PRIVACY, FREEDOM OF EXPRESSION AND SURVEILLANCE IN NIGERIA: NAVIGATING THE MURKY WATERS

Oghomwen Rita Ohiro,
Lecturer, LL.B, LLM, PhD (in view),
Department of Public Law, Faculty of Law, University of Benin, Email: oghomwen.igbinedion@uniben.edu, Telephone: +2347062368221

Abstract
In Nigeria, balancing national security with fundamental rights like privacy and freedomof expression remains a complex challenge. The existing legal framework for surveillancelacks transparency and potentially falls short of international standards, raising concerns about its impact on fundamental rights. This paper delves into this intricate relationship, examining how surveillance practices intersect with the right to privacy and freedom of expression in Nigeria. Through a doctrinal research methodology, it criticallyanalyses the national framework against internationally recognised standards, highlighting discrepancies and their consequences. The analysis reveals concerning gaps, including unclear legal justifications for surveillance, insufficient oversight mechanisms, and potential for discriminatory targeting. These shortcomings expose individuals, particularly vulnerable groups like journalists and activists, to risks of unwarranted surveillance, self-censorship, and privacy violations. By shedding light on these critical challenges, this article aims to contribute to the ongoing discourse on reforming Nigeria's legal framework for surveillance. Such reforms, aligned with international standards, are essential to ensure legitimate and accountable surveillancepractices that respect and uphold fundamental rights. The findings of this paper underscore the need for thoughtful legal reforms and policy measures to navigate the challenges posed by surveillance technologies while upholding democratic values and individual rights in the unique context of Nigeria's socio-political landscape.

Keywords: Surveillance, Privacy, Freedom of Expression, Legal Framework, self-censorship

Introduction
According to a recent study, Nigeria has been identified as the foremost purchaser of surveillance technology contracts in Africa.[1] The country reportedly spends hundreds ofmillions of dollars annually on such contracts, with at least US$2.7bn spent on known contracts between 2013 and 2022.[2] These findings have important implications for the use of surveillance technology in the region, as well as the ethical and legal considerations

1 T. Robert and others, *Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia* (2023, Institute of Development Research) 5 Nigerian national and state governments have acquired multiple spyware technologies such as FinFisher (UK/Germany), Circles (Israel), andFiber Optic Landing Solution to snoop on calls, texts, and phone locations, totalling over US$18m

2 Ibid, 5

surrounding its implementation.[3] For instance, the requirement for mandatory biometric registration in Nigeria raises concern.

The imperative for Nigerian citizens to undergo compulsory biometric registration for theacquisition of mobile phone SIM cards, bank accounts, and national ID engenders a formidable apparatus, endowing the state with the latent capability to monitor citizens' real-time location, financial transactions, and communication.[4] It is submitted that this pervasive surveillance regime raises profound concerns about the erosion of individual privacy and autonomy within the Nigerian socio-political landscape.

Nigeria emerges as a top purchaser of all major surveillance technologies studied, rangingfrom internet and mobile interception to social media monitoring, biometric ID data, andthe "safe city" surveillance of citizens in public areas.[5] Furthermore, the study indicates that the Nigerian government authorizes significantly more agencies to conduct surveillance than other nations surveyed and has established agreements with the leadingsurveillance technology vendors based in the United States, China, the European Union,the United Kingdom, and Israel.[6]

In recent years, studies have shown that self-censorship has increased in Nigeria following the disclosure of the expansive surveillance and interception capabilities wielded by Nigerian security services.[7] The surge in self-censorship observed in Nigeriain recent years, as indicated by studies, holds significant implications for the country. Therevelation of the extensive surveillance and interception capabilities of Nigerian securityservices has likely contributed to a climate where individuals, including journalists and citizens, feel compelled to restrain their expressions and limit their discourse.[8] This trendcan cause fear, potentially stifle free speech, hinder open dialogue, and impede the free flow of information, thereby impacting democratic principles and the robust exchange ofideas within Nigerian society.[9] Moreover, heightened self-censorship may contribute to

---

3 Ibid

4 Ibid, 18

5 Ibid, 18-19

6 Ibid, 6,

7 Freedom House, 'Nigeria: Freedom on the Net 2021 Country Report' (2021, July 6) <https://freedomhouse.org/ country/nigeria/freedom-net/2021> accessed 2 February 2024; F. O. Anyim-Ben and A. Itumo and A. Benjamin 'Challenges of Shrinking Civic Space and the Path towards Sustainable Democracy in Nigeria: Lessons from thePresident Muhammadu Buhari Administration' *African Journal of Politics and Administrative Studies (AJPAS)* (2023) 16(2), 8

8 A. Kabir and K. Adebanjo 'How Digital Surveillance Threatens Press Freedom in Nigeria, West African Countries' <https://www.thecable.ng/how-digital-surveillance-threatens-press-freedom-in-west-africa> accessed9 February 2024

9 UN Human Rights Office of the High Commissioner, 'Use of Spyware to Surveil Journalists and Human Rights Defenders Statement by UN High Commissioner for Human Rights Michelle Bachelet' <https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un- high-commissioner> accessed 9 February 2024

a chilling effect on civic participation, limiting the diversity of voices and perspectives essential for a vibrant and democratic public discourse.[10]

This article aims to analyse the impact of surveillance on the rights to privacy and freedom of expression in Nigeria. This paper is divided into various parts. The first section deals with the definition of the various concepts that run through the work. The second discusses the legal framework governing the right to privacy and freedom of expression. The third section outlines the legal framework governing surveillance. The fourth section examines the impact of surveillance on privacy and freedom of expression.

Conceptual Framework

Lyon defines surveillance as 'any collection and processing of personal data, whether identifiable or not, to influence or manage those whose data have been garnered.'[11] Thereare two aspects of this definition, data collection and processing, influence, and management. This means that surveillance involves collecting, analysing, and using datato influence and manage individuals. The Nigeria Data Protection Regulation (NDPR) broadly defines personal data, encompassing any information that can directly or indirectly identify a specific individual.[12] Surveillance entails not just collecting but alsoprocessing individuals' personal data to exercise some form of influence or control overthem. It is the power dynamics inherent in surveillance that raise ethical concerns about privacy, autonomy, and freedom of expression.[13]

Direct awareness of surveillance induces profound discomfort in an individual, it can also prompt alterations in their behaviour.[14] According to Solove, while casual observation ineveryday life often goes unnoticed and unchallenged, systematic, and pervasive surveillance by individuals or the government presents distinct and concerning harms.[15] While we may tolerate occasional unwanted glances or overhearing snippets of conversation, continuous monitoring raises significant red flags.[16] The chilling effect of surveillance on expression and behaviour simply means a situation where individuals refrain from expressing unpopular opinions or engaging in sensitive activities for fear ofrepercussions due to constant awareness of being watched leading to self-censorship.[17]

The definition of privacy remains a contested concept, lacking a definitive and universallyaccepted characterization. Solove contends that the notion of privacy is in disarray,

[10] Anyim-Ben and Itumo and Benjamin 'Challenges of Shrinking Civic Space and the Path towards Sustainable Democracy in Nigeria' (n.) 5; M. Clark and A Grech 'Journalists Under Pressure Unwarranted Interference, Fearand Self-Censorship In Europe' (Council of Europe, 2017) 19

[11] D. Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001), 2

[12] Nigeria Data Protection Regulation 2019, art.1.3

[13] C Rentmeester, 'Kant's Ethics in the Age of Online Surveillance: An Appeal to Autonomy' in L. Samuelsson and others (eds.) Everyday Life in the Culture of Surveillance (Nordicom, University of Gothenburg, 2023) 187

[14] D. J. Solove, 'A Taxonomy of Privacy' *University of Pennsylvania Law Review* (2006) 154(3) 493

[15] Ibid, 493

[16] ibid

[17] J. Kang, 'Information Privacy in Cyberspace Transactions' *Stanford Law Review* (1998) 50(4) 1193-1294

further highlighting the complexity and ambiguity surrounding the concept.[18] Within the multifaceted discourse surrounding privacy, the control-based perspective occupies a prominent position. As articulated by Westin this approach posits privacy as the individual's right to manage their personal information and determine how and to what degree it is shared with others. This emphasis on individual autonomy in managing personal information resonates deeply in a modern landscape increasingly permeated bydata collection and dissemination. Critics argue that its singular focus on informational privacy risks disregarding equally fundamental aspects of the concept, power dynamics and the potential for privacy harms beyond mere data access.[19] Privacy has also been defined as the degree to which human information is neither known nor used.[20]

Without delving into the debate of what privacy entails, this work attempts to describe privacy in the context of the impact of surveillance on privacy and freedom of expression.Privacy, under the shadow of surveillance, becomes the ability to exist without pervasivemonitoring and data collection practices that could be used to limit free expression, target,or discriminate against individuals, and undermine personal autonomy.[21] It becomes a right actively fought for in an environment where transparency, accountability, and ethical frameworks for data usage are crucial safeguards.

Freedom of expression also lacks a precise definition, but there are three main justifications why free expression should get special protection, they are the search for the truth, democratic self-government, and human autonomy.[22] Universal Declaration ofHuman Rights Article 19 guarantees the right to freedom of opinion and expression.[23] Itdefines the right to include includes freedom to hold opinions without interference and toseek, receive and impart information and ideas through any media and regardless of frontiers.

Surveillance, a double-edged sword, offers potential benefits like deterring crime and safeguarding society.[24] However, unfettered monitoring risks chilling free expression,

---

[18] Solove, 'A Taxonomy of Privacy' (n.14) 477

[19] H. Nissenbaum 'Privacy in Context Technology, Policy, and the Integrity of Social Life' (Stanford University Press, 2010); D. J. Solove, 'A Taxonomy of Privacy' *University of Pennsylvania Law Review* (2006) 154(3) 493;
A. L. ALLEN, *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability* (Rowman & Littlefield Publishers 2003)

[20] N. Richards, *Why Privacy Matters,* (Oxford University Press, 2022) 21

[21] This definition draws upon and integrates key concepts from various sources and discussions surrounding privacyand its challenges in the context of surveillance. Richards, *Why Privacy Matters*, (n.) in which the author discussesthe multi-faceted nature of privacy and its importance in contemporary society.
D. J. Solove, *Understanding Privacy*, (Havard University Press 2008) where Solove explores the "chilling effect" of surveillance on freedom of expression and individual autonomy. S. Zuboff, *The Age of Surveillance Capitalism:The Fight for a Human Future at the Frontier of Power*, (PublicAffairs, 2019) which critiques the pervasiveness of data collection and its potential for discrimination and social control.

[22] Richards, *Why Privacy Matters,* (n.20) 21; M. Amos and J. Harrison and L. Woods, 'Introduction: Freedom of Expression and the Media' in M. Amos and J. Harrison and L. Woods, (eds.) *Freedom of Expression and the Media* (Martinus Nijhoff, 2012) 1

[23] Universal Declaration of Human Rights, adopted 10 December 1948, A/RES/3/3, art. 19

[24] Solove, 'A Taxonomy of Privacy' (n.14)494

perpetuating discrimination, and eroding privacy.[25] Navigating these murky waters necessitates acknowledging both surveillance's potential and its pitfalls, aiming for a framework that prioritizes both security and individual liberties.

Theoretical Framework

1. Social Control Theory

Social control theory posits that societies establish and enforce norms and rules to maintain order and limit deviant behaviour.[26] Surveillance acts as a mechanism of socialcontrol, allowing authorities to monitor and potentially sanction individuals deemed threats to societal stability. In the Nigerian context, social control theory can be used to demonstrate how surveillance practices target specific groups perceived as challenging the status quo, like journalists or activists. This theory highlights the potential for surveillance to stifle dissent and restrict the free flow of information. The theory argues that social control is not applied equally across society.[27] Surveillance practices can exacerbate existing inequalities by disproportionately targeting specific groups, like minorities, youth, or politically dissenting individuals.[28] This selective targeting can create a chilling effect on freedom of expression for these groups. The subsequent sectionof this work shows how certain provisions of the Cybercrime Act 2015 of Nigeria have been used to prosecute journalists.[29]

2. Foucauldian Power-Knowledge Theory

This theory explores how power operates through the production and control of knowledge.[30] Foucault's power-knowledge theory explores the intricate relationship between power, knowledge, and discipline in society.[31] Knowledge is not neutral; it carries power and shapes how we understand and interpret the world.[32] Those who control knowledge production and dissemination (experts, authorities) hold significant power over others.[33] Power controls existing knowledge, it also actively produces new knowledge by defining what is knowable, establishing research agendas, and silencing certain narratives.[34] Foucault uses the metaphor of the "Panopticon," a prison design where inmates are constantly seen but cannot see the observer.[35] This symbolizes how individuals internalize the gaze of power, self-regulating their behaviour based on

---

25 ibid

26 D. Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford UniversityPress, 2001)

27 Edwin Lemert, *Social Pathology* (McGraw-Hill, 1951)

28 ibid

29 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Laws of Federation of Nigeria) and The Terrorism (Prevention and Prohibition) Act 2022 Federal Republic of Nigeria Official Gazette No.91 Vol. 109 (16 May 2022)

30 M. Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage Books, 1995)

31 Ibid

32 Ibid, 27-29

33 Ibid

34 ibid

35 Foucault, *Discipline and Punish: The Birth of the Prison*, (n.30) 197

perceived surveillance, even if they are not actively monitored. It is the ever-growing knowledge of the behaviour of the observed that makes them to be divided in prison basedon the disposition they revealed.[36]

Applying these theories to the Nigerian context, this paper is going to explore how surveillance practices generate knowledge about citizens, potentially used for categorization, control, and manipulation. How the state holds power through their control over data collection and analysis and how individuals may self-censor and limit their expression due to perceived surveillance, creating a chilling effect.

Legal Frameworks Governing the Right to Privacy and Freedom of Expression in Nigeria

In its March 23, 2017, Resolution on Digital-Age Privacy Rights, the United Nations Human Rights Council urged all states to reassess their procedures, practices, and legislation related to communication surveillance, interception, and personal data collection, including mass surveillance.[37] The aim is to safeguard the right to privacy andeffectively fulfil international human rights obligations. Ensuring privacy is a fundamental human right, as affirmed by various international human rights instruments.[38] In Nigeria, Section 37 of the 1999 Constitution[39] provides that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is at this moment guaranteed and protected.' Other than this provision, no specific dedicated legislation specifies the manifestation or detailing the facets of theright to privacy."[40] It has been submitted that the right to privacy is vital in safeguardinghuman dignity and constitutes a foundational element of any democratic society. Furthermore, it lends support to and fortifies other rights, including but not limited to freedom of expression, information, and association.[41]

A data protection law has been enacted in Nigeria which contains some significant provisions.[42] Noteworthy is the creation of the Nigerian Data Protection Commission, along with a provision emphasizing the precedence of the Act over any sector-specific legislation on data privacy in Nigeria. The Act also outlines mechanisms for enforcing compliance and establishing accountability, which entail imposing penalties for non-

[36] Ibid, 126

[37] 'The Right to Privacy in the Digital Age' UN Human Rights Council Resolution, A/HRC/RES/34/7 (23 March 2017) <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/34/7> accessed 30 January 2024

[38] Universal Declaration of Human Rights, 10 December 1948, United Nations General Assembly ratified by Nigeriain 1993, art. 12, the International Covenant on Civil Political Rights (ICCPR), U.N. General Assembly Resolution 2200A (XXI) of 16th Dec. 1966; in force 23rd March 1976, art. 17, the European Convention on Human Rights and Fundamental Freedoms (ECHR) European Treaty Series No. 5; opened for signature 4th Nov. 1950; in force3rd Sept. 1953, art.8 among others.

[39] Constitution of the Federal Republic of Nigeria 1999 (as amended), Act No.24, 5 May 1999

[40] I. S. Nwankwo, 'Information Privacy in Nigeria' in A. B. Makuililo, *African Data Privacy Laws: Law Governance and Technology Series*, (Springer, 2016) 45

[41] The Right to Privacy in Nigeria, Stakeholder Report Universal Periodic Review 31st Session - Nigeria, 4

[42] The Nigeria Data Protection Act 2023 Federal Republic of Nigeria Official Gazette No.119 Vol. 110 (1 July 2023),for example, the provision for legitimate interest assessment in the NDPA 2023, s.23(1) among others

compliance.[43] It is submitted that the enactment of Nigeria's Data Protection Act 2023 signifies a significant step toward safeguarding the right to privacy. Notably, the establishment of the Nigerian Data Protection Commission is a pivotal provision, ensuring a centralized body for overseeing data protection matters. Emphasizing the Act'sprecedence over other sector-specific legislation on data privacy underscores its comprehensive nature, bolstering the overall protection of individuals' privacy rights in Nigeria. Furthermore, the inclusion of robust enforcement mechanisms and penalties for non-compliance enhances accountability, fostering a regulatory environment that activelyupholds and safeguards the right to privacy in the country.

Article 19(2) of the International Covenant on Civil Political Rights (ICCPR) provides that 'everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or print, in the form of art, or through any other media of his choice.' Article 19 (3) of the ICCPR provides that any restriction on the right to freedom of expression any restriction must be provided by law and necessary for the respect of the rights or reputations of others, the protection of national security or of public order, or public health or morals to be legitimate.

The right to freedom of expression is guaranteed under Section 39 of the 1999 Constitution of Nigeria (as amended), which provides: "Every person shall be entitled tofreedom of expression, including freedom to hold opinions and to receive and impart information without interference …" Significantly, the implementation of the Freedom of Information Act (2011) in Nigeria has bolstered the exercise of the right to access information, thereby reinforcing individuals' rights to opinion and expression.[44]

Legal Framework Governing Surveillance

Surveillance is defined as 'any collection and processing of personal data, whether identifiable or not, to influence or manage those whose data have been garnered.'[45] Underseveral international human rights instruments, actions impinging upon the right to privacy, such as surveillance and censorship, find justification solely when they are prescribed by law, deemed necessary for a legitimate objective, and proportionate to thepursued aim.[46] Article 29(2) of the Universal Declaration of Human Rights (UDHR) stipulates that in the exercise of rights and freedoms, individuals should be subject only to limitations as established by law to ensure due recognition and respect for the rights and freedoms of others. These limitations should also meet the just requirements of morality, public order, and the general welfare within a democratic society.

---

43 ibid, part X

44 Office of the United Nations High Commissioner for Human Rights 'Nigeria' <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/Nigeria.docx> accessed 30 January 2024

45 D. Lyon, *Surveillance Society: Monitoring Everyday Life* (OpenUniversity Press, 2001), 2

46 Universal Declaration of Human Rights, art 29; Hum

Article 17(1) of the International Covenant on Civil and Political Rights (ICCPR) guarantees the right to privacy. This right includes the gathering of domestic data by a state regarding an individual if such collection qualifies as 'interference'[47] Article 17(2) of the ICCPR guarantees protection against unjust and random interference or attacks onthe right to privacy. Nigeria is a signatory to the International Covenant on Civil and Political Rights (ICCPR), it ratified the covenant on July 29, 1993.[48] By Article 17 of theICCPR, Nigeria is required to enact laws and implement additional measures to always preserve people's rights to privacy and to prohibit any type of interference with such rights.[49]

The UN Draft Legal Instrument on Government-led Surveillance and Privacy outlines principles and safeguards regarding the minimum standards for conducting surveillance.
[50] Article 3 of the instrument establishes fundamental conditions for government surveillance, including that surveillance activities must be conducted by designated law enforcement or intelligence agencies as stipulated by a clearly defined law, which must be made accessible to the public. [51]

Other prerequisites include that surveillance laws must serve the objectives of crime prevention, investigation, detection, or prosecution, enhancing public safety, and safeguarding state security.[52] Additionally, these laws must incorporate sufficient safeguards against misuse, such as legislative supervision, pre-authorization by an entity entirely separate from the executive and legislative branches, operational oversight independent from the authorizing entity and government branches, cross-institutional whistleblower mechanisms, and regular reporting by oversight bodies at a minimum. [53]

The Draft instrument stipulates that surveillance should only occur for a clearly defined,legitimate purpose and in response to a legitimate need.[54] Authorization for surveillancemust be granted by legislation that upholds and defends fundamental human rights principles.[55] Surveillance activities must be deemed necessary and proportionate, utilising the least intrusive methods feasible.[56] Any legislation allowing monitoring must also

---

47 A. Deeks, 'An International Legal Framework for Surveillance' *Virginia Journal of International Law* [2015] 55(2) 305

48 United Nations Human Rights Treaty Bodies 'UN Treaty Body Database' <https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR&Lang=en> accessed 8 February 2024

49 Office of the United Nations High Commissioner for Human Rights ICCPR General Comment No. 16: Article 17(Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation (Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988

50 UN Privacy Rapporteur, 'The United Nations Draft Legal Instrument on Government-led Surveillance and Privacy'. <https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf> accessed January 30, 2024

51 ibid, art.3(1) and (2)

52 ibid, art.3(3)

53 ibid, art.3(7)

54 ibid, art.3(9)

55 ibid, art.3(4)

56 ibid

include clear and effective procedural remedies for individuals whose rights may have been infringed.[57] States should establish and implement mechanisms that guarantee accountability for and transparency regarding government requests for surveillance dataand non-surveillance data.[58]

There is also the International Principles on the Application of Human Rights to Communications Surveillance.[59] This instrument provides that the conduct of surveillance by a state must be consistent with the principles of legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, the integrity of communications and systems,safeguards for international cooperation and safeguards against illegitimate access.[60]

Nigeria has made efforts to implement the international principles governing surveillancethrough various laws and policies governing surveillance activities. In safeguarding the public interest, particularly in matters of national security, limitations on the right to privacy may be deemed permissible under Section 45 of the 1999 Constitution of Nigeria.Nigeria has implemented legislation that grants the State authority to engage in electronicsurveillance and intercept private communications. [61] For instance, there is the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.[62]

Under the Act, service providers in Nigeria are required to keep and store all traffic data and subscriber information as directed by the authority responsible for communications services, for a period of up to two years.[63] Service providers are required to implement suitable measures to protect the privacy of the data they collect, handle or retrieve.[64] TheAct requires service providers to at the request of any law enforcement agency, preserve, hold, or retain any traffic data, or release any information required to be kept under the Act.[65] The Cybercrime Act stipulates that data retained, processed, or retrieved can onlybe utilized for lawful purposes outlined in the Act, any other applicable law, or by a court order.[66] The Cybercrime Act mandates respect for an individual's constitutional right to privacy, requiring the application of suitable safeguards to guarantee the confidentiality of the data.[67]

---

57 ibid, art.3(11)
58 ibid, art.4(2)
59 International Principles on the Application of Human Rights to Communications Surveillance <https://www.eff.org/files/necessaryandproportionatefinal.pdf> accessed 6 July 2023
60 ibid
61 Some of these laws include Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Laws of Federation of Nigeria)and The Terrorism (Prevention and Prohibition) Act 2022 Federal Republic of Nigeria Official Gazette No.91 Vol. 109 (16 May 2022)
62 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015
63 Cybercrimes Act 2015, s.38 (1)
64 ibid, s.38 (5)
65 ibid, s.38 (2) and (3)
66 Cybercrimes Act 2015, s.38 (4).
67 Cybercrimes Act 2015, s.38 (5).

Section 24 of the Cybercrime Act states that intentionally sending or causing to be sent grossly offensive, pornographic, or menacing content through computer systems or networks is an offence. It also covers knowingly sending false messages to cause annoyance, inconvenience, or harm to others. Offenders can face a fine of up to N7,000,000.00, imprisonment for up to 3 years, or both. Section 26 Cybercrime Act prohibits various actions conducted through computer systems or networks with the intentto spread racist or xenophobic material or to threaten, insult, or distribute material that denies or justifies genocide or crimes against humanity. Offenders can face imprisonmentfor up to 5 years, a fine of up to N10,000,000.00, or both upon conviction. These provisions could potentially be misused to punish legitimate expression if they are appliedtoo broadly or if there is a subjective interpretation of what constitutes 'racist or xenophobic material,' 'threats.' 'insults,' or 'material which denies or justifies acts constituting genocide or crimes against humanity.'

In fact, concerns have been raised that since its adoption, Nigeria's 2015 cybercrime act has been repeatedly used against journalists for their reporting.[68] Many argue that these provisions of the Cybercrimes Act of 2015 are a violation of the right to freedom of expression entrenched in the Nigerian Constitution. Scholars express growing concern about the Cybercrimes Act, particularly its definition of 'Cyberstalking,' and its potentialimpact on constitutionally protected rights such as freedom of expression and freedom ofthe press, as outlined in Section 39 of the 1999 Constitution of Nigeria, (as amended).[69] In *Solomon Okedara v A.G. Federation*,[70] the Appellant contended that what constitutesan offence under the Cybercrimes Act was not clearly defined and that no limit of actionsor omissions is set out in the section.[71] The Appellant argued that the provisions of the section are unclear, undefined, ambiguous and capable of subjective interpretations.[72] Thecourt upheld the constitutionality of Section 24 of the Cybercrime Act holding that the provision is quite clear and defined.[73] The Court went further to hold that the provision does not threaten the right to freedom of expression under Section 39 of the Constitution and was within the permissible restrictions pursuant to Section 45 of the Constitution.[74]

---

68 Committee to Protect Journalists, 'Journalist Arrested, Charged under Cybercrime Law in Nigeria,"
< https://cpj.org/2019/03/journalist-arrested-charged-under-cybercrime-la….> accessed 7 February 2024, P. Nkanga 'How Nigeria's Cybercrime Law is being used to Try to Muzzle the Press' Committee to Protect Journalists, <https://cpj.org/2016/09/how-nigerias-cybercrime-law-is-being-used-to-try-t/> accessed 7 February 2024, Committee to Protect Journalists, 'Journalist arrested, charged under cybercrime law in Nigeria' Committee to Protect Journalists, <https://cpj.org/2019/03/journalist-arrested-charged-under-cybercrime- la….>accessed 7 February 2024

69 E. Odeh, 'Cybercrime Act and Freedom of the Press in Nigeria.' <https://ijsser.org/2022files/ijsser07128.pdf> accessed 8 February 2024; E. I. Amah and K. M. Mbam: Domestic Regulation of the Cyberspace: An Appraisal of the Impact of the Nigerian Cybercrime Act on the Rights to Freedom of Expression and Privacy Guaranteed under the Nigerian Law, *African Journal of Law and Human Rights* (2023) 7 (1) 18-24

70 (CA/L/174/18, Lagos Judicial Decision, 28 February 2019,)

71 Ibid, 6

72 Ibid, 7

73 Ibid, 28

74 Ibid, 28-29

In *Incorporated Trustees of Paradigm Initiative for Reformation Technology Development & 2 ors v. AG Federation & 2 ors*[75], the Appellants contended that Section24 of the Cybercrimes Act was illegal, unconstitutional, and violated their fundamental rights to freedom of expression and the press guaranteed by Section 39 of the 1999 Constitution and Article 9 of the African Charter on Human and People's Rights (Ratification and Enforcement) Act.[76] The court did not agree with the Appellants' submissions on the unconstitutionality of the sections.[77]

There is also the Terrorism (Prevention and Prohibition) Act 2022.[78] The law allows law enforcement agencies to intercept information to prevent terrorism or detect crimes related to the preparation or prosecution of offenders.[79] There is also the Lawful Interception of Communications Regulations 2019 which permits only authorised agencies to lawfully intercept communications.[80] Within the legal framework for surveillance in Nigeria, there are sufficient provisions to indicate that intrusion on the right to data privacy must be for a legitimate aim such as national security.[81] Although the laws provide for the requirement of applying for warrants before processing personaldata for national security, there are, however, no sufficient provisions in the laws establishing any guidelines for the courts to follow when deciding whether to grant such warrants. However, it may be argued that the requirement for warrants acts as a check onstate power and the specifics of court decision-making should be at the discretion of judges.

It has been proposed that amendments to the Cybercrime Act should entail conferring judicial authority to determine the permissibility of regulatory agencies accessing privatecitizen information.[82] Such amendments would necessitate regulatory bodies to demonstrate sufficient cause before the court for accessing such private information.

There is the Lawful Interception of Communications Regulation 2019 which provides a 'legal and regulatory framework for lawful interception of communications, collection, and disclosure of intercepted communications in Nigeria.'[83] In the Nigerian context, it has been observed that the Lawful Interception of Communications Regulation 2019 failsto incorporate provisions for post-surveillance notification to subjects. This inadequacy,

---

75 (CA/L/556/2017, Lagos Judicial Division, 1 June 2018)

76 Ibid, 2

77 Ibid, 34

78 The Terrorism (Prevention and Prohibition) Act 2022 Federal Republic of Nigeria Official Gazette No.91 Vol. 109(16 May 2022)

79 The Terrorism (Prevention and Prohibition) Act 2022, s.68(1)

80 Lawful Interception of Communications Regulations 2019 Federal Republic of Nigeria Official Gazette No.12 Vol.106 (23 January 2019) (hereafter referred to as LICR 2019), reg. 4

81 CFRN 1999, s.45

82 E. I. Amah and K. M. Mbam: Domestic Regulation of the Cyberspace: An Appraisal of the Impact of the Nigerian Cybercrime Act on the Rights to Freedom of Expression and Privacy Guaranteed under the Nigerian Law, *African Journal of Law and Human Rights* (2023) 7 (1), 23

83 Lawful Interception of Communications Regulation, Federal Republic of Nigeria Official Gazette No. 12 Lagos 23rd January 2019, Vol. 106 Government Notice No. 23, reg. 1

in turn, leads to a consequential deprivation of the right to an effective remedy in the event of unlawful surveillance.

There are no provisions in the laws to ensure that interference with the right to privacy complies with the principles of necessity and proportionality. Furthermore, there is no provision for independent oversight mechanisms. According to Oloyede, the absence of a robust institutional mechanism designed to ensure checks and balances in compliance with Nigeria's surveillance laws is a major concern.[84] Apart from the courts, there is no independent oversight body to monitor compliance with the law; Oloyede observes that the role of the Federal High Court is limited to surveillance requests brought to its attention.[85] Furthermore, it has been noted that none of the existing laws mandates the conduct of a human rights impact assessment before the deployment of surveillance toolsby the government.[86] This raises questions about the adequacy of the existing legal framework in safeguarding the fundamental rights and freedoms of Nigerian citizens in the context of government surveillance.

It is submitted that the absence of provisions in the laws to ensure that interference with the right to privacy complies with the principles of necessity and proportionality, and thelack of independent oversight mechanisms, have significant implications in the context of state surveillance in Nigeria. From 2014 to 2023, the national government authorized a cumulative budget allocation exceeding N336 billion (US$733 million) for the NationalSecurity Adviser (NSA), the Directorate of State Security Services (DSSS), and the National Intelligence Agency (NIA).[87] It is worth noting that in Nigeria, there exist several policies that facilitate the mass collection of personal data. These policies include mandatory registration for the National Identification Number (NIN) and Bank Verification Number (BVN), as well as the linking of Subscriber Identification Module (SIM) cards to the NIN.[88]

The Nigerian Communications Commission (NCC) is required by Regulation 4 of the 2011 Registration of Telephone Subscribers Regulations to establish and manage a Central Database containing comprehensive information on registered subscribers.[89] Users of mobile phones are required to give their consent for the collection and registration of their fingerprints and a biometric map of their faces on their SIM cards to

---

84 R. Oloyede 'Surveillance Law in Africa: A Review of Six Countries. Nigeria Country Report' in T. Roberts,
*Surveillance Law in Africa: A Review of Six Countries (*Institute of Development Studies, 2021) 119

85 Ibid, 122

86 Ibid, 119

87 Budget Office of the Federation, 'Budget Documents'
<https://www.budgetoffice.gov.ng/index.php/ resources/ internal-resources/budget-documents?layout=columns> accessed 2 February 2024

88 NCC, 'Press Statement: Implementation of New SIM Registration Rules'
<https://www.ncc.gov.ng/media-centre/news-headlines/928-press-statement-implementation-of-new-sim-registration- rules> accessed 2 February 2024

89 Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 FederalRepublic of Nigeria Official Gazette No.101 Vol. 98 (7 November 2011)

be saved in a central database.[90] It has been posited by some that the establishment of centralised databases linked to SIM card registration can facilitate the process of mass communication surveillance.[91] There exist significant weaknesses in the system that allow for individuals to be monitored without proper legal procedures.[92]

It has been contended that the most optimal approach for the protection of citizens' constitutional rights, in the realm of surveillance, would involve a singular and comprehensive surveillance law.[93] This proposed law would entail detailed provisions forjudicial safeguards, and independent oversight, and restrict the importation and deployment of surveillance technologies to a single state agency.[94] It is submitted that this raises the question of whether a single state agency may have the resources or expertise to effectively oversee all surveillance technologies and activities and whether asingle surveillance law can effectively address concerns about the potential for government overreach and violations of privacy rights under a single surveillance law.

According to international standards, any interference with the right to privacy must be necessary and proportionate to the aim pursued and must be subject to independent oversight mechanisms to ensure compliance with these principles.[95] Without these safeguards, there is a risk that state surveillance activities could be conducted arbitrarilyor excessively, potentially infringing on individuals' rights to privacy and freedom of expression. This could have a chilling effect on free speech and the ability of individualsto express dissenting views or engage in political activism without fear of reprisal. Therefore, it is crucial that laws and regulations governing state surveillance be designedin a manner that adheres to the principles of necessity and proportionality, and that independent oversight mechanisms are put in place to ensure compliance. This can help strike a balance between the legitimate interests of the state and the fundamental rights and freedoms of individuals.

---

90 ibid, reg.11

91 A. Mare, 'An Analysis of the Communications Surveillance Legislative Framework in South Africa' 18<https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf> accessed February 2, 20234, O. Adebayo, 'Nigeria: Considering The Legal Tenability Of The Implementation Of New Sim Registration Rules' < https://www.mondaq.com/nigeria/telecoms-mobile--cable-communications/ 1021168/considering-the-legal-tenability-of-the-implementation-of-new-sim-registration-rules> accessed 2 February, 2024

92 ibid

93 Robert and others, *Mapping the Supply of Surveillance Technologies to Africa* (n.1) 19

94 ibid

95 See International Principles on the Application of Human Rights to Communications Surveillance <https://www.eff.org/files/necessaryandproportionatefinal.pdf> accessed 1 February 2024, UN PrivacyRapporteur, 'The United Nations Draft Legal Instrument on Government-led Surveillance and Privacy'. <https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pd> accessed 1 February 2024, art. 3 (4) and (7)

Examination of Legal Implications of Surveillance on Privacy and Freedom of Expression

Contemporary intelligence agencies and law enforcement entities carry out extensive andprogressively expanding mass surveillance using diverse methods. These methods range from direct mass interception of communications, acquisition of bulk communications data retained by telecommunications operators and other entities, widespread hacking initiatives, and indiscriminate deployment of facial recognition technology among other techniques.[96] Surveillance has profound implications for the right to privacy and freedomof expression, influencing the delicate balance between national security concerns and human rights and liberties:

1. **Erosion of Privacy Rights:** The issue of privacy encroachment through surveillance practices has garnered significant attention in recent years. With the rise of mass surveillance programs, the collection and analysis of personal information have become a major concern for individuals and organisations alike not just in Nigeria but in many other countries. In framing the definition of privacy, one perspective within the literature advocates for an emphasis on control.[97] According to this viewpoint, an individual's privacy remains undisturbed as long as they maintain control over their personal information Westin defined privacy as 'the claim of an individual to determine what information about himself or herself should be known to others.'[98] In contrast, an alternative perspective contends that privacy is contingent on access rather than control. Under this viewpoint, an individual's privacy remains intact as long as no one accesses their personal information and that mere loss of control does not mean that privacy has reduced.[99] In synthesizing these perspectives, Konig submits that a comprehensive definition of privacy could acknowledge both dimensions, emphasizing the preservation of control over personal information and the prevention of unauthorized access as integral components of safeguarding privacy.[100]

   There exist three concerns regarding surveillance and privacy rights:[101]

   i. Governments diminishing citizens' privacy through extensive data collection.
   ii. Risks associated with potential access to collected data, whether by government employees, exposure through hacking, or leaks.
   iii. Concerns about the misuse of collected data for objectionable purposes beyond mere access.

---

96 Privacy International, 'Mass Surveillance' <https://privacyinternational.org/learn/mass-surveillance#:~:text=Mass%20surveillance%20is%20indiscriminate%20surveillance,is%20reasonable%20suspicion%20of%20wrong doing> accessed 9 February 2024

97 P. Konigs, 'Government Surveillance, Privacy, and Legitimacy' *Philosophy & Technology* (2022) 35(8), 6

98 A. F. Westin, 'Social and Political Dimensions of Privacy' *Journal of Social Issues* (2003) 59(2), 431

99 Konigs, 'Government Surveillance, Privacy, and Legitimacy' (n.97), 6

100 Ibid

101 Ibid, 3

Konig argues that the concept of finding state surveillance objectionable solely because the extensive data collection diminishes people's privacy is unfounded.[102] This perspective contends that such a premise lacks a compelling and standalone reason to object to government surveillance, especially when compared to the other two concerns.[103] One point that supports this argument is that there are situations where sacrificing some level of privacy may be necessary for the greater good of society. For example, in cases of national security or criminal investigations, surveillance may be necessary to prevent or solve crimes, protect citizens, and maintain public safety. Another point is that governments have a responsibility to protect their citizens, and surveillance can be an effective tool for achieving this. By monitoring potential threats, governments can take proactive measures to prevent harm from occurring.

Following Konig's argument, the act of collecting data may indeed be perceived as diminishing individuals' control of privacy.[104] However, the significance of this particular privacy aspect is contingent upon the interplay with the other two concerns, namely the risk of accessed data and the potential use of data for objectionable purposes.[105] Konig asserts that defining privacy, specifically in terms of control privacy, provides a plausible framework. Nevertheless, he contends that the reduction of control privacy, on its own, does not constitute an autonomous concern that surpasses apprehensions regarding data access (losses of access privacy) and the potential misuse of collected data.[106] This perspective from Konig underscores the intricate relationship between different dimensions of privacy within the context of government surveillance.

For instance, there is a difference between loss of control privacy and loss of access. Where intelligence agencies monitor an individual's behaviour, eavesdrop on conversations, read email, or employ other means to compromise access privacy, these breaches in privacy are deemed problematic even in the absence of any risk that the collected information will be used for malicious purposes or exposed to the public, further exacerbating the impact on individuals' privacy.[107]

2. **Chilling Effect on Freedom of Expression:** Schauer submits that the chilling effects mainly stem from individuals' concerns regarding legal repercussions and the uncertainties inherent in the legal system.[108] According to Solove, continuous public surveillance, akin to the discomfort experienced when consistently being

102 Ibid, 5
103 ibid
104 ibid
105 ibid
106 ibid
107 Konigs, 'Government Surveillance, Privacy and Legitimacy' (n.) 7
108 F. Schauer, 'Fear, Risk and the First Amendment: Unraveling the Chilling Effect' *Faculty Publications* (1978)701

stared at in public, undeniably induces unease.[109] A recent study highlights the widespread use of digital surveillance technologies in various African countries, including Nigeria, leading to significant human rights violations.[110] Those unfairly targeted by surveillance technology experience lasting physical and psychological harm, facing unjustified detentions and even torture by authorities.[111] Whether journalists, activists, or ordinary citizens, individuals posting critical messages on social media are tracked, arrested, and detained.[112] Governments, citing national security, have exceeded legal surveillance powers, contributing to a concerning erosion of human rights.[113] According to reports, internet monitoring, mobile interception, and social media monitoring are all being carried out in Nigeria. [114] Furthermore, it has been disclosed that Nigeria has obtained the technology necessary to engage in these activities.[115] An illustrative instance of social media monitoring in Nigeria is the case of a pharmacist named Solomon Akuma, who was arrested on April 2, 2020, due to a critical social media post on Twitter where he posted that he would 'pay a Russian sniper to eliminate Buhari and Kyari' referring to the then President Muhammadu Buhari and his Chief of Staff, Abba Kyari.[116] This case, among several others, underscores the impact of social media scrutiny on individuals expressing dissenting views in Nigeria. Surveillance can generate chilling effects, discouraging individuals from affiliating with specific groups, participating in rallies, or expressing their views in meetings.[117] It has been reported that the use of surveillance technology in Nigeria exerts a 'chilling effect' on citizens, stifling debate and democracy.[118] Surveillance disproportionately hampers the freedom of expression for vulnerable groups, including minorities, certain political affiliations, civil society, human rights defenders, and professionals such as journalists and lawyers.[119] Additionally, victims of violence, abuse, and children are adversely affected.[120] Extensive surveillance practices have been found to have a significant impact on the exercise of freedom of expression, as individuals may refrain from voicing their opinions due to the fear of facing retaliation or

[109] Solove, 'A Taxonomy of Privacy' (n.14) 493

[110] T. Robert and others, *Mapping the Supply of Surveillance Technologies to Africa* (n.1)

[111] Ibid, 6

[112] ibid

[113] ibid

[114] T. Robert and others, *Mapping the Supply of Surveillance Technologies to Africa* (n.1) 48-53

[115] ibid

[116] A. Adebayo, 'UPDATED: Pharmacist detained for nine months 'for threatening Buhari' – Father' *Premium Times* (12 January 2021)<https://www.premiumtimesng.com/news/headlines/ 436368-updated-pharmacist-detained- for-nine-months-for-threatening-buhari-father.html?tztc=1> accessed 2 February 2024

[117] Solove, 'A Taxonomy of Privacy' (n.14) 493

[118] T. Robert and others, *Mapping the Supply of Surveillance Technologies to Africa* (n.1) 6

[119] Office of the United Nations High Commissioner for Human Rights, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' A/HRC/29/32 Twenty-ninth Session, 22 May 2015 <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32> accessed 30 January 2024

[120] ibid

being subjected to scrutiny by the surveillance apparatus.[121] Such self-censorshipcan have far-reaching implications, as it not only undermines the principles of democratic governance but also stifles the free flow of ideas and opinions, whichis crucial for the growth and progress of any society. Therefore, it is imperative that measures are put in place to safeguard the right to free expression and protectindividuals from any undue surveillance practices that might impede their exercise of this fundamental right. This study underscores the potential chilling ordeterrent effects arising not only from legal uncertainties but also from the erosion of trust in the legal system. As we navigate the complexities of modern surveillance, understanding these chilling effects becomes imperative for a comprehensive examination of their implications on individual freedoms and behaviours in Nigeria.

3. **Threats to Journalistic Freedom:** The prevalence of surveillance targeted towards journalists has raised significant concerns regarding the freedom and privacy of media personnel, ultimately limiting their ability to report and investigate without fear of intrusion. This unwarranted surveillance poses a significant threat to their safety, as well as the credibility of their work. It has been reported that journalists in Nigeria are subject to surveillance both online and offline, including the hacking of their email and social media accounts.[122] The confidentiality of sources, vital for investigative journalism and the protection ofwhistleblowers, is at risk.[123] Mandating the disclosure of sources is seen as a threatto freedom of speech and media freedom.[124] The requirement to reveal sources isperceived as a significant threat to freedom of speech and media freedom,particularly in the context of pervasive surveillance. When journalists are subjected to monitoring, both online and offline, including the hacking of their email and social media accounts, it creates a climate of fear and self-censorship. The fear of being surveilled can compel journalists to disclose their sources or refrain from pursuing sensitive stories, limiting the flow of information, and impeding the investigative function of the media. This chilling effect on journalists' ability to protect their sources directly stems from the omnipresent surveillance, highlighting the broader impact on press freedom and the democraticdiscourse. On August 9, 2018, journalist Ogundipe published an article disclosing communication between Nigeria's police chief and vice president.

[121] Office of the United Nations High Commissioner for Human Rights, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' 15 A/HRC/32/38 Thirty-Second Session, 11 May 2016<https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session32/Documents/A_HRC_32_38_EN.docx> accessed 30 January 2024

[122] K. Yusuf, ' SPECIAL REPORT: Heightened Surveillance by Security Operatives Puts Nigerian Journalists underClimate of Fear' Premium Times (31 March 2023) <https://www.premiumtimesng.com/news/headlines/591048-special-report-heightened-surveillance-by-security- operatives-puts-nigerian-journalists-under-climate-of-fear.html> accessed 31 January 2024

[123] ibid

[124] ibid

[125] Shortly after, police investigating the source issued a summons not addressed to Ogundipe, he was however made to face a charge of theft and possession of policedocuments.[126] In this case, the police utilised phone call records to establish connections between the journalist and other media professionals, demonstrating a methodical approach in tracking and subsequently arresting journalists.[127] In fewother cases, by scrutinizing call records, law enforcement was able to trace relationships and employ information as a basis for apprehending individuals within the journalistic community.[128] This illustrates a concerning use of surveillance techniques in targeting and implicating journalists in Nigeria.[129]

4. **Disproportionate Impact on Vulnerable Communities: [130]** Surveillance measures may disproportionately impact marginalized communities, leading to heightened social inequalities. Individuals deemed vulnerable are those who, dueto their race, class, gender, sexual identity, religion, or other intersecting characteristics, face a heightened risk of privacy breaches leading to emotional, financial, or physical harm or neglect.[131] McDonald and Forte have broadened thescope of vulnerable individuals to encompass survivors of domestic abuse, individuals with a history of incarceration, immigrants, activists, journalists, thosepolitically oppressed by society or their culture, individuals with HIV, LGBTQ individuals, as well as the very young and elderly.[132] The authors illustrate that the diverse identities mentioned have distinct needs and experiences, often necessitating tailored privacy protections that differ from those applicable to the general population.[133]

It is submitted that extending the definition to include survivors of domestic abuse, those with a history of incarceration, immigrants, activists, journalists, andindividuals politically oppressed, among others, as identified by McDonald and Forte, emphasizes the multifaceted vulnerabilities present. These diverse identities which exist in Nigeria, encompassing a range of socio-political and cultural contexts, demand tailored privacy protections to address their unique needs and experiences. The consequences of surveillance on vulnerable individuals in Nigeria extend beyond privacy concerns, influencing their ability

---

[125] J. Rozen, ‘’How Nigeria’s Police used |Telecom Surveillance to Lure and Arrest Journalists,” *Committee to Protect Journalists*, (13 February 2020) <https://cpj.org/blog/2020/02/nigeria-police-telecom-surveillance-lure- a…> accessed 2 February 2024

[126] ibid

[127] ibid

[128] ibid

[129] ibid

[130] N. McDonald and A. Forte, ‘Privacy and Vulnerable Populations’ in B. P. Knijnenburg and others *Modern Social Technical Perspectives on Privacy* (2022, Springer) 337

[131] ibid

[132] ibid

[133] Ibid, 338

to freely express themselves, and exacerbating the challenges faced by these communities in the democratic discourse. Thus, it is submitted that understanding and mitigating the impact of surveillance on vulnerable populations in Nigeria iscrucial for safeguarding both their privacy rights and freedom of expression.

Recommendations

To help address the chilling effect of surveillance and protect freedom of expression inNigeria, this study makes the following recommendation:

1. Establish clear and transparent laws governing surveillance, outlining permissible uses, ensuring judicial oversight, and enforcing strong data protection measures.
2. Create independent bodies with the authority to review and investigate surveillance activities, ensuring accountability and preventing abuses of power.
3. Implementation of transparency measures, requiring authorities to disclose the nature and extent of surveillance programs. Accountability mechanisms should bestrengthened to ensure that those conducting surveillance are held responsible forany abuses or illegal actions.
4. Integration of privacy-enhancing technologies

   Crafting regulations that specifically address emerging surveillance technologies, such asfacial recognition and mass data collection. This ensures that legal frameworks keep pace with technological advancements while safeguarding individual rights.
5. Promotion of digital literacy to empower individuals by the implementation of public awareness campaigns and educational programs to inform citizens about their rights regarding privacy and the potential impact of surveillance on democratic freedoms. Informed citizens are better equipped to advocate for theirrights.
6. Legal reforms to safeguard citizens' rights and balance security imperatives by encouraging citizen participation in the formulation and review of surveillance policies, fostering a more inclusive and democratic approach to decision-makingin this critical area. Implementing these legal reforms and policy measures can contribute to a more balanced and rights-centric approach to surveillance in Nigeria, mitigating the risks of privacy infringements and safeguarding democratic freedoms.

Conclusion

The findings of this study reveal a gap between Nigeria's legal framework for surveillanceand international standards. This mismatch has significant implications for several aspects of individual rights. Policies like mandatory NIN and BVN registration, coupledwith SIM card linking, create vast databases with sensitive personal information. Weaknesses in the system and non-compliance with international frameworks raise concerns about unauthorized access, misuse, and lack

of individual control over personal data. Collecting fingerprints and facial scans for SIM registration further intensifies privacy concerns. Without robust safeguards and clear regulations, thisbiometric data could be used for surveillance beyond its intended purposes, leading to discrimination and profiling. Weaknesses in the legal framework, like unclear proceduresand insufficient oversight, create an environment where surveillance can occur without proper legal justification, hindering transparency and accountability for potential abuses. The absence of independent bodies to review surveillance activities makes it difficult to detect and address misuse of power and violations of individual rights. The study also reveals the fear and uncertainty created by surveillance, leading to self-censorship, and hindering open discourse, particularly for vulnerable groups like journalists and activists. which violates fundamental rights.

Usage of surveillance measures against political dissidents, journalists, and civil society actors has yielded a chilling effect on journalistic pursuits, concurrently constricting the civic space essential for democratic deliberation and debate.[134] It has been submitted that within the Nigerian legal framework, ambiguity rather than lucidity prevails concerning the specific conditions under which surveillance aligns with legitimacy and remains consistent with human rights law.[135] Thereby underscoring the critical necessity for deliberate legal reforms and policy measures, particularly in the context of the multifaceted challenges associated with surveillance, privacy infringements, and the potential curtailment of democratic rights.

[134] Institute of Development Studies, 'Mapping the Supply of Surveillance Technologies to Africa' (n.1) 18
[135] Ibid, 18