African Journal on Privacy & Data Protection

To cite: AO Salau 'Cybersecurity, state surveillance and the right to online privacy in Nigeria: A call for synergy of law and policy' (2024) 1
African Journal on Privacy & Data Protection 152-175
https://doi.org/10.29053/ajpdp.v1i1.0008

Cybersecurity, state surveillance and the right to online privacy in Nigeria: A call for synergy of law and policy

*Aaron Olaniyi Salau**
Reader in Law, Faculty of Law, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria
https://orcid.org/0000-0002-6703-7794

Abstract:

As presented in this article, the conditions of mutual dependence and interactions between cybersecurity and state surveillance equally pose risks to the right to online privacy (also referred to as 'internet privacy') regarding the collection, use, access and protection of personal data by the individual and the state. While cybersecurity measures are necessary to safeguard against threats to computer networks and public infrastructure and prevent identity theft, these must not become a subterfuge for unlawful surveillance and interference by the state with personal data. Indeed, the right to online privacy is protected internationally, and among the cluster of privacy rights guaranteed in section 37 of the amended Constitution of the Federal Republic of Nigeria 1999. The right protects personal data contained in communications and metadata but extends also to communication infrastructure and software systems that are increasingly being required to have in-built privacy and data protection controls in their design for better protection of personal information. Conversely, wide-ranging laws and policies enable the state to intercept and monitor internet and electronic

* LLB (Hons) LLM (OAU, Ile Ife) BL (Lagos) PhD (Cape Town); aaron.salau@oouagoiwoye.ed.ng

communications in disregard of personal privacy to uphold cybersecurity interests. Interestingly, the recently-passed Nigeria Data Protection Act 2023 has now set the required standards for data protection and privacy. Consequently, this article aims to determine the extent to which the right to online privacy is respected and may be restricted in Nigeria for state security reasons, including cybersecurity, and whether these accord with online privacy and data protection standards. Using the lens of liberal democratic theory to re-orientate the normative framework for privacy for the internet age, the article conceptualises the imperative of online privacy in the age of cyber (in)security and undertakes doctrinal scrutiny of international human rights instruments, particularly the African Union Convention on Cyber Security and Personal Data 2014, and relevant literature. The article recommends that the Nigeria Data Protection Act 2023, which was passed to domesticate the AU Convention on Cyber Security, be rigorously enforced, the national security exemptions applicable thereto must be spelt out from the inception while the adjustments necessary for its smooth implementation must be made to ensure data protection and privacy.

Key words: cybersecurity; Data Protection Act Nigeria; personal data; state surveillance; right to online privacy

1 Introduction

Internet-enabled computer networks, information and communication technology (ICT), and social networking platforms that enable the digital transmission of information in real-time have become indispensable for cost-effective access to public, social and commercial services. This increased dependence on the internet and ICT is based on a capitalist business model that requires the surrendering and processing of vast amounts of personal information of individuals (data subjects) that may be searched, aggregated and cross-referenced.[1] The latter allows for the commercialised sharing and dissemination of data, the systematic monitoring of the citizens' communications by service providers and the yielding of access thereto to the government by tech giants without the data subject's prior consent. The availability of public services on the internet also comes with increased threats of attack on critical infrastructure from hacktivists, internet fraudsters, terrorists and other cyber criminals which can endanger the national interest. Countering such threats against computer networks is achieved through cybersecurity policies/strategies that serve to justify data retention laws and 'dataveillance', which pertains to data-intensive surveillance technologies that monitor human behaviour, digital communications and online activities.[2] Consequently, the traditional conception of privacy as the ability to control

1 D Boyd & K Crawford 'Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon' (2012) 5 *Information, Communication and Society* 662, 663.

2 E Luiijf and others 'Nineteen national cyber security strategies' (2013) 9 *International Journal of Critical Infrastructures* 3, 5-8.

access to personal information, which protects human dignity and autonomy, becomes challenging in an atmosphere of mass surveillance and availability of 'Big Data'. In modern democracies based on the rule of law, any government intrusion on privacy calls for the legality, legitimacy and proportionality of such measures and the principled protection of informational privacy. In Nigeria, the challenge is that despite the pervasive incidents of cybercrimes in the country, the uncoordinated state of law and policy on cybersecurity seriously limits the enjoyment of online privacy. Consequently, the article explores the importance of democratic theory and the nature of reforms required to stimulate synergy between cybersecurity and privacy protections in Nigeria. Part 2 examines the principles of a democratic theory to guide the protection of online privacy in the cyber (in)security age. Part 3 expounds on the imperative of international human rights law and the African Union (AU) Convention on Cyber Security and Personal Data 2014 for online privacy protection. Part 4 examines the merits of the recently-enacted Nigeria Data Protection Act, 2023 in order to address the gaps in Nigeria's legal framework on online privacy and discusses how the theoretical framework developed in part 2 can inform the cybersecurity policy related thereto. Concluding, part 5 proposes legal and policy reforms to enhance online privacy and cybersecurity in Nigeria.

2 A democratic theory of privacy and cybersecurity

This part of the article develops a theory inculcating principles of online privacy that should guide the regulation of cybersecurity and inform the law on state surveillance in a democratic polity. To flesh out the theory, it is argued that the traditional conception of privacy as a private space of inviolate personality or self-identity based on the exercise of control, dominance or authority over personal information has become outmoded due to the impact of the internet on human activities. In the internet age, this yields a normative understanding of privacy beyond the private/public dichotomy due to the expanded opportunities for state surveillance in the name of cybersecurity measures to safeguard computer networks, public infrastructure and personal data against threats. This lends weight to the right to online privacy which offers a counterpoint to pervasive surveillance in the Internet age. The right serves to constrain mass surveillance of the citizens in view of the expansive meanings that are being ascribed to cybersecurity by both democratic and authoritarian governments. The notion of a private realm involving intimacy, secrecy, solitude or seclusion is of great social value, which is innate to human beings, although this has varied across cultures, civilisations, and historical and legal traditions.[3] Privacy is a reasonable and legitimate expectation of non-intrusion in all societies that enables every person or group to live a life free of patronising, paternalistic or meddlesome influences by others. Privacy is equally required to develop and nurture intimate,

3 S Gutwirth *Privacy and the information age* (2002) 24-26.

familial and other interpersonal relationships in a dignified manner even within public and private spaces.[4] Privacy thus is a multidimensional but much-interrogated concept as it can protect a person's bodily integrity, private life, home and communications from unwarranted searches and seizures and help to uphold one's life choices, reproductive autonomy, and so forth.[5] Nonetheless, the legal protection of privacy is one of the essential conditions for the furtherance of a free and democratic society, a means for the development of the human personality and enjoyment of civil liberties. The right to online privacy, which is the totality of the legal procedures, processes and systems available to protect one's personal information/data from unauthorised access, use or interference in the online environment, can be said to be an extension of this right.[6]

Classical expositions on the right to privacy see it foremost as evoking concerns over the control of personal information. Westin calls it 'the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others'.[7] Westin identified four 'basic states of individual privacy': (i) solitude; (ii) intimacy; (iii) anonymity; and (iv) reserve.[8] In this way, the expectation of privacy that a person has can be in terms of restriction: of intrusion by government agents; of access to sensitive, intimate, or confidential information; and into private spaces. Hence, the right to privacy is a value of much purchase in free and democratic societies due to the role it plays in limiting government's power over the citizens.[9] In their 1890 seminal article on privacy, Warren and Brandeis view privacy as the 'right to be let alone' based on the exegesis of the United States Constitution and Bill of Rights which, to a significant extent in the digital age, now includes the 'right to be forgotten'.[10]

Privacy also is a requirement for maintaining human agency, personhood or individual autonomy and consequent human flourishing in an atmosphere of dignity.[11] Autonomy in this context denotes the assertion of control over personal information relating to preferences, goals, aspirations, tastes, commitments, and so forth, which a person has cultivated over time ably assisted by zones of 'relative insularity' and uninhibited by traditions and conventions. The latter is the mark of a liberal citizenship defined by critical reflection over personal choices.[12] Furthermore, privacy provides the condition and ingredient to critical reflection

4 As above.
5 DJ Solove 'A taxonomy of privacy' (2006) 154 *University of Pennsylvania Law Review* 477, 549-550.
6 JE Cohen 'What privacy is for' (2013) 126 *Harvard Law Review* 1919.
7 AF Westin *Privacy and freedom* (1967) 31-32.
8 Westin (n 7) 33-36.
9 H Nissenbaum 'Privacy as contextual integrity' (2004) 79 *Washington Law Review* 119, 128-129.
10 A Forde 'Implications of the right to be forgotten' (2015) 18 *Tulane Journal of Technology and Intellectual Property* 83, 120.
11 B van der Sloot 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of big data?' (2014) 5 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 230, 234.
12 J Cohen 'Examined lives: Informational privacy and the subject as object' (2000) 52 *Stanford Law Review* 1373, 1424; Nissenbaum (n 9) 148-149.

required for active citizenship, which is the participation in activities and discussions concerning political and other issues of general interest. This is because the citizens' ability to reach out to one another on matters of common interest may only be fully realised under an atmosphere free of an overbearing government. Similarly, privacy is an enabler and key condition for the enjoyment of freedom of expression and journalistic freedom, to mention but a few democratic rights.[13] For instance, those who provide information that journalists have a duty to publish do so on the basis of confidentiality. Journalistic freedom would be seriously hampered if the government were to force journalists to reveal their sources of news and information.[14] Contrariwise, freedom of expression itself would be 'chilled' if journalists become subject to reprisal attacks from persons who would otherwise wish that information that the public is entitled to receive be kept secret. From the foregoing, it may be safe to surmise, albeit at first glance, that aside from the need to protect individual interests, the collection and processing of personal or private information could also serve to protect countervailing collective values of a liberal democratic order such as national security, which may implicate the need for trade-offs and balance.[15] However, a binary conception of privacy that produces a static stimulus on the development of personhood or autonomy has become outmoded in the internet age as the concept always yields itself to varied changing contexts in which personal information is externally observable.[16] Moreover, Cohen observes that even in modern democracies, the internet has become a principal means of expression, information dissemination, and behavioural modulation.[17] As Rengel posits, considering that spaces for the expression of privacy shift and expand in response to innovations in information and computing and other internet-enabled technologies, the challenge then is how and to what extent a person's online privacy can be protected.[18] Nissenbaum thus argues for an approach to privacy regulation that considers the social context whereby data collected in a private setting ought not to be appropriated for public (online surveillance) purposes.[19] Surveillance could then ordinarily not be conceived as pernicious but as a public good and a means for social control and effective governance in which citizens, governments, businesses and other organisations have vested interests.[20] Furthermore, technological cybersecurity measures could also serve to protect the individual's data-based (digital rights) and personal data from being violated through cyber-attacks and, in turn, be complemented by data protection measures for privacy protection. This

13 'The right to privacy in the digital age' 71/199 (2017) UN General Assembly Resolution.
14 UNESCO 'The right to privacy in the digital age', https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-UNESCO.pdf (accessed 31 March 2023).
15 Nissenbaum (n 9) 151.
16 Nissenbaum (n 9).
17 JE Cohen 'Surveillance vs privacy: Effects and implications' in D Gray & SE Henderson (eds) *Handbook of surveillance law* (2017) 455-469.
18 A Rengel 'Privacy as an international human right and the right to obscurity in cyberspace' (2014) 2 *Groningen Journal of International Law* 36, 41.
19 Nissenbaum (n 9).
20 AS Elmaghraby & MM Losavio 'Cyber security challenges in smart cities: Safety, security and privacy' (2014) 5 *Journal of Advanced Research* 491, 493-494.

should factor-in 'the right to [online] privacy as a necessary component in the development of a citizen-centric security policy'. The legal regime of 'cyber privacy' could therefore be accentuated by related statutory or regulatory prohibition of interference with, disruption or unauthorised access to a computer network, information system and related data or the unauthorised processing, interception or transmission of data.[21] However, 'cybersecurity' has no fixed definition but varied approaches. The International Telecommunications Union has defined cybersecurity as 'the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organisation, as well as users' assets'.[22] Cybersecurity could be said to relate to the practices and tools devised to ensure the confidentiality, integrity, and availability (the 'CIA triad') of computer systems and networks.[23] Also, cybersecurity involves the technical protection of the internet and ICT systems, the development of organisational and institutional capability by states to prevent and detect illegal cyber activity, and policy and legal measures to safeguard users against cybercrimes and the unauthorised use or appropriation of personal data.[24] Nonetheless, cybersecurity attracts cyber surveillance.[25] Democratic states have often used the growth in the various international dimensions of cybercrimes and cyber-attacks to justify the warrantless surveillance of citizens in the name of national security but with less concern for privacy.[26] Anticipatory surveillance of online activities by security agencies may be meant to detect, deter and counter the threats to national security in real-time, but its mass surveillance and data interception methods violate the dignity of persons with no criminal involvements and are discriminatory of individuals and groups thereby profiled.[27]

Furthermore, the interconnectedness of individuals and institutions in cyberspace and the role of technology in shaping human behaviour and the understanding of privacy cannot be overemphasised in exposing the power dynamics between individuals and the state. To reduce the ensuing asymmetric relationship, a way forward is that cybersecurity must be moderated by judicial and technical solutions.[28] Technological advancement has also opened

21 As above.
22 See ITU High Level Experts Group (2008), ITU Global Cyber-Security Agenda (GCA) High Level Experts Group (HLEG) Global Strategic Report, Geneva: ITU, 27.
23 AM Matwyshyn 'Cyber!' (2018) 2017 *Brigham Young University Law Review* 1138-1139.
24 National Initiative for Cybersecurity Careers and Studies 'Glossary' (2017), https://niccs.us-cert.gov/glossary (accessed 23 September 2023); Luiijf and others (n 2) 6.
25 Q Eijkman 'Indiscriminate bulk data interception and group privacy: Do human rights organisations retaliate through litigation?' in L Taylor and others (eds) *Group privacy: New challenges of data technologies* (2017) 162.
26 E Sutherland 'Digital privacy in Africa: Cybersecurity, data protection and surveillance' https://ssrn.com/abstract=3201310 (accessed 31 March 2023).
27 Y McDermott 'Conceptualising the right to data protection in an era of big data' (2017) *Big Data and Society* 4.
28 D Broeders and others 'Big data and security policies: Towards a framework for regulating the phases of analytics and use of big data' (2017) 33 *Computer Law and Security Review* 309, 319-320; ML Sundquist 'Online privacy protection: Protecting privacy, the social contract, and the rule of law in the virtual world' (2012) *Regent University Law Review* 153, 171.

unimaginable pathways for data collection and unobtrusive monitoring in cyberspace, for example, through digital 'cookies' or mobile phone applications, which allow unlimited access to personal information that may be easily misused or turned over to the government.[29] Concerning the proportionality of such data-gathering methods, international human rights institutions (dealt with in part 3 below) and civil society organisations have weighed in several times. The widely-acclaimed International Principles on the Application of Human Rights to Communications Surveillance of 2013 is one such intervention.[30] Relatedly, most modern democratic and hybrid legal regimes have aggregated several core general principles on privacy and cyber privacy, which are hereby re-iterated.

(1) Activities within homes enjoy the greatest level of protection from intrusion except on reasonable grounds and based on judicial orders.
(2) The privacy of activities within perimeters of the home may be protected at varying levels based on a 'reasonable expectation of privacy' or statutory provision.
(3) Activities carried out publicly may enjoy little or no privacy protection absent special statutory protection.
(4) Access to public services subject to data collection and regulated by the state may carry lesser or no privacy protections.
(5) Activity-related data may be processed if the data subject consents and if no prohibition exists for its processing.[31]

Moreover, the routine or indiscriminate processing of data would make it difficult to keep abreast of why and how data is being processed. That is why data protection rules are required to protect individuals against surveillance and foster accountability by public institutions. This is vital to protect citizens against the unconscionable exercise of government power in a democracy.[32]

Consequently, the framework of online privacy protection must focus on the asymmetric relations between individuals and the state to ensure that surveillance conducted for the public good must be demonstrably seen to achieve its purpose. This must be in a manner consistent with the cherished democratic values of autonomy, accountability and transparency. Indeed, Abdulrauf and Fombad, referring to De Hert and Gutwirth, traced the origin and development of data protection principles to the inadequacy of privacy *simpliciter* and as a mechanism to reconcile conflicting values of privacy and government surveillance in a democracy.[33] The respect for autonomy based on the informed consent of

29 Eijkman (n 25) 154.
30 Electronic Frontier Foundation 'Necessary and proportionate', http://www.necessaryandproportionate.net/ (accessed 23 September 2023).
31 Elmaghraby & Losavio (n 20) 493.
32 G de Gregorio 'Digital constitutionalism, privacy and data protection' in G de Gregorio *Digital constitutionalism in Europe*: *Reframing rights and powers in the algorithmic society* (2022) (ch 6) 216, 222-223; V Boehme-Neßler 'Privacy: A matter of democracy. Why democracy needs privacy and data protection' (2016) 6 *International Data Privacy Law* 222, 232; DJ Solove *Nothing to hide: The false trade-off between privacy and security* (2011) 93.
33 LA Abdulrauf & CM Fombad 'Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms' (2017) 38 *Liverpool Law Review* 105, 109-110.

individuals is a primary principle of digitised data protection that lends weight to a democratic theory of online privacy in the age of cyber insecurity. Consent, other basic principles of data privacy such as the so-called Fair Information Processing Principles (FIPP),[34] as well as other rules that enhance an individual's control over personal information comprise the norms of any data privacy system.[35] This means that individuals must have the right to control the way their data is collected, used and shared, which enlivens the right to be informed about data collection, the right to access and correct data, the right to delete data, and the right to withdraw consent to data processing. Online privacy should be protected by ensuring that individuals have reasonable control over their personal data so they can choose how it is collected, used, stored and shared. Security of data should be maintained by ensuring that it is protected from unauthorised access, use and disclosure. Moreover, data processors must be transparent and fair in their processing activities. This includes providing clear and accessible information on the data processing activities they conduct, the purposes for which they process data, the types of data they process, and how data is shared, if at all. Also, every democracy should provide measures to ensure that those responsible for collecting, storing and using data are held accountable for any misuse, unauthorised access or privacy breaches. This should include measures to ensure that data is processed in accordance with the principles on penalties for data breaches and a system of oversight and monitoring.[36] This means that there should be an external mechanism for ensuring that organisations are respecting individuals' online privacy rights and for the auditing of government surveillance programmes.

Considering the foregoing, international human rights institutions, intergovernmental bodies, privacy advocates and non-governmental organisations (NGOs) continue to grapple with how to ensure that the cybersecurity measures adopted by states do not stultify online privacy. This issue is extensively considered in part 3 below.

3 Online privacy and cybersecurity: International and African perspectives

The quest for cybersecurity has taken centre stage in global policy due to increased cyber criminality, including identity thefts, distributed denial of service (DDOS), internet hacking and even cyberterrorism, the prevention and prosecution of which may require states to access or collect personal data from

34 These include proportionality, minimality, purpose limitation, data subject influence, data quality, data security and sensitivity; see L Bygrave *Data privacy law: An international perspective* (2014) 145-165.

35 LA Abdulrauf 'Giving "teeth" to the African Union towards advancing compliance with data privacy norms' (2021) 30 *Information and Communications Technology Law* 87, 89-94.

36 See Organisation for Economic Cooperation and Development (OECD) Guidelines on the protection on privacy and transborder flows of personal data adopted 23 September 1980 para 11 (OECD Privacy Guidelines).

third parties, including business enterprises, or to intercept, disclose or share digital communications and intelligence data. This has made the protection of online privacy more challenging. Yet, efforts by the international community and regional institutions to address profiling, automated decision making, the gathering of sensitive personal information and resolve other challenges at the intersection of cybersecurity (as a sub-set of state security) and privacy have been faltering under the domain of cyber sovereignty.[37] The desired results are within reach if an international consensus on data control policy could be achieved.[38] This part engages with the evolving human right to digital privacy and its implications for personal data security within the ambience of state surveillance.

3.1 International human rights law and the cybersecurity-privacy conundrum

The international legal protection of online privacy, which lies at the heart of the networked information society, is a relatively recent concern, the normative basis of which derives from extant international human rights instruments negotiated under the auspices of the United Nations (UN), including article 12 of the Universal Declaration of Human Rights 1948 (Universal Declaration)[39] and article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR).[40] The right to online privacy protects personal data from misappropriation or unlawful use and is the enabler of the panoply of digital rights that are activated through the internet, smartphones, electronic communication media, search engines, social media networks, and computational technologies. This emergent right can be found in a patchwork of international soft laws. The interventionist elaborations by various human rights mechanisms, special procedures and other inter-governmental bodies acting under the auspices of the UN on 'the right to privacy in the digital age' confirm that this is a vital right.[41]

For instance, the 5 July 2012 resolution of the UN Human Rights Council (UNHRC) heralded the emergence of digital rights when it affirmed: '[T]he same rights that people have offline must also be protected online.'[42] These extend

37 EB Sultanov and others 'Transformation of the right to privacy in the context of the development of digital technologies' (2022) 7 *BiLD Law Journal* 223, 228.

38 ML Rustad & TH Koenig 'Towards a global data privacy standard' (2019) 71 *Florida Law Review* 365, 453.

39 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' (UN 1948).

40 '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks' (UN 1966). See also regional instruments such as the European Convention on Human Rights (European Convetion) and the Inter-American Convention on Human Rights.

41 The UN Guidelines for the Regulation of Computerised Personal Data Files was the first attempt under the auspices of the UN that broached concrete protection for personal data.

42 'The promotion, protection and enjoyment of human rights on the internet' (A/HRC/RES/20/8). See also 'The promotion, protection and enjoyment of human rights on the

to privacy online,[43] which states are obligated to protect in the digital context by adopting legal, policy and other measures on data protection. In addition, technical solutions such as privacy-enhancing technologies (PETs) are required in the design of new technologies.[44] This is meant to give consumers more control over their online activities and prevent abuses through state surveillance or by businesses collecting, processing, sharing and storing biometric information in compliance with international human rights law. The UN through the General Assembly and the UNHRC also maintain that arbitrary surveillance and interception of communications, the arbitrary collection of personal data and the indiscriminate use of biometric technologies violate the right to privacy.[45] The UN has since 2013 in a General Assembly Resolution taken a stance against the tendency by states towards mass surveillance because of its implications on privacy. The Resolution called on states 'to respect and protect the right to privacy', especially in the context of electronic surveillance and digital communications.[46] Similarly, the 'United Nations Human Rights Report 2022' Office of the UN High Commissioner for Human Rights (OHCHR) 2022 Report amply demonstrates that general public surveillance is disproportionate and should be subject to judicial oversight.[47] Moreover, states are obliged to protect the 'confidentiality of [digital] communications'.[48] This may be done through encryption, pseudonymisation, anonymity and other measures, which means that anonymising technologies are vital for the uninhibited expression of views and exchange of ideas by individuals and groups online.[49] The UN General Assembly has also noted that 'privacy online is important for the realisation of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association'.[50] Considering the important of data privacy, the UNGA has called upon states:[51]

To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding

internet' (A/HRC/20/L.13), United Nations General Assembly Resolution, adopted by the Human Rights Council on 29 June 2012.

43 'The promotion, protection and enjoyment of human rights on the internet' (A/HRC/32/L.20), Resolution adopted by the Human Rights Council on 27 June 2016 para 8.

44 Para 5.

45 UN General Assembly Resolution 71/199 (2017); 'The right to privacy in the digital age' Human Rights Council Resolution 42/15 adopted at its 42nd session on 26 September 2019.

46 UNGA Resolution 68/167 on 'the right to privacy in the digital age', https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf (accessed 31 March 2023).

47 OHCHR Report 2022 412.

48 'The right to privacy in the digital age' (A/HRC/39/29) UNHCHR Report of 3 August 2018 para 20.

49 UNHCHR (n 48).

50 Resolution on the 'promotion, protection and enjoyment of human rights on the internet'.

51 'The right to privacy in the digital age' UNGA Resolution A/RES/68/167 adopted 18 December 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed 31 March 2023); 'The right to privacy in the digital age' UNGA Resolution A/RES/69/166 adopted 18 December 2014, https://undocs.org/en/A/RES/69/166 (accessed 31 March 2023).

the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law'.

However, while potentially legitimate circumstances may exist to protect national security, democratic states often ignore these guidelines to justify mass surveillance, bulk data and metadata collection concerning their citizens based on the cybersecurity narrative. As UNGA Resolution 68/167 recalls, any limitation by data surveillance to the right to privacy must satisfy a tripartite test of legality, legitimacy and democratic necessity. In a nutshell, a limitation must be provided in a clear and accessible law (as to its authorisation or circumstances) which provides for safeguards and oversight against abuse; serve a legitimate purpose (which includes state security); and be necessary towards such legitimate purpose (that is, state security). Ultimately, international human rights law will juxtapose compelling interests of cybersecurity with the values of online privacy to ensure that a limitation is proportionate in terms of a cost and benefit analysis (to the aim, be least intrusive, and rationally connected to the legitimate aim.[52] In addition, an assessment of proportionality requires transparency of the surveillance, its purpose and the likelihood of its objective being achieved.[53]

Relatedly, besides the well-known article 8 privacy protection in the European Convention on Human Rights and Fundamental Freedoms 1950 (European Convention), the EU is the global norm leader in data privacy in terms of its network of instruments and obligations of collection, use, safeguards, and so forth, placed on data controllers and processors.[54] In a nutshell, the foregoing correspond with the EU Charter of Fundamental Rights to the effect that data processing must be fair and lawful; for specified and lawful purpose(s); adequate and non-excessive in relation to purpose; accurate and up-to-date; and not kept for longer than is necessary; in accord with data subjects' rights (for example, non-transfer to a jurisdiction not having reciprocal adequate protection, and so forth).[55] Most significantly, an independent state institution, such as a data protection commissioner, must be statutorily mandated to monitor and enforce data protection rules. Such concerns have been brought closer home to African

52 UNODC 'International human rights and cybercrime law', https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html (accessed 23 September 2023).

53 Geneva Academy 'The right to privacy in the digital age: Meeting Report', https://www.geneva-academy.ch/joomlatoolsfiles/docmanfiles/ReportThe%20Right%20to%20Privacy%20in%20the%20Digita l%20Age.pdf (accessed 21 September 2023).

54 See OECD Privacy Guidelines (n 36) paras 7-14; E-privacy Directive; Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 108 of 1981 (CoE Convention 108/1981); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (principles on the processing of personal data) OJ 2016 L 119/1, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 31 March 2023); Charter of Fundamental Rights of the European Union (OJ C 364 of 18 December 2000) art 7 (Charter), http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 31 March 2023); EU-US Safe Harbour Pact and its amendment; McDermott (n 27) 1-7.

55 See EU Charter of Fundamental Rights art 8(2).

governments and multilateral institutions on the need to reckon with canons that underline the protection afforded by privacy-related laws that have been recognised internationally.[56]

3.2 African data privacy regime

In Africa the increased internet access and penetration and ownership of smartphones have created a networked society with significant boosts for commerce and governance particularly in the telecoms industry,[57] although the data protection field remains fluid which has facilitated government surveillance. State surveillance, particularly, has grown in sophistication due to the increased availability of intrusive technologies to authoritarian governments to monitor citizens and political dissenters.[58] There is also increasing evidence of 'pervasive surveillance programmes and data mining activities' on the continent 'obviously in violation of data privacy norms'.[59] In Africa, just like in other climes, since the ultimate goal of surveillance is to collect information that, in most cases, relates to or identifies an individual, data protection laws have a direct bearing and are among the category of legal instruments that have been established specifically to regulate the gathering of personal information by electronic means including electronic surveillance.[60] Also, considering the improved access to internet technologies and related infrastructures, Africans are now becoming more concerned not only about the safety of critical ICT infrastructure from opportunistic cyber-attacks, but also the need to safeguard the fundamental rights of persons against the risks associated with the security of personal data shared online.[61]

Africa's first multilateral instrument to protect data privacy on the continent was the Supplementary Act A1SA.1f01f10 on Personal Data Protection Within Ecowas (EPDP Act). It was signed by member states of the Economic Community of West African States (ECOWAS) on 16 February 2010 in Abuja, Nigeria. The EPDP Act, to some extent, is patterned after the former EU 'Directive 95/46/EC', that is, Data Protection Directive with the objective of 'a harmonised legal framework in the process of personal data' within ECOWAS member states.[62] The EPDP Act protects the data of an identifiable individual through eight principles

56 J Terstegge 'Privacy in the law' in M Petkovíc & W Jonker (eds) *Security, privacy, and trust in modern data management* (2017) 13-14; OECD Privacy Guidelines (n 36) para 1(b); CoE Convention 108/1981.
57 Sutherland (n 27).
58 As above.
59 Abdulrauf (n 36) 88.
60 LA Abdulrauf 'The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa' (2018) 18 *African Human Rights Law Journal* 365, 372-374.
61 R Alunge 'Africa's multilateral legal framework on personal data security: What prospects for the digital environment?' (2020) 38-58, https://doi.org/10.1007/978-3-030-41593-8_4 (accessed 30 March 2023).
62 EPDP Act, Preamble.

of data processing, the foremost being the consent of data subjects.[63] Others are fairness, specification of purpose, accuracy, transparency, confidentiality, and so forth.[64] The latter requires the protection and confidentiality of personal data, particularly during transmission over a network.[65] The EPDP Act mandates the establishment of an independent data protection authority with powers to protect the data-related rights of persons, to hear complaints, issue compliance directives, and penalise any controller or processor of data for the contravention of relevant rules.[66] The EPDP Act is directly binding on Nigeria as a state party by virtue of the revised ECOWAS Treaty of 1975. The EPDP Act was followed by the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention), adopted in Malabo on 27 June 2014.

The African Commission on Human and Peoples' Rights (African Commission) – the AU continental body mandated to promote human and peoples' rights – has elaborated on the right to privacy in the digital age. The African Commission's Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (DoP 2019) reads:[67]

> (1) Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information.
> (2) Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies.

Furthermore, DoP 2019, which is legally non-binding, obligates states to provide safeguards for the right to privacy in terms of 'any law authorising targeted communication surveillance' such as through 'the prior authorisation of an independent … judicial authority', 'specific limitation on the … scope of the surveillance' and other 'due process safeguards'.[68] The 'notification of the decision authorising surveillance within a reasonable time' post-conclusion, transparency thereof, and regular 'monitoring and review by an independent oversight mechanism' are other germane requirements.[69] However, the EU Data Protection Directive 1995, the *General Data Protection Regulation* (GDPR)'s forerunner's influence in the drafting of data protection laws in Africa, cannot be underrated more, with the result that the African Charter on Human and Peoples' Rights of 1981 (African Charter), the flagship African human rights treaty, has no

63 EPDP Act art 23.
64 EPDP Act arts 24-29.
65 EPDP Act art 28.
66 One Trust Data Guidance 'African bodies: ECOWAS Act on Personal Data Protection', https://www.dataguidance.com/opinion/african-bodies-ecowas-act-personal-data-protection (accessed 31 March 2023).
67 Adopted by the African Commission at its 65th ordinary session held from 21 October to 10 November 2019 in Banjul, The Gambia, Principle 40.
68 DoP 2019 Principle 41(2)(3)(a)(b)(c).
69 DoP 2019 Principle 41(3)(d)(e)(f).

privacy provision.[70] While most African states have privacy protection in their constitutions, the right to online privacy is embryonic and suffers from poor implementation in the face of data retention conditions imposed on digital intermediaries and social network platforms by authoritarian governments.[71]

Nonetheless, the AU Convention on Cyber Security and Data Protection 2014 draws inspiration from CoE's Convention 108/1981 to provide a template for cybersecurity and protection of personal information in Africa.[72] The Convention is a great boost for data protection and privacy in Africa and provides a laudable standard for the right to online privacy that can be adapted by Nigeria and other African countries. The Convention became operative on 8 June 2023 after Mauritania deposited its instrument of assent with the AU Chairperson being the fifteenth AU state to do so in terms of its provisions.[73]

3.2.1 Data privacy and protection in Africa: An overview

In bridging the normative gap on data privacy and protection on the continent, the ministers on information technology (IT) in Africa secured the AU Commission (AUC) and UN's regional Economic Commission for Africa's assistance in preparing a Declaration on Cybersecurity for the African context based on the principles of data protection and cybersecurity. The Declaration was eventually adopted by African Heads of State and Government at its meeting held in Malabo in 2014 as the AU Convention on Cyber Security and Data Protection 2014 (Malabo Convention), an analysis of which hereby follows.

The Convention provides for the establishment of a National Personal Data Protection Authority as the supervisory and regulatory body and the *loci* of enforcement with authority, among others, to prescribe sanctions for violations.[74] The Malabo Convention prescribes six basic principles of data processing towards individual data privacy. First, the data subject's consent must be obtained before their data is processed. Confidentiality and security are required particularly when personal data is transmitted over a computer network. Second, data processing must be fair and lawful. Third, the processing of data must serve a specific or related purpose (purpose limitation). Fourth, data controllers must ensure that data is up-to-date and erase or amend it when inaccurate or incomplete (data

70 The African Charter on the Rights and Welfare of the Child protects the right to privacy; see AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2 *International Data Privacy Law* 163, 168-171.

71 YE Ayalew 'The right to privacy in the digital era in Africa' (2022) 12 *International Data Privacy Law* 16, 19.

72 Signatory countries to the ECOWAS Treaty including Nigeria have undertaken obligations under the EPDP Act to create legislative, policy and other actions as regards 'personal data protection' subject to public interest.

73 African Union 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection', https://dataprotection.africa/wp-content/uploads/2305121.pdf (accessed 10 September 2023).

74 AU Cybersecurity Convention arts 11, 12(2) & 19(1)(f).

accuracy principle). Fifth, data controllers must process data in a transparent manner (transparency principle). Lastly, the principle of confidentiality obligates data controllers to process personal data in secure and confidential ways.[75] In addition, specific principles apply to the processing of sensitive personal data. these include data that relate to intimate relationships, sexual orientation, religious inclination, political persuasion, and so forth.[76] Furthermore, as regards the rights of data subjects, the Convention provides for the right to information, to access data, the right to object to data processing, and to rectify data.[77] These embody the entitlements of the individual to demand from a data controller the extent to which her data has been processed, shared or disclosed to a third party. The coverage of data privacy under the Convention, therefore, extends to photographs, voice messages, emails, internet login passwords, search history, and so forth.

The 'principle of confidentiality and security' must be operationalised any time personal data is to be transmitted over a (computer) network. Data controllers under both the Convention and ECOWAS Data Act will perform the same duties as regards data security.[78] Moreover, a data controller must be ready to give the assurance of data security and will be vicariously liable for any breach thereof even when an independent data processor works for it.[79] The Convention makes the DPA the *loci* of enforcement, monitoring and supervisory activities being entitled to '[e]ntertaining [of] claims, petitions and complaints regarding the processing of personal data' and violations of data security but must advise petitioners on the way forward.[80] As regards data subjects' rights, there is a right to access and rectify data.[81] These embody the data subject's entitlements to demand to know the extent to which their data has been processed, shared or disclosed to a third party. In addition, other Convention rights as regards personal data protection include access to information, data access, objection to data processing, and 'to be forgotten'. The coverage of data privacy under the Convention, therefore, extends to photographs, voice messages, emails, internet login passwords, search history, and so forth, which should, however, not detract from the need for free flow of data. The 'processing of personal data relating to public security, defence, research, criminal investigation or state security' can also be undertaken, but subject to the provisions of other existing laws.[82]

Notably, the Convention aims to commit parties thereof to cybersecurity policy and strategy and legal instruments to respond to cyber-attacks and cyber-crimes that adequately satisfy the security interests of the state and protect online

75 AU Cybersecurity Convention arts 13(1)-(6).
76 AU Cybersecurity Convention art 14.
77 AU Cybersecurity Convention arts 16, 17, 18 & 19; EPDP Act arts 38(6) & 39.
78 AU Cybersecurity Convention arts 20 & 21.
79 AU Cybersecurity Convention art 13(b); EPDP Act art 29.
80 AU Cybersecurity Convention art 12(2)(e); EPDP Act art 19(1)(f).
81 AU Cybersecurity Convention art 17; EPDP Act arts 38(6) & 39.
82 AU Cybersecurity Convention art 9(1)(d).

privacy in consonance with personal data protection.[83] The Convention applies to personal data processing, automated or otherwise, by individuals and public institutions in a state party's territory.[84] However, it is subject to exemptions or authorisations by a state for the processing of data for 'state security', 'defence', and 'sensitive data' and in terms of 'an executive or legislative act'.[85] So, considering that the AU Cybersecurity Convention is a model law, how it is implemented by its state parties will determine the extent to which the state and private businesses will be able to process data, intercept calls, and carry out surveillance without subject to the requisite safeguards and oversight.

Now, given the foregoing targeted international and African human rights-focused analyses, the next activity of this article is to engage with Nigeria's privacy and cybersecurity landscape.

4 Nigeria's constitutional and legal safeguards for online privacy

This part engages with an analysis of the cybersecurity and surveillance laws, policies and practices in Nigeria and assesses their compatibility with the right to online privacy, starting with an overview of Nigeria's constitutional framework on the domestic application of international human rights. The analysis exposes the potential risks and harms associated with state surveillance and inadequate cybersecurity measures on online privacy in Nigeria.

Under the amended Constitution of the Federal Republic of Nigeria, 1999 (1999 Constitution, CFRN 1999 or Constitution) an international treaty or agreement must be incorporated into the domestic legal framework before it can bind institutions, persons and the government.[86] This is the case with the African Charter. Even where not yet incorporated into domestic law, a treaty signed or ratified by the country is binding based on the principle of *pact sunt servanda* whereby the government may not act contrary to its undertaking. The provisions of an unincorporated treaty may also be relied upon by the courts as an interpretive aid in construing other legal instruments not contrary thereto. The human rights provisions in chapter IV of the Constitution also borrowed extensively from the Universal Declaration and have also ratified several other human rights treaties that guarantee human rights, including the right to privacy under ICCPR. This makes the tripartite tests of legality, necessity and legitimacy applicable to the limitations of such rights. Moreover, Nigeria developed a National Security Policy and Strategy in 2014 (updated in 2021) and passed

83 AU Cybersecurity Convention Preamble, arts 1 & 8(1).
84 AU Cybersecurity Convention Preamble, arts 24 & 25(3).
85 AU Cybersecurity Convention arts 5(a)(d), 9(1)(a)-(d) & 10(4)(a)-(d).
86 CFRN 1999 sec 12.

the Cybercrimes Act 2015 and Data Protection Act 2023 partly in terms of its obligations under the AU Cybersecurity Convention.

4.1 Privacy and the emergence of digital communications

CFRN 1999 recognises privacy as an inalienable human right, but the need for robust laws and policies to protect the citizens' digital rights, including online privacy, only sparsely receives attention from policy makers considering the extant patchwork of legislations and regulations.[87] Section 37 of CFRN 1999 reads: 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.' The provision guarantees the right to privacy of family life, homes, correspondences, telephone and telegraphic communications of Nigerians from unlawful interference by the state and non-state agents. Section 37 mimics an earlier provision that was first drafted in the era of analogue telephones (fixed landlines), telegraphic and telex services when internet-enabled devices and computer networks were still a rarity in Nigeria.[88] In addition, the common law of torts applicable in Nigeria does not recognise a general tort of privacy, although a limited common law action for breach of confidence could be relied upon to remedy a wrongful interference with personal data. Even such a limited legal right remains subject to restrictions under some inherited colonial/military era statutes such as the Official Secrets Act 1962 (OS Act 1962)[89] and National Security Agencies Act 1986 (NSA Act 1986)[90] that deny public access to state secrets and sensitive law enforcement, foreign relations and national security-related information.

The opening-up of political space in the aftermath of the democratic transition in 1999 led to improvements in individual and collective freedom of digital communications in Nigeria. Consequently, the Nigerian Communications Act 2003 (NC Act),[91] the main legal and regulatory framework on electronic and digital communications, was enacted and established the Nigerian Communications Commission (NCC) as the regulatory body for Nigeria's telecoms industry. The NC Act 2003 obligates licensees or service providers to

87 Reference could be made to the following: Central Bank of Nigeria; Consumer Protection Framework 2016 (bank customers' right to confidentiality); Credit Reporting Act 2017 (protects data subjects' right to privacy and confidentiality of their credit); Child Rights Act 2003 (guarantees the child's right to privacy of correspondence, telephone communications, etc, subject to parental or legal guardians' reasonable supervision): National Health Act 2014 (makes information relating to a healthcare user confidential, sets out conditions for the disclosure of such information, and prescribes measures to safeguard health records); Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission (requires telecommunication operators to take reasonable steps to prevent 'improper or accidental disclosure of data and ensure safe storage of personal information; Freedom of Information Act 2011 (requires the government to protect personal privacy by denying access to personal information unless the individual concerned consents.

88 Constitution of the Federal Republic of Nigeria 1979 (as amended) sec 37.

89 Cap O3 Laws of the Federation of Nigeria (LFN) 2004.

90 Cap N7 LFN 2004.

91 Act 19 of 2003.

'upon written request by the Commission or any other authority, to assist as far as reasonably necessary' in preventing an offence, enforcing the law, and in the preservation of national security.[92] Section 146(3) of the NC Act protects licensees from any liability while carrying out any such duty. The NCC may also determine that a licensee or class of licensees implement the capability to allow authorised interception of communications.[93] This could be in the event of a public emergency, in the interest of public safety, to protect national security, and so forth.[94] Pursuant to its enabling powers, the NCC has made some regulations and codes relating to the protection of subscribers' personal information.[95] This article tracks only those directly related to state surveillance.

The Lawful Interception of Communications Regulations 2019 (LICR 2019), pursuant to the NC Act 2003, set out the conditions in which communications originating from Nigeria may be intercepted, collected and disclosed. The LICR 2019 permits an 'authorised agency' such as the State Security Service (SSS) and the Office of the National Security Adviser (NSA) to intercept any communication in Nigeria based on a court warrant. Warrantless interception and monitoring of online communications are authorised to prevent danger to human life or where otherwise necessary, although judicial authorisation must be obtained within 48 hours thereof. The authorised agencies must submit an annual report of all concluded interception cases to the Attorney General of the Federation (AGF). This creates a real conflict of interest situation considering that the AGF is expected to publicly scrutinise the secret activities of a government from which she benefits politically.

Relatedly, the Registration of Telephone Subscribers Regulations 2011 (RTSR 2011) mandates licensees to capture subscriber information and to transmit such to a central database to be established and maintained by the NCC. The latter can grant security agencies access to the database provided it receives a prior written request from an official, not below the rank of an Assistant Commissioner of Police (ACP) or coordinate rank. Furthermore, RTSR 2011 mandates licensees to retain call data, which may also be released by the NCC upon a written request to it signed by a police officer at or above the rank of ACP or equivalent.[96] All the foregoing provisions call for a law targeted at data privacy, the safeguarding of computer networks from criminal interference and the continuous promotion of technological innovation.

92 NC Act 2003 sec 146(2).
93 NC Act 2003 sec 147.
94 NC Act 2003 sec 148(1).
95 See, eg, the Federal Republic of Nigeria Official Gazette, Nigerian Communications (Enforcement Process, etc) Regulations 2019, https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/840-enforcement-processes-regulations-1/file (accessed 30 March 2023); Consumer Code of Practice Regulations 2007 (CCPR 2007) and its Schedule, the General Consumer Code of Practice (GCCP).
96 RTSR 2011 Reg 8 (2)(a)(b).

4.1.1 Cyber-crimes and data privacy

Globalisation and e-commerce, aided by the internet, technological developments and improvement in IT infrastructure and digital technologies, have percolated down to Nigeria, but the authorities were late in responding to the cybersecurity threats and criminality related thereto until very recently. Several policy initiatives of the government have now been enunciated. There is the National Cybersecurity Policy and Strategy 2021 (NCPS 2021) adumbrated by the National Security Adviser (NSA),[97] which focuses on safeguarding Nigeria's critical infrastructure and the protection of its cyber-space from cyber-attacks, online fraud, and so forth, besides its economic outlook.[98] The National Digital Economy Policy and Strategy 2020-2030 from Professor Isa Pantami-led Digital Economy Ministry also addresses the nation's cybersecurity challenges to enhance the national digital economy.[99] Based on these policy responses, state surveillance has increased and is becoming more widespread even with the enactment of cyber-crime laws. This has negative impacts on online privacy rights and other fundamental freedoms. For example, Nigeria's Cybercrimes (Prohibition, Prevention, etc) Act, 2015, which was enacted to strengthen the fight against organised crime, criminalises unauthorised access to computer systems.[100] The law also criminalised certain activities carried out in cyber-space with a computer or through computer systems and networks. These include cyber-stalking, sending obscene, menacing or hate messages, internet fraud, cyber-terrorism, and so forth.[101] Incidentally, some of these offences have been targeted at journalists, bloggers and the political opposition while their phrasing is open-ended, thus giving a cause for concern.[102] Section 38 of the Cybercrimes Act also permits data and traffic retention by internet intermediaries and telecom companies for two years at the government's request. Notably, the retained data 'shall not be utilised except for legitimate purposes as may be provided for under th[e] Act, any other legislation', whilst the authority to use such information must be exercised with 'due regard to the individual's right to privacy' while 'tak[ing] appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved'.[103] However, what

97 Federal Republic of Nigeria 'National cybersecurity policy and strategy 2021', https://ctc.gov.ng/national-cybersecurity-policy-and-strategy/ (accessed 22 September 2023).

98 N Okoh '2021 national cybersecurity policy and strategy: Enhancing digital safety and economic growth' *The Journal* 25 February 2021, https://thejournalnigeria.com/cybersecurity-policy-strategy-digital-safety-economic-growth/ (accessed 30 March 2023).

99 Federal Ministry of Communications and Digital Economy 'National Digital Economy Policy and Strategy 2020-2030', https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file (accessed 23 September 2023).

100 Cybercrimes Act 2015 sec 6.

101 Cybercrimes Act 2015 secs 24(1)(a) & (b).

102 In *The Incorporated Trustees of Rights and Laws Awareness v Nigeria* Suit ECW/CCJ/APP/53/2018 (judgment delivered on 10 July 2020), the ECOWAS Court of Justice struck down section 24 of the Cybercrimes Act that prescribes the offence of cyberstalking for vagueness; see Sahara Reporters 'ECOWAS Court declares Nigeria's Cybercrime Act section 24 vague, arbitrary, unlawful', https://saharareporters.com/2023/03/22/ecowas-court-declares-nigerias-cybercrime-act-section-24-vague-arbitrary-unlawful (accessed 30 March 2023).

103 Cybercrimes Act 2015 sec 38(4)(5).

amounts to 'legitimate purposes' is not specified while there is no provision on the notification of data breach under the Act.

4.1.2 The Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 (NDP Act 2023, NDP Act or Act) was enacted in reforming the overall legal framework for data protection. It replaces the erstwhile Nigeria Data Protection Regulations 2019 (NDPR 2019) issued by the National Information Technology Development Agency (NITDA).[104] The Act is applicable only where the processing of personal data occurs within the Nigerian jurisdiction concerning a data subject within Nigeria or by a data controller or processor who markets to or monitors residents within Nigeria. The Act establishes the Nigeria Data Protection Commission (NDPC) with a governing council to be headed respectively by political appointees, which creates the issue of independence from the government. The Act mimics the EU's GDPR in several respects. For instance, it defines personal data as 'any information relating to an identified or identifiable natural person' or individual, that is, the data subject. This includes personal data and metadata such as a name, address, photo, email address, bank details, social media posts, medical information, or a computer's IP address. The NDP Act enunciates six principles of data processing: (i) fair, lawful and transparent processing, that is, with the consent of the data subject and for the performance of the data subjects' legal obligation, vital interests or the public interest; (ii) purpose specification, that is, only for specified, explicit and legitimate purposes and no further processing in an incompatible manner; (iii) adequacy, that is, limited to the minimum necessary for collection or further processing; (iv) limited retention, that is, not retained for longer than necessary; (v) accuracy, that is, complete and kept up-to-date; (vi) data security, that is, processed in a manner that secures against loss, destruction, or any form of data breach.[105] Several safeguards against unlawful processing include a data protection impact assessment (DPIA)[106] and improvement in the rules on the processing of sensitive personal data.[107]

It is worth noting that the Act has created substantive data protection and privacy standards against which the plethora of regulations and policies regarding the creation of databases in Nigeria must be subsumed. For instance, the e-communications regulatory environment currently is riddled with requirements for biometrics registration and the creation of e-databases as part of the ongoing modernisation of e-governance processes in the banking, health, educational and

104 Aelex 'A summary of the Nigeria data protection Bill 2022', https://www.aelex.com/a-summary-of-thenigeriadata-protection-bill-2022/ (accessed 31 March 2023).
105 NDP Act 2023 sec 24.
106 NDP Act 2023 sec 28.
107 NDP Act 2023 sec 30.

other sectors in Nigeria.[108] Furthermore, the government through the NCC may direct telecom providers to collect, intercept or retain personal data for national security reasons without the requisite data subject's consent.[109] Such surveillance and data interception actions require serious scrutiny in relation to the NDP Act to assess their legality, legitimacy, democratic necessity and ultimate proportionality when carried out in the name of cybersecurity or national security.

4.2 Whither state surveillance?

Section 3(2) of the NDP Act 2023 exempts from its purview, subject to the human rights provisions of the Constitution and their limitations, the processing of personal data carried out by a 'competent authority' as is necessary for national security. Under section 3(3) the NDPC may by regulation prescribe the types of personal data and processing that may be exempted from application of the Act, while section 3(4) further empowers NDPC to issue a guidance notice as to legal safeguards and best practices as regards any aspect of data processing that is exempted if it violates or is likely to violate section 24 of the Act (the principles of data processing). Such 'competent authorities' are yet to be designated but they would ordinarily include the national security agencies established under the NSA Act 1986.[110] These are the Defence Intelligence Agency (DIA), the National Intelligence Agency (NIA) and the State Security Service (SSS) (otherwise called the DSS). Again, while the exemptions that have been envisaged under sections 3(2) and 3(3) are yet to be carved out, it is not inconceivable that the 'competent authorities' may rely on the NC Act, LICR 2019, NCPS 2021 and Cybercrimes 2015 as basis for the interception of communications (see also paragraphs 4.1 and 4.1.1 above).

State surveillance in Nigeria could easily fail the requirement of legality prescribed under international human rights law (part 3.1 above) because the judicial and political safeguards against abuse are not well-established. As already stated, Regulation 8(2) of RTSR 2011 empowers the NCC to demand the release of subscribers' data by service providers to the security agencies, while section 38 of the Cybercrimes Act 2015 permits the interception of communications but has not specified the legitimate national security purpose for such or the need to notify the data subject thereafter.[111] Regulation 18 of LICR 2019 permits

108 See the Federal Republic of Nigeria Official Gazette, Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 (popularly called 'SIM card registration'), https://www.ncc.gov.ng/docman-main/legalregulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file (accessed 31 March 2023); Bank Verification Number (BVN) registration; Electoral Act 2022 (mandatory registration for the e-voting system). Government has plans to merge these databases electronically for administrative purposes though many of these projects have turned up with incomplete or mismatched information while persons affected face serious hurdles to make corrections. See the National Identity Management Commission Act 2007 (NIMC Act 2007).

109 NC Act 2003 secs 146(2) & 147.

110 NSA Act 1986 sec 1(1)(a)(b)(c).

111 See RTSR 2011 Reg 8(2)(a)(b).

the intercepted communication to be stored for three years. The challenge relates to the security of such data. The legal provisions are also widely drafted, which is a 'red flag' for potential abuse. The legitimacy and democratic necessity of any so-called national security or defence rationale to intercept and analyse communications data, therefore, can be seriously queried.

Furthermore, there is a very troubling conflict between the two statutes governing the national security agencies and other statutes such as the NDP Act 2023. Under the NSA Act 1986, the *modus operandi*, spending and personnel matters of the national security agencies are state secrets that are not amenable to public or legislative scrutiny while it specifically voids other laws inconsistent with it.[112] Currently, there is no system of oversight for the national security agencies under the NSA Act 1986 while the one envisaged under NDP Act 2023 is not yet in place. Even the so-called oversight by the AGF under LICR 2019 is weak and questionable considering that the AGF might be politically defensive towards its political benefactors.

However, a brief comparative overview of the legal frameworks for national security and intelligence in South Africa and the United Kingdom can yield some insights into how these democratic countries provide for their oversight and audit which may be tapped and adapted for Nigeria. In South Africa, state surveillance by its State Security Service (SSA) and other agencies is permitted under the National Strategic Intelligence Act of 1994, Intelligence Services Oversight Act of 1994, Intelligence Services Act of 2002, and [General Intelligence Law Amendment Act] GILAA of 2013.[113] The latter statute expressly defines the term 'national security'. South Africa's Intelligence Services Oversight Act of 1994 created the parliamentary Joint Standing Committee on Intelligence (JSCI) and the Inspector-General for Intelligence, either of which may hear complaints of unlawful surveillance from citizens.[114] The JSCI, which is composed of members of different political parties, has the responsibility to scrutinise and report on the operations of the SSA. In the United Kingdom, the political oversight of the investigatory powers of the secret service, namely, the Secret Intelligence Service (MI6), Security Service (MI5), and Government Communications Headquarters (GCHQ), is handled by a parliamentary Intelligence and Security Committee (ISC) under Investigatory Powers Act of 2016 (IP Act 2016). Under the IP Act 2016, an ISC report concerning its work must be published every year.[115] To provide transparency and accountability, the IP Act 2016 also established the Investigatory Powers Commissioner's Office (IPCO) to oversee the use of GCHQ's operational powers and the Investigatory Powers Tribunal (IPT), an

112 NSA Act 1986 secs 3 & 7(2).
113 See E Sutherland 'Governance of cybersecurity – The case of South Africa' (2017) 20 *African Journal of Information and Communication* 96.
114 Sutherland (n 113) 96-97.
115 Investigatory Powers Act 2016 (UK) sec 234.

independent judicial body to grant redress to victims of unlawful investigation.[116] The IP Act 2016 provides that interception warrants will only be granted when authorised by a secretary of state and approved by a judicial commissioner and if proportionate to what it seeks to achieve, such as the interests of national security.[117]

4.3 Call for synergy of law and policy

Many democracies are adopting cybersecurity strategies encompassing laws, policies and practices to prevent crime and in sync with human rights law of data privacy, but several gaps in Nigeria's existing cybersecurity legal and policy frameworks in comparison to evolving international standards call for a synergy of law and policy. There is no gainsaying that the numerous public projects and methods through which personal data is obtained, processed and managed neglect the right to access by data subjects for needful correction. Purportedly acting for the national cybersecurity or economic interest, public and private agencies could hand over personal and communications data collected to security agencies without transparency, properly laid down procedures or later notification. This constitutes a violation of the right to online privacy and raises data protection concerns under the prevailing data protection regulations in Nigeria. Consequently, the strategies for the synergy of law and policy at the intersection of cybersecurity and online privacy should ordinarily encompass (i) a legislative oversight of national security agencies; (ii) collaboration between government and citizens to address cybersecurity threats and protect citizens' privacy; (iii) proposals for new laws and policies or the amendment of the ones existing to address the gaps in Nigeria's cybersecurity and online privacy laws such as the absence of a clear definition of 'national security'; (iv) the importance of public education and awareness to promote better cybersecurity practices; and (v) technological solutions and policy strategies such as privacy-enhancing technologies, and to strengthen the capacities and skills of data controllers and processors to adopt state-of-the-art technologies to ensure privacy by design and default.

5 Conclusion

The article has dwelled on the national appropriation of the advantages of internet penetration and ICT usage among Nigerians for commerce, socialisation and access to public services as a rapidly-advancing process. The vital gains of a digital economy and the global internet infrastructure are now being threatened by cyber-related crimes and other vices. It accords with democratic principles for

116 GCHQ Governance 'Oversight', https://www.gchq.gov.uk/section/governance/oversight (accessed 20 September 2023).
117 GCHQ Governance 'Legal framework', https://www.gchq.gov.uk/section/governance/legal-framework (accessed 21 September 2023).

the strategies and laws designed to arrest cyber criminality to be proportionately balanced by a data privacy law that meets international standards, but the situation in Nigeria currently is skewed in favour of the state despite the existence of the NDP Act 2023. This has grave implications for the enjoyment of online privacy and related freedoms by citizens, professional journalists and more politically-conscious persons. The situation also has broader implications for the protection of online privacy and cybersecurity in other contexts. Cybersecurity law and policy measures are needful but pose risks of overreaching the state's surveillance powers and consequent loss of control over personal data, including citizens' ability to communicate anonymously. Ensuring online privacy requires that state surveillance practices be transparent and limited and involves a call to action for policy makers, civil society organisations and other stakeholders in Nigeria to work towards compliance with the NDP Act 2023.

In addition to paragraph 4.3(i)-(v) above, the article recommends a synergistic approach to the enhancement of cybersecurity and privacy in Nigeria as being complementary in the internet age. Cybersecurity strategies and surveillance practices must be reformed through the injection of institutional safeguards and independent multi-party oversight as in the UK, increased public awareness and enhanced democratic participation. Since Nigeria now has a Data Protection Commission under the NDP Act 2023, it must establish its regulatory independence from the onset by swiftly imposing sanctions on errant data controllers and processors and enriching a safe online environment by creating awareness of the data subjects' rights. There is also the need to encourage private sector participation in cyber protection.