelines for the Provision of Internet Service prescribes a limit of twelve months Arbitrary retention of data deprives people of anonymity. According to EFF (Electronic Frontier Foundation 2021):

> Government mandated data retention impacts millions of ordinary users compromising online anonymity which is crucial for whistle-blowers, investigators, journalists, and those engaging in political speech. National data retention laws are invasive, costly, and damage the right to privacy and free expression. They compel ISPs and telcos to create large databases of information about who communicates with whom via Internet or phone, the duration of the exchange, and the users' location.

The institutional mechanism to ensure checks and balances is almost non-existent. There is no independent oversight body to monitor activities of investigating authorities. The role of the Federal High Court is limited to surveillance requests brought to its attention. There is no similar provision to request an audit or to publicly publish a transparency report of authorisations and interception requests. Although the LICR makes it a requirement for law enforcement agencies to submit a report to the attorney general, there is no way to verify if this is observed in practice. The provision that seems to have paved the way for accountability, the transparency report, is meant to be presented to the attorney general, a political appointee, who is not an independent authority. It is instructive to say that Nigeria has an access to information law, the Freedom of Information Act.

There is also no obligation for organisations to publish a transparency report on the number and types of requests they get from the government. The Digital Rights and Freedom Bill makes it a requirement to publish a transparency report stating the types of request made by the government. To get an idea of the extent and types of requests made by the Nigerian government, one may look at the transparency report published by big technology companies. It is hard to independently verify the practical application of and adherence to these principles because surveillance is shrouded in secrecy (Dada and Tafida 2014). Also, the role of research and disclosures by entities selling surveillance tools has provided insights into the government's capability (Citizen Lab 2020). Finally, none of the laws makes it a requirement to conduct a human rights impact assessment before deployment of surveillance tools by the government.

8. How effective are existing laws and practices in protecting privacy and limiting surveillance?

The Nigerian court has recognised the right to privacy and data protection. Data protection rights available to individuals are contained under the NDPR. However, public authorities could use derogations in areas such as public interest, national security and investigation of crime to limit the exercise of those rights. The constitutional guarantee of the right to privacy is also limited in similar circumstances and when it would affect the rights of another individual. This is a common scenario with many regulations: they broadly provide for a right, then list wide-ranging exceptions that derogate from the right that seeks to be protected. The efficacy of existing privacy laws is affected by the inadequate regulatory framework surrounding privacy protection in Nigeria. Nigeria lacks a comprehensive data protection law and an independent data protection authority to enforce the law. The gaps in laws and practices have been consistently exploited by authorities to violate the privacy rights of Nigerian citizens, civil society and the media (Adegoke 2021).

The laws enabling surveillance impose obligations to preserve the right to privacy guaranteed under the constitution, but government agencies are known for violating this right. For example, the NITDA issued a notice of enforcement on the Nigeria Immigration Service for violating a citizen's privacy by publishing their biodata on social media platform Twitter, but they failed to issue a sanction or disclose the outcome of the investigation (Umoren 2019). Measures adopted by the government cast doubt on the intention to preserve privacy. The enactment of a law allowing the decryption of encrypted communication, the requirement on network providers to install interception capability, the requirement for mandatory registration of SIM cards for mobile devices, the forced integration of SIM registration with the national biometric identity number, and evidence of procurement of surveillance tools do not suggest the intention to preserve privacy. Surveillance is shrouded in secrecy and it is often hard to know which law is being relied upon.

However, section 26(3) of the National Identity Management Commission (NIMC) Act 2007 allows the information of an individual to 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.' The

problem with this provision is that the terminologies are not defined; and simply throwing around the defence of national security or public interest without a qualified, legitimate purpose would only occasion arbitrary restriction of citizens' rights. States must instead 'demonstrate the risk that a specific expression poses to a defined national security or public order interest' (United Nations General Assembly 2014) and show that it is in the interest of the whole nation, and not just 'the sole interest of a Government, regime or power group' (Office of the High Commissioner for Human Rights 2019).

9. Are existing surveillance practices in Nigeria 'legal, necessary and proportionate'?

The constitutional guarantee of the right to privacy can only be derogated in limited circumstances. Safeguards should ensure that any such interceptions are legal, necessary and proportionate. The comparative assessment in this report suggests that existing surveillance law and practices in Nigeria do not entirely meet the legal threshold. Although surveillance is founded in law, it is hard to know which laws enforcement agencies rely upon in practice. A case in hand is the procurement of surveillance tools by some governors in the south of the country. The tools were acquired mainly to spy on political opponents (Ogala 2016). Presumably, all of this happened outside of the law and without the authorisation of the court.

Article 13(3)(b) of the LICR specifies that a judge should only grant a warrant where 'interception of such communication is the only means of obtaining the information required' and if the 'facts alleged in the application are reasonable and persuasive enough' to provide sufficient evidence that the surveillance subject has or is about to threaten a legitimate aim. The provisions suggest the requirement of necessity. Section 39 of the Cybercrimes Act requires that interception can only be done where there is reasonable suspicion of a crime. However, tracking journalists' phones and their subsequent arrests or conducting forensic investigations on their computers does not appear to be necessary (CPJ 2019). Similarly, the retention period of data for up to two and three years under the Cybercrimes Act and the LICR, respectively, is excessive. Consequently, these extreme measures cannot be considered proportionate, but rather a violation of fundamental rights. In Nigeria, then, multiple examples of surveillance are neither legal, necessary nor proportionate. However, these failings have yet to be challenged in court.

The LICR also imposes a limit on the duration of surveillance, which should be restricted to the period of the investigation and the record should be deleted upon completion of investigation. Intercepted communication can only be used for investigation and criminal prosecution. The judge may grant a warrant for three months or for a lesser period.

10. How has surveillance law played out in court in Nigeria?

Due to the secrecy around state-sanctioned surveillance in the country, the absence of transparency about interceptions and notification of individuals under surveillance, there were no records of court decisions specifically challenging surveillance at the time of writing. However, there are number of cases that slightly impact surveillance. The Court of Appeal has recognised the right to privacy in the case of *Emerging Markets Telecommunication Services Ltd v. Godfrey Eneye (2018) LPELR-46193(CA)*. In 2013, Pan-African digital rights organisation, Paradigm Initiative, filed a freedom of information request before the Nigerian government to provide additional details about its contract with Elbit Systems to purchase surveillance tools, which was not responded to (Irene 2013). Earlier, it become public that the government awarded a US$40 million to Elbit Systems to purchase surveillance tools (Ogala 2013). Subsequently, the organisation instituted a case before the Federal High Court to mandate the government to provide more information about the contract. The court did not grant the request (Premium Times 2013).

In 2017, Paradigm Initiative filed a freedom of information request before the Ministry of Science and Technology, requesting information about the details of the proposed launch of two satellites by the National Space Development and Research Agency (NASDA) (Okunola 2017). The ministry refused to respond to the request. Consequently, the group approached the Federal High Court to direct the ministry to provide information about the satellite launch. The court granted the request of the organisation and directed the ministry to provide the information requested.[5]

In another case, Paradigm Initiative challenged the provision of section 38 of the Cybercrimes on mandatory data retention for violating the right to privacy under the constitution and other international human rights instruments Nigeria is committed to. Both the Federal High Court and the Court of Appeal ruled against the organisation. The Court of Appeal decided that the provision on data retention is necessary to assist in the detection and investigation of crime for the public good.[6] The organisation appealed the decision, and the case is currently pending at the Supreme Court at the time of writing (Paradigm Initiative 2018). Similarly, in 2019, the organisation

5 Incorporated Trustee of Paradigm Initiative for *Information Technology Development v. Ministry of Science and Technology.* FHC/CS/481/2017

6 Incorporated Trustee of Paradigm Initiative for *Information Technology Development and others v. Attorney General of the Federation.* CA/L/556/2017

sent a Freedom of Information Request to the NCC asking for information about the legal safeguards in the surveillance practices of the government after enacting the Mutual Assistance in Criminal Matters Act (Paradigm Initiative 2019). The act permitted the interception and sharing of intelligence with other countries. Also, there is an increasing number of cases going before the court founded on the violation of the right to privacy and data protection.

Regardless, there is a significant role for strategic litigation to challenge existing legal provisions that violate fundamental human rights enshrined in the constitution and international human rights norms to which Nigeria has committed. The media have a huge role in drawing attention to these laws and holding intelligence services to account. The use of the freedom of information law to test accountability and transparency could prove significant in understanding law enforcement agents' activities.

11. What is working? What gaps are there in existing policy, practice, knowledge, and capacity?

Some of the laws have provisions that comply with UN principles, which is commendable. However, the challenge has been the government's non-adherence to provisions of the law and the arbitrary use of state power. A noticeable gap in existing policies is the lack of a comprehensive framework that regulates the country's data protection and privacy space and the absence of an independent data protection authority. How then does a country without an exhaustive legal framework for data protection intend to monitor communications or guarantee a remedy for violations of the data protection right within the ambit of the law?

The country also lacks the needed political will to drive such exhaustive policies. For instance, the country's draft data protection bill was presented before the 6th National Assembly (2011–2015) without success. The 7th National Assembly passed the data protection bill in 2019, which President Muhammadu Buhari rejected. No reason was adduced publicly for the bill's rejection (Oloyede 2021). Rather than drive policies, budgetary spending on surveillance has increased in the past decade (Adegoke 2021). The enactment of a law allowing the decryption of encrypted communication, the requirement for mandatory registration of SIM cards and forced integration with a national biometric identity, and evidence of procurement of surveillance tools do not suggest the intention to preserve privacy. Also, the requirement on network providers to install interception capability is contrary to the principle of integrity of communications.

The increased introduction of surveillance technologies in the country without independent institutional oversight and a mandatory requirement to conduct a human rights impact assessment before using them makes it easy to subject citizens to unnecessary and disproportionate surveillance. In addition, safeguards such as the right to notification, right to effective remedy, an independent oversight regime for intelligence sharing and review and the right to appeal an assessment contained in international human rights instruments are also missing. Lastly, transparency about requests and authorisation is shrouded in secrecy.

12. What recommendations arise from this analysis for legislation, practice or further research?

For policymakers and legislators

- Existing laws should be reviewed to incorporate the principles espoused in the UN Draft Legal Instrument. The amendment should consider the following:
    - Mandatory notification of individuals to enable them to contest surveillance;
    - Institutionalising an independent oversight body to review decisions and intelligence sharing with third countries;
    - A mandatory requirement to conduct human rights and data protection impact assessments before deploying surveillance tools;
    - The right to appeal assessment; and
    - An obligation to notify the data protection authority when there is a data breach.
- Nigeria should enact a comprehensive data protection law.
- The Digital Rights and Freedom Bill should be passed and enacted into law.
- NCC regulations should be reviewed to enforce judicial oversight and to accommodate a mandatory publicly accessible annual report. Only a judge should determine legitimate purposes.
- Members of the legislature should pass a resolution demanding greater transparency about the activities of law enforcement agencies concerning requests for communications data. They should also exercise their supervisory powers guaranteed under the constitution to audit the affairs of law enforcement agencies.

For civil society organisations and activists

- There is a need for mode data-driven research to show the extent of the government's surveillance capability.
- There should be an increase in the use of freedom of information requests to demand accountability and transparency from public authorities on procurement and use of surveillance tools.

- There is a need to demand greater accountability and transparency from the government through constant engagement, using freedom of information law and exploring strategic litigation to clarify the law, narrow surveillance targets, and protect and safeguard citizens' rights.
- Civil society organisations should challenge intelligence services over violations of the laws or existing human rights instruments that Nigeria is a party to.
- Civil society organisations should raise public awareness concerning privacy and data protection rights. This would promote citizens' self-awareness concerning protection of their digital rights.
- There is an urgent need for strategic litigation to demand accountability and question the disregard for the provisions of existing laws. Also, vague words that could lead to abuse of power should be challenged before the courts.

For government

- The government should be transparent about its procurement of surveillance tools.
- Publication of details of interception requests made should be publicly available to promote transparency and accountability.
- The attorney general's office should serve the interests of the people instead of seeking to preserve the government that appointed it.
- Institutions should be adequately funded to carry out their statutory duties.

For researchers and academia

- It is recommended that a regulatory impact assessment should be conducted to highlight failures, gaps and what is currently working in the existing legal framework.
- There is a need to build additional capacity within Nigerian legal, civil society and academic research communities to more effectively monitor, map and analyse the existing characteristics of surveillance law and practice in Nigeria, which is a necessary precondition for defining effective legal and policy measures to improve the current situation.
- It is recommended that more research should be carried out to reveal new evidence on the tools, scale, methods and tactics the government uses to conduct surveillance.

For journalists

- Journalists should raise public awareness about the government's surveillance practices and their effects to build political pressure for changes in law and practice.
- There is a need to invest in capacity building of journalists to understand the implications of surveillance and its different manifestations to present the public with an informed perspective.
- More research needs to be done to understand the categories and volume of cases in which surveillance data are used as evidence.

References

Adegoke, A. (2020) ***'Digital Rights and Privacy in Nigeria'*** *Paradigm Initiative* (accessed 26 May 2021)

Adegoke, B. (2021) **'COVID-19, digital rights and Nigeria's emerging surveillance state'** *Global Voices* (accessed 26 May 2021)

Advox (2013) ***'Nigerian Government to Ramp up Internet Surveillance?'*** *Global Voices* (accessed 29 July 2021)

Ajayi, A. (2021) **'Insecurity: Oyo to Register Residents'**, *Peoples Gazette*, (accessed 18 September 2021)

Al Jazeera (2020) ***'Nigerian Intelligence Bought Tool to Spy on Citizens: Report'***, (accessed 12 May 2021)

Arise News (2021) ***'Nigerians Opt for VPNs Following Twitter Ban'*** (accessed 15 July 2021)

Billstrack (2016) ***'Digital Rights and Freedom Bill'*** (accessed 26 May 2021)

BusinessTech (2021) ***'South Africa's RICA Law Is Unconstitutional: Court Ruling'*** (accessed 31 July 2021)

Budget Office of the Federation (2021) ***'Budget Document'*** (accessed 12 May 2021)

Citizen Lab (2020) ***'Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles'*** (accessed 1 July 2021)

Collins, K. (2013) ***'Nigeria embarks on a mobile phone surveillance project'*** (accessed 26 May 2021)

Committee to Protect Journalists (CPJ) (2018) ***'Nigerian Journalist Jailed for Refusing to Reveal Source'*** (accessed 26 May 2021)

Dada, J. and Tafida, T. (2014) ***'Communications surveillance in a digital age'*** (accessed 11 May 2021)

Dada, J and Tafida, T. (2014) ***'Online surveillance: Public concerns ignored in Nigeria'*** Global Information Society *Watch* (accessed 1 July 2021)

Damien G. (2021) **'Morocco, Rwanda, Togo...How Involved Is Africa in 'Pegasus Gate'?'**, *The Africa Report* (accessed 28 July 2021)

Egbunike, N. and Burbidge, D. (2013) ***Nigerian Government to Ramp Up Internet Surveillance?*** (accessed 26 May 2021)

Ehiagwina, F. (2015) ***'Managing Insecurity with Biometric Engineering: An Overview of the Nigerian Experience'***, paper presented at the International Academic Conference on Globalization and Contemporary Issues: Opportunities for Sub-Sahara African Transformation & Development (accessed 4 August 2021)

Ekott, I. (2013) **'ACN Urges Nigerians to Resist Jonathan's 'Evil' $40million Internet Spy Contract'**, *Premium Times*, 29 April (accessed 11 May 2021)

Electronic Frontier Foundation (EFF) (2021) ***'Mandatory Data Retention'*** (accessed 28 July 2021)

Electronic Frontier Foundation (EFF) (2014) ***'International Principles on the Application of Human Rights to Communications Surveillance'*** (accessed 26 May 2021)

Federation of American Scientists (2021) ***'State Security Service (SSS) – Nigeria Intelligence Agencies'*** (accessed 1 July 2021)

Feldstein, S. (2019) ***'The Global Expansion of AI Surveillance'*** *Carnegie* (accessed 26 May 2021)

Guardian (2021) **'Response from NSO and Governments'** (accessed 28 July 2021)

Irene P. (2013) ***'Paradigm Initiative Nigeria Seeks Information on Surveillance Systems in Nigeria'*** *The Citizen Lab* (accessed 28 July 2021)

Iroanusi, Q. (2021) **'Nigerian Govt Moves to Control Media, Allocates N4.8bn to Monitor WhatsApp, Phone Calls'**, *Premium Times* (accessed 15 July 2021)

Jili, B. (2020) ***'Surveillance Tech in Africa Stirs Security Concerns'*** *Africa Center for Strategic Studies* (accessed 1 July 2021)

Johnson, J. (2013) ***'Scandal in Nigeria over Israeli arms firm's Internet spying contract'***, *The Electronic Intifada* (26 May 2021)

Jonathan R (2020) ***'How Nigeria's police used telecom surveillance to lure and arrest journalists'***, *Committee to Protect Journalists* (accessed 28 July 2021)

Jonathan R. (2019) '***Nigerian Military Targeted Journalists' Phones, Computers with 'Forensic Search' for Sources'*** *Committee to Protect Journalists* (accessed 28 July 2021)

Kirchgaessner, S. (2021) **'Hotel Rwanda Activist's Daughter Placed under Pegasus Surveillance'**, *The Guardian*, (accessed 29 July 2021)

Kirchgaessner, S.; Hopkins, N. and Holmes, O. (2019) **'WhatsApp 'Hack' Is Serious Rights Violation, Say Alleged Victims'**, *The Guardian*, (accessed 29 July 2021)

Lagos State Resident Registration Agency (2020) ***'Welcome!'*** (accessed 28 May 2021)

LawNigeria (2018) ***'Constitution of the Federal Republic of Nigeria 1999 (With Amendments)'*** (accessed 26 May 2021)

LawNigeria (1999) ***'Constitution of the Federal Republic of Nigeria'*** (accessed 26 May 2021)

Lynsey C. (2021) ***'Pegasus Lands in Africa'***, *Foreign Policy* (accessed 28 July 2021)

Marquis-Boire, M. (2013) ***'For Their Eyes Only: The Commercialisation of Digital Spying'*** *The Citizen Lab* (accessed 26 May 2021)

Munis, V.O. (2014) ***'CBN Introduces Bank Verification Numbers'*** *International Law Office* (accessed 26 May 2021)

Office of the High Commissioner for Human Rights (2019) ***'Surveillance and human rights – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression'*** (accessed 26 May 2021)

Ogala E. (2016) ***'Investigation: How Governors Dickson, Okowa Spend Billions on High Tech Spying on Opponents, Others'***, *Premium Times,* (accessed 28 July 2021)

Ogala, E. (2013) **'Jonathan awards a $40million contract to an Israeli company to monitor computer, Internet communication by Nigerians'**, *Premium Times,* (accessed 26 May 2021)

Okunola, F. (2017) ***'Digital Rights Organization Gets Boost in Suit against the Science & Tech Ministry'*** *Pulse* (accessed 28 July 2021)

Oloyede R. (2021) ***'Legislative prediction for privacy and data protection in Nigeria'*** (accessed 15 July 2021)

Oloyede, R. (2020) ***'A comparative analysis between the Digital Rights and Freedom Bill and other legislation in Nigeria'*** (accessed 26 May 2021)

Paradigm Initiative (2019) ***'Paradigm Initiative sends FoI Request to NCC on Nigeria's New Surveillance Provisions'*** (accessed 28 July 2021)

Paradigm Initiative (2018) ***Legal Battle Over Cybercrimes Act Moves to the Supreme Court*** (accessed 28 July 2021)

Paradigm Initiative and Privacy International (2018) ***'Stakeholder Report Universal Periodic Review 31st Session'*** (accessed 26 May 2021)

Premium Times (2013) **'Judge Asks National Assembly to Restrict Application of FOI Act'** (accessed 28 July 2021)

Privacy International (2014) ***'Nigerian Government under Fire for Expansion of Surveillance Programs***' (accessed 3 June 2021)

Quartz Africa (2020a) ***Nigeria, Kenya Use Israeli Surveillance Tool to Listen to Calls*** (accessed 1 July 2021)

QED (2018) ***'We Now Use Cameras to Track Vehicles in Lagos'*** (accessed 26 May 2021)

Quartz Africa (2020b) ***'Uganda Uses China's Huawei Facial Recognition to Snare Protesters'*** (accessed 1 July 2021)

RightDocs (2017) ***'The right to privacy in the digital age'*** (accessed 26 May 2021)

Rozen, J. (2019) ***'Nigerian Military Targeted Journalists' Phones, Computers with 'Forensic Search' for Sources,*** Committee to Protect Journalists (accessed 20 May 2021)

Sahara Reporters (2020) ***'How Ex-Nigerian President, Goodluck Jonathan, Got University Student Who Created Parody Twitter Account in His Name Detained for 54 Days'*** (accessed 28 July 2021)

Salau, G. and Akomolafe, J. (2021) **'Lagos Kits LASTMA, VIO, Others with Body Cameras to Check Abuse, Crime'**, *The Guardian* (accessed 28 May 2021)

Sesan, G.; Soremi, B. and Oluwafemi, B. (2013) ***'Economic Cost of Cybercrime in Nigeria'*** (accessed 26 May 2021)

Shaquile G. (2021) **'Pegasus Project: Morocco's Public Prosecutor Orders Probe into 'False Allegations''**, *Morocco World News*, (accessed 29 July 2021)

The New York Times (2021) **'Millions Flock to Telegram and Signal as Fears Grow over Big Tech'** (accessed 15 July 2021)

Tukur, S. (2017) **'Shocking Revelation: 100,000 Killed, Two Million Displaced by Boko Haram Insurgency, Borno Governor Says'**, *Premium Times* (accessed 11 May 2021)

TVC News (2020) ***'Kano Installs 24/7 CCTV Surveillance Cameras to Curb Crime'***, (accessed June 30)

Umoren, B. (2019) **'NITDA commences investigation on alleged breach of NDPR'**, *Today.ng* (accessed 26 May 2021)

United Nations General Assembly (2014) ***'The right to privacy in the digital age'*** (accessed 26 May 2021)

United Nations General Assembly (2016) ***'Oral Revisions of June 30'*** (accessed 26 May 2021)