ABUAD Law Journal (ALJ)
Vol. 9, No. 1, 2021, Pages 1-22 *https://doi.org/10.53982/alj.2021.0901.01-j*
Published by College of Law, Afe Babalola University Law Journal,
College of Law, Afe Babalola University, Km 8.5, Afe Babalola Way,
P.M.B. 5454, Ado Ekiti, Ekiti State, Nigeria ISSN: *2971-7027*
www.abuad.edu.ng, abuadlawjournal@abuad.edu.ng

An Assessment of the Protection of Children under the Nigerian Data Protection Regulation 2019

Dr. Ifeoluwa A. Olubiyi*
Aghohovwia Kwame-Okpu**

Abstract

Data protection which evolved out of the established notion of privacy to deal with threats posed to privacy by information communications technology is concerned with the use of laws and policies to regulate the collection and processing of personal data. This paper discusses the level of protection given to children under the Nigerian Data Protection Regulation which is the primary law on the subject matter in Nigeria. To achieve its aim, the paper examines the development of data protection as an offshoot of the established notion of privacy and the need to specifically protect children before discussing the level of data protection afforded children in Nigeria with a view to showing its adequacy or otherwise. The paper found that as a vulnerable group, children face privacy risks posed by information communications technology and may unknowingly disclose personal information due to several factors. So, it is necessary for data protection law to establish safeguards for their protection. The paper also found that the Nigerian Data Protection Regulation does not designate children as vulnerable groups. Further findings are that the law also does not adequately regulate the processing nor provide for the protection of personal data belonging to children and some of its inadequate provisions may adversely affect the effective protection of children's privacy in today's digital world. To remedy these shortcomings the paper makes some recommendations that can be implemented immediately and in the future before concluding.

Key words: personal data, data privacy, online privacy of children, data protection in Nigeria

1.0 Introduction

When advancements in information communications technology (ICT) resulted in the invention of systems that could collect, store and process large quantities of personal data, which is essentially any information that can be used to identify an individual,[1]individual privacy concerns arose regarding losing control of personal data once it is collected and subjected to technological processes. Concerns also arose on the potential abuses by government and corporations that regularly collect personal data.[2]Out of these concerns, data protection emerged to address the intricacies of privacy issues raised by these developments. Building upon the established right to privacy, data protection is concerned with the protection of personal data relating to an individual in their capacity as Data Subjects (DS) and their ability to determine what happens to their personal data. In that sense, it regulates the collection, control and processing of personal data and provides for penalties as well as remedies in the event that personal data is handled contrary to laid down regulations.[3]

Children are not exempt from the danger posed by these threats to personal data, and as vulnerable members of society,[4] they belong to categories of persons that are exposed to further risks and could suffer peculiar violations. Children have long been considered candidates for special protection in different endeavours of human life,as a result, there is a need to ensure that particular safeguards are in place to protect their personal data. This is why data protection laws across

*Reader/Ass Prof, Department of Private and Business Law, College of Law, Afe Babalola University, Ado-Ekiti (ABUAD), Nigeria. Email: olubiyiia@abuad.edu.ng; ifejemilugba@gmail.com
**PhD candidate, College of Law, Afe Babalola University, Ado-Ekit (ABUAD), Nigeria. Email: akwameokpu@gmail.com

[1] Mark Burdon, *Digital Data Collection and Information Privacy Law*(Cambridge University Press 2022) 67-69

[2] Patricia Boshe, *Data Protection Legal Reforms in Africa* (Doctoral dissertation, Universität Passau, Germany 2017)<*https://opus4.kobv.de/opus4-uni-passau/files/514/Data+Protection+Legal+Reforms+in+Africa.pdf*>accessed 23 August 2022

[3]B Garbin and K Staunton and M Bourdon, 'Tracking Legislative Developments in Relation to "Do Not Track" Initiatives' in MG Michael and K Michael(eds), *Uberveillance and The Social Implications Of Microchip Implants: Emerging Technologies* (IGI Global, 2014) 235-259

[4]Fabio Macioce, 'The Vulnerable Groups and Their Legal Value', in Stephen Eric Bronner (ed), The *Politics of Vulnerable Groups. Critical Political Theory and Radical Practice*(Palgrave Macmillan, 2022) 31-59

jurisdictions contain special provisions on their protection and why there is a need to include such provisions where they are non-existent.

Despite the presence of a constitutional right to privacy, the overall level of data protection in Nigeria could do with some improvements, and even more so for the protection afforded children. Under data protection law in Nigeria children are not considered as vulnerable and there are less than adequateprovisions requiring special rules for the collection and processing of their personal data.

This article is divided into four sections, the first section serves as the introduction and briefly discusses the concept of data protection, while the second gives an overview of data protection in Nigeria. The third section discusses children as candidates for special data protection and the fourth assesses the level of protection afforded them under the NDPR while comparing it to that in selected jurisdictions. The fifth section recommends ways to improve the protection afforded children in Nigeria. Thereafter, the article concludes.

2.0 Overview of Data Protection in Nigeria

It was not until 2019 that the right to privacy under section 37 of the Constitution of the Federal Republic of Nigeria Constitution 1999 (as amended) **(**CFRN 1999) was explicitly translated into the domain of data protection[5]by the NDPR which was issued by the National Information Technology Development Agency (NITDA) pursuant to thepowersunder its enabling act.[6]Prior to the NDPR, sector specific laws on data protection existed in the banking and communications industries in form of the Nigerian Communications Commission (NCC) General Consumer Code of Practice Regulations for Telecommunication Service Providers of 2007 (the General Code), the NCC Registration of Telephone Subscribers Regulation (RTS) of 2011 and the Central Bank of Nigeria (CBN) Consumer Protection Framework (CPF) of 2016.

There is also in existence certain laws which in themselves are not data protection laws but contain provisions which impact upon and regulate data protection in specific contexts. These include, the National Identity Management Commission

[5]Justin Bryant, 'Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights' *Stanford Technology Law Review* (2021) (24) (2) 389
[6]National Information Technology Development Agency (NITDA) ActCap N156 Laws of the Federation of Nigeria 2010, s 6 (c)

(NIMC) Act of 2007,[7]The Freedom of Information Act (hereinafter FOIA) of 2011,[8] the National Health Act (NHA) of 2014,[9] theCybercrimes (Prohibition, Prevention, Etc.)of 2015 (Cybercrimes Act) and the Credit Reporting Act (CRA)of 2017. These sector specific laws and specific provisions in conjunction with the NDPR and the CFRN 1999 (specifically section 37) which have general application (the latter only to citizens), form the legal framework on data protection in Nigeria. However, a consideration of all these legislations are beyond the scope of this paper; hence, the paper shall examine the provisions of the NDPR which is its focus.

2.1 The Nigeria Data Protection Regulation of 2019

The NDPR is greatly influenced by the European Union (EU) General Data Protection Regulation[10] (GDPR) and prior to its issuance, data protection in Nigeria was regulated by the constitutional provision on privacy and the above-mentioned sectoral laws and specific provisions.[11]The material scope of itsapplication covers all forms of processing of personal data in respect of citizens of Nigeria whether they reside in Nigeria or not as well as those of natural persons in Nigeria.[12]The territorial scope covers personal data of natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent.[13] To facilitate effective implementation and enforcement of theNDPR, the NITDA developed an Implementation Framework in 2020,[14] as a guide to assist data controllers and administrators understand the controls and measures needed to comply with the NDPR.

[7] Cap N108 Laws of the Federation of Nigeria 2010
[8] CAP F43 Laws of the Federation of Nigeria 2011
[9] Act no 8 of 2014
[10]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 GDPR), OJ 2016 L 119/1.
[11] Folabi Kuti and Ugochukwu Obi and Seth Azubuike, 'Nigeria' in Alan Charles Raul (ed),*The Privacy, Data Protection and Cyber security Law Review- Edition 4* (The Law Reviews, 2017) 50-66
[12] NDPR reg 1(2) (a)-(b)
[13] ibid
[14]NITDA, 'Nigeria Data Protection Regulation 2019: Implementation Framework.' March, 2020(NDPR Implementation Framework) para 2

The NDPR strives to meet international standards in the sphere of data protection, therefore it directs that personal data be collected and processed in accordance with certain governing principles. These governing principles which are contained in regulation 2.1 of the NDPR are an iteration of the globally accepted Fair Information Practices/Principles (FIPs) on how to handle personal data.[15]The NDPR creates rights for DS[16] and contains definitions as well as provisions on consent, data, personal data, data subject, and other terms in data protection.[17]The rights created for DS under the NDPR include the rights to access personal data; request rectification; object to processing and have personal data erased.[18]DS also have a right to data portability[19]and a right to be informed of the appropriate safeguards for data protection where personal data is to be transferred to a foreign country or to an international organization.[20]
Under the NDPR, a DS is any person that can be identified, directly or indirectly by reference to an identifier.[21] Personal data is any information relating to an identified or identifiable natural person (Data Subject)[22] such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The definition of personal data as contained in the NDPR is wide in scope and includes identifiable information that could be created using technology and also information which can identify a natural person including children directly or indirectly.

Under the NDPR, a data controller[23] is a person who either alone, jointly or commonly with other persons or a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed. This definitionis quite expansive and includes statutory bodies who in reality regularly

[15]Lewis Brisbois and Sean Hoar. 'GDPR, Part I: History Of European Data Protection Law' [2018] <*http://www.mondaq.com/unitedstates/x/643052/data+protection/GDPR+Part+I+History+of+European+Data+Protection+Law*> accessed 4 June 2022
[16] NDPR Reg 3.1
[17] ibid reg 1.3
[18] ibid reg 3.1 (7) (h)
[19] ibid
[20] ibid reg 3.1 (f)
[21] ibid reg 1.3 (xiv)
[22]ibid reg 1.3 (xix)
[23] ibid reg 1.3 (x)

collect and process personal data perhaps more than other parties. The NDPR does not define the term data processor explicitly, however, its definition of data controllers, is encompassing enough to cover data processors because a data processoris an entity that process data on behalf of the controller.[24]

The issue of consent in the collection and processing of personal data is topical,[25] it is therefore worth noting that the NDPR contains provisions on it. To this end, regulation 1.3 (c) of the NDPR, defines consent as freely given, specific, informed and unambiguous indication of the wishes of a DS, by a statement or by a clear affirmative action, signifying agreement to the processing of personal data. The NDPR also makes consent one of the five basis upon which lawful processing can be carried out.[26] The other bases for lawful processing under the NDPR are if the processing of personal data is necessary in a particular situation, such as the performance of a contract, compliance with a legal obligation, protection of the vital interests of the DS, the performance of a task carried out in the public interest and the exercise of official authority.
The NDPR places a responsibility on data controllers to make sure no data is obtained without letting the DS know the specific purpose of the collection.[27]Furthermore, any medium through which personal data is being collected or processed is directed to display a simple and conspicuous privacy policy which the class of DS that is being targeted can understand.[28]

Due to their nature and because of the harm that could be occasioned from indiscriminate processing, the best data protection regimes generally restrict the processing of special categories of data except on certain grounds after specific requirements have been met. The NDPR does not do this, it only lists items that constitute sensitive data[29] to includedata relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records. After which it places a responsibility on anyone

[24]GDPR art 4 (8)
[25]YP Yang, 'Data Protection In The Big Data Era: The Broken Informed Consent Regime And The Way Forward', In Joseph Lee and Aline Darbellay (eds), *Data Governance in AI, FinTech and Legal Tech* (Edward Elgar Publishing 2022), 59-78; Fedeli P and others, 'Informed Consent and Protection of Personal Data in Genetic Research on COVID-19' *Healthcare* (2022) (10) (2) 349 <*http://dx.doi.org/10.3390/healthcare10020349*> accessed 6 July 2022
[26] NDPR reg 2.2
[27] ibid reg 2.3
[28] ibid reg 2.5
[29] NDPR reg 1.3 (xxv)

involved in processing or the control of sensitive data to develop security measures to protect such data.[30] There is however a provision in the Implementation Framework that processing sensitive data will require a higher standard of consent except where processing is for health emergency, national security and crime prevention.[31]

Categories of personal data identified as special or sensitive can be related to the types of discrimination addressed in human rights instruments and those enshrined in constitutional protections to prohibit discrimination.[32]Theypertain to groups of individuals who are deemed vulnerable, such as children, the elderly, those with mental illnesses, those seeking asylum, those with disabilities, members of ethnic minorities, and the sick. These persons often lack legal capacity, are incapable of giving their consent, or may suffer extremely negative outcomes from misuse of their personal data.[33]

Apart from being without a provision on the actual and specific requirements for processing special categories of data, the NDPR, is without robust provisions on profiling. Profiling is automated processing of data to analyse or to make predictions about individuals.[34]The NDPR does not contain prohibitions or restrictions on the kind of data that can be subject to profiling only that data controllers provide DS with information on the existence of automated decision-making, including profiling, as well as the significance and the envisaged consequences of such processing for the DS.[35]

A breach of the other provisions of the NDPR is deemed as a breach of the provisions of the NITDA Act of 2007,[36] however persons who breach the rights

[30] ibid reg 2.6
[31] NDPR Implementation Framework para 6.2
[32] An example is section 42 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) (CFRN 1999); European Commission, *Ethics in Social Science and Humanities* (European Commission 2021) 11-12
[33]Stanislaw Piasecki and Jiahong Chen, 'Complying with the GDPR When Vulnerable People Use Smart Devices', *International Data Privacy Law*, (2022) (12) (2) 113–131 <*https://doi.org/10.1093/idpl/ipac001*>accessed 6 June 2022; Ghent University, 'GDPR: Who are considered as vulnerable persons?' <*https://onderzoektips.ugent.be/en/tips/00001782*/> accessed 6 June 2022
[34] Lee Matheson, 'WP29 releases guidelines on profiling under the GDPR'<*https://bit.ly/3Duagek*>accessed 6 June 2022
[35]NDPR reg 3.1 (l)
[36] NDPR reg 4.2 (6)

of DSunder the NDPR are liable to fines in addition to any other criminal liability.[37] Where the violator is a data controller dealing with more than 10,000 DS, the fine is 2% of annual gross revenue of the preceding year or the sum of ₦10 million, depending on which is greater. Where the data controller deals with less than 10,000 DS, the fine is 1% of the annual gross revenue of the preceding year or the sum of₦2 million depending on which is greater. Unless data controllers realize large sums of annual gross revenue from which 2 % or 1% will be a substantial amount of fine to be paid, the fines stipulated in the NDPR case may not be punitive, but just mild reprimands for corporations.[38]

At the time of writing this paper, DS in Nigeria, are without effective mechanisms to assist them in seeking and getting personal remedies for data privacy violations. While there are provisions for fines payable to the government coffers, the NDPR is silent on personal remedies for DS who have suffered the data privacy violations.

3.0 Children as candidates for Special (Data) Protection

While children are entitled to and protected by standard human rights, the realization that as a result of their situation they might be exposed to risks and injustice such as violence, child labour, trafficking, sexual exploitation and female genital mutilation/cutting led to a movement to better protect them.[39]Beginning in the early twentieth century, there arose a necessity under international law to protect, prevent and respond to the violence, exploitation and abuse of children in all contexts.[40] This resulted in a series of policies and programs which culminated in the adoption ofUnited Nations (UN) Convention on the Rights of a Child[41] (CRC) by the UN General Assembly in 1989. The CRC would enter into force the next year and since then the legal framework for

[37] ibid reg 2.10
[38]Graham Greenleaf and Bertil Cottier, 'International and regional commitments in African data privacy laws: A comparative analysis', *Computer Law & Security Review* (2022) (44) (105638) <*https://doi.org/10.1016/j.clsr.2021.105638*>accessed May 202022
[39]United Nations Children's Fund (UNICEF), 'History of Child's Rights' <*https://www.unicef.org/child-rights-convention/history-child-rights*> accessed 7 July 2022
[40] ibid
[41]Convention on the Rights of the Child General Assembly resolution 44/25, November 20 1989 (CRC)

the protection of children under international law has continued to grow with the adoption of three optional protocols to support the CRC[42].

Under international law, children are persons under the age of 18,[43] this is the same position under the Nigerian Child Rights Act[44] (CRA) which was passed in 2003 to domesticate the CRC and the African Charter on the Rights and Welfare of the Child[45] (ACRWC). The ACRWCexpressly protects privacy of childrenin its Article 10 and the CRC provides in Article 16 (1) that, 'no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.'

While it is established that as a subset of the general population, children require additional protection due to their peculiar nature,[46]as DS they also form part of vulnerable groups and the use of technology which collects and processes personal data can put children's right to privacy at greater risk of intrusion.[47] With a world that is becoming increasingly digitized, just like it is done for adults, there is a constant development of data driven technologies meant for the benefit and use of children and persons involved in parenting.[48] As a result, we find that children can be tracked online and businesses can collect and monetize

[42] UNICEF History of Child's Rights (n 40)
[43] CRC art 1
[44]Child Rights Act 2003 Cap C50 Laws of The Federation of Nigeria 2010 (CRA) s 16
[45]African Charter on the Rights and Welfare of the Child 1990 CAB/LEG/24.9/49 (ACRWC)
[46] Macioce (n 4); Henrietta Fore 'An open letter to the world's children'<*https://www.unicef.org/child-rights-convention/open-letter-to-worlds-children#digital*> accessed 22 May 2022
[47] Fore ibid; Eva Lievens and Valeria Verdoodt, 'Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation' *Computer Law & Security Review* (2018) (34) (2) 269–278. <*https://doi.org/10.1016/j.clsr.2017.09.007*> accessed 22 May 2022; Lina Jasmontaite and Paul De Hert, 'The EU, Children Under 13 Years, And Parental Consent: A Human Rights Analysis Of A New, Age-Based Bright-Line For The Protection Of Children On The Internet'*International Data Privacy Law*(2015) (5) (1) <*https://doi.org/10.1093/idpl/ipu029*> accessed 22 May 2022
[48]Claire Bessant, 'Sharenting: Balancing the Conflicting Rights of Parents and Children.' *Communications Law* (2018) (23) (1)7-24; Sonia Livingstone and Alicia Blum-Ross, *Parenting for a Digital Future: How Hopes and Fears about Technology Shape Children's Lives* (Oxford University Press 2020) 3

data[49] gathered from social media, smart toys,[50] and digital devices.[51]The personal data collected is also utilised to generate digital profiles, which are then used for data-driven customised services and targeted marketing.[52]

A report on the challenges to protecting the personal data of children in the modern day revealed that while these profiles, curated and gathered by the technological system may be helpful, often they are not.[53]More importantly, research has also revealed that, with increased internet and overall ICT usage by children of all ages, children are exposed to computer devices from an early ageand parents/guardiansare not always digitally literate and may be unware of the greater impact of how this data collection and the profiling will affect children when they get older.[54] Children themselves are also less likely to understand the long-term effects of sharing personal data in the time before they become adults.[55]

Granted that children lack theknow how to navigate the use of ICT, with the emergence and prevalence of sharenting, which is a portmanteau of the words 'share' and 'parenting' to describe the habitual use of social media to share news, images, etc. of one's child or children. The collection of children's data now

[49] Lievens and Verdoodt (n 47); S Sharma, *Data privacy and GDPR handbook* (John Wiley & Sons 2019) 319

[50]Piasecki and Chen (n 33); Liam Berriman and Giovanna Mascheroni, 'Exploring the affordances of smart toys and connected play in practice',*New Media & Society*(2019) (21) (4) 797-814

[51]MarsaliHancock and Sierra Hawkins, 'The importance of protecting and regulating children's personal data' (2019) <*https://www.openaccessgovernment.org/childrens-personal-data/69928/*>accessed 22 May 2020

[52] ibid

[53] ibid

[54]L Pasquale and others, 'Digital Age of Consent and Age Verification: Can They Protect Children? *IEEE Software* (2022) (39) (3) 50-57 <*https://doi.org/10.1109/MS.2020.3044872*> accessed 22August 2022; Karen McCullagh, 'The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?' in *Data Protection, Privacy And European Regulation In The Digital Age*, Tobias Bräutigam And Samuli Miettinen (eds), (Unigrafia, 2016) 110-139; Simone van der Hof and Eva Lievens, 'The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR' *Communications Law* (2018) (23) (1) 33

[55] UNICEF, 'Children's Online Privacy and Freedom of Information' <*https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1)*.pdf> accessed 22 June 2022

beginsprior to birth (through access to health data of parents or parents who share pictures of the ultrasound), and during infancybefore children are able to knowingly consent to its collection and use.[56]
While the world was coming to terms with the consequences of ICT on children's privacy rights, the COVID-19 pandemic happened and exacerbated already existing risks.[57]The pandemic necessitated lockdowns across the world,required parents and guardians tohome-school their children and wards with increasing help from the internet and technological devices which collect personal data. While distance learning[58] and home-schooling is not an entirely new development, it has since become a practice that involves the use of technology commonly referred to as education technology[59] (EdTech)which spiked during the period of enforced lockdown across the world[60] and has since continued even after lockdown restrictions were lifted. At the time, the UN Children's Fund (UNICEF) and its partners through a technical note raised an alarm at an increased risk of harm facing the privacy rights and general wellbeing of children due to less regulated communication, game-playing and learning with technological devices.[61]

In the years since the pandemic, the fears expressed by UNICEF have been confirmed, with an investigation carried out by Human Rights Watch revealing that 49 of the world's most populous countries (including Nigeria) harmed

[56] Bessant (n 48) 7; Fore (n 46)
[57] Jaclyn Jaeger, 'Coronavirus heightens focus on children's online privacy compliance' (2020)<*https://www.complianceweek.com/data-privacy/coronavirus-heightens-focus-on-childrens-online-privacy-compliance/28976.article*>accessed 25June 2022
[58] According to Sumner the first attempts at distance learning were made during the nineteenth century when print-based course materials were sent to learners through the postal service. Jenifer Sumner 'Serving the System: A critical history of distance education', *Open Learning: The Journal of Open, Distance and e-Learning* (2000)
(15) (3) 267-285
[59] Byeongwoo Kang, 'How the COVID-19 Pandemic Is Reshaping the Education Service' in J Lee and SH Han (eds) *The Future of Service Post-COVID-19 Pandemic*, (Volume 1 Springer, 2021) 15-36
[60]Jacob Hoofman and Elizabeth Secord, 'The effect of COVID-19 on education.' *Pediatric Clinics* (2021) (68) (5) 1071-1079
[61] UNICEF 'COVID-19 and the Implications for Protecting Children Online' (2022) <*https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf*> accessed 25June 2022

children's rights by endorsing online learning products and EdTechduring Covid-19 school closures without adequately protecting children's privacy.[62] The report stated that these products monitored or were capable of monitoring children, in most cases in secret and without the consent of the children or their parents. In other cases they collected personal information relating to the students location, activity in the classroom as well as identity of family and friends.[63]

Child rights experts under the auspices of UNICEF have suggested that reasons for repeated incidence of infringements into children's privacy is because interests of children do not feature at the forefront of design and implementation of technology.[64] They faulted the operations of data controllers and processors as well as software developers, who they argue are typically not trained in children's rights and do not prioritise children's interests. For the developers especially, it is said that they frequently, they do not develop or implement the additional safeguards required for children and their data.

Experts have alsoanalysed the privacy policies[65] of the leading technological companies in the world and found them to be complex, verbose and containing legal jargons confusing enough for an adult with above elementary education, let alone a child,[66]which results in DS including children and unsuspecting parents consenting to them without understanding them. The resultant effect is that it gives corporations the ability to defend their data collection practices in a lawsuit while making it more difficult for users to comprehend what is happening with their data.[67] Another criticism is that businesses have a typical privacy policy

[62]Human Rights Watch, 'How Dare They Peep into My Private Life?: Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic'(2022) <*https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments*>accessed 25 June 2022

[63] ibid

[64]Steven Vosloo and Melanie Penagos and Linda Raftree 'COVID-19 and children's digital privacy' <*https://www.unicef.org/globalinsight/stories/covid-19-and-childrens-digital-privacy*>accessed 22July 2022

[65] A privacy policy is a statement that is meant to reveal the methods a party will collect, use, disclose, and manage the data of a user, customer or client. It can be found on websites and with devices which collect and use personal data.

[66] Fore (n 46): Kevin Litman-Navarro, 'We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.' *The New York Times* (New York, 6 June 2019) <*https://nyti.ms/2T6YcqB*> accessed 22 July 2020

[67] ibid

which they use for different categories of customers without adapting it to meet different and specific peculiarities.[68]

In Nigeria, studies have revealed that one of the primary concerns around the collection and use of personal data in Nigeria is that children are exposed to privacy risks online and often lack the legal capacity to give valid consent, and may unknowingly disclose personal information to online platforms due to the appealing nature of their visual content.[69]In addition to these challenges, UNICEF has highlighted the failure of legal frameworks to adequately provide for the protection of personal data belonging to children, particularly for sensitive data of children and for the profiling of their data.[70]All of these are of serious concern and raises questions about how effectively the personal data of child is protected around the world and specifically in Nigeria.

Therefore, it is important to ensure that the privacy of children is protected online and when they use devices that can collect as well as store personal information. To achieve this, there is a need to adapt the right that children have to privacy and the special protection afforded them in different areas of life to the digitalage.[71]

4.0 Assessing the Protection Afforded Children under Data Protection Law in Nigeria, the United States of America, the European Union and China

4.1 The United States of America

[68] Nicole Olsen, '10 Common Privacy Policy Issues' (2022) <*https://www.privacypolicies.com/blog/privacy-policy-common-issues/#5_You_Don_T_Ask_For_Consent*> accessed 22July 2022
[69]C Izuogu, 'Personal Data Protection in Nigeria' (2018)<*http://webfoundation.org/docs/2018/03/WF_Nigeria_Full-Report_Screen_AW.pdf* > accessed 22 May 2020
[70] UNICEF, 'The Case for Better Governance of Children's Data: A Manifesto' (2022) <*https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf*> accessed 22June 2022
[71]Milda Macenaite, 'From Universal Towards Child-Specific Protection Of The Right To Privacy Online: Dilemmas In The EU General Data Protection Regulation' *New Media & Society* (2017) (19) (5) 765-799

In the United States of America (USA),children's online data is safeguarded by the Children's Online Privacy Protection Act of 1998[72] (COPPA) andits corresponding rule[73](the COPPA rule), enacted in 2000 to prescribe how the Act should be observed. COPPA is applicable to websites and online servicestargeted at children or to owners of such websites and online services (classified as operators)who knowingly collect personal information online from children.[74]
Under this legal regime, children are persons under the age of 13 and consent from a child is only valid if the holder of parental responsibility (parent or guardian) also grants consent which must then be verified through reasonable attempts[75]including, a consent form to be printed and returned via mail, fax or scanned; requiring holder of parental responsibility to use a credit card, debit card or other online payment system providing notification to the primary account holder; having the parent/guardian call or video conference with trained personnel on the staff; or by checking government issued identification.[76]
The COPPA however provides certain instances where verifiable parental consent will not be required, and these include when online contact information collected from a child is not retained and only used on a one time basis to respond directly to a specific request from the child.[77]

4.2 The European Union

In the EU, the GDPR in consideration of children's status as a vulnerable group, explicitly recognises that they deserve specific protection of their personal data and introduces additional safeguards in the exercise of their rights and for the operation of lawful basis for processing.[78] This recognition is evident throughout the GDPR and Recital 38 which expresses how going online can put children's right to privacy at greater risk of intrusion, underscores this by stating *inter alia* that 'Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.'

[72]Children's Online Privacy Protection Act, 1998 15 U.S.C. 6501–6506 (COPPA)
[73] COPPA Rules, Federal Register Volume 78, No 12
[74] COPPA s 1302 (2), 1303 (a) (1)
[75] ibid s 13012 (9)
[76] COPPA Rules s 312.5 (b)
[77] COPPA s 1303 (2)
[78] Sharma (n 49) 75,134

Children have the same rights as adults under the GDPR, the GDPR however provides extra safeguards explicitly for the children and separate rules apply to how they are to exercise their rights and how any of the lawful basis can be chosen when it comes to the personal data of children. For example, consent cannot be a gotten from a children under the age of 16[79] for processing by information society services[80] like social networks, online storage facilities and emails (other personal email).[81] So an information society service that processes the personal data of a child under 16 on the basis of consent obtained from that child will be liable for unlawful processing. Meaning that another lawful basis must be chosen before the personal data of a child under 16 can be processed. Parental consent is however not necessary for preventative or counselling services offered directly to a child[82] and children over 16 can give consent to an information society service.

For children under 16, consent has to be given or authorised by the holder of parental responsibility over the child and data controllers are obligated to verify (using available technology) that such consent was given or authorised by an actual holder of parental responsibility over the child.[83] While all DS have a right not to be subject to profiling, the GDPR provides that profiling measures where personal data is used for marketing purposes or creating personality/user profiles should not 'concern a child' except suitable measures are in place to protect the rights, freedoms and legitimate interests of that child.[84]To encourage the protection of the data privacy rights of children, the GDPRstates that a DS's right to erasure becomes particularly relevant if consent to process data was given as a child.[85]

4.3 The People's Republic of China

[79]GDPR art 8 (1). The GDPR however allows individual member states to lower the age of consent to a minimum of 13 years old.

[80]An information society service is a broad classification of services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. ibid art 4 (25); EU Directive 2015/1535 on Technical Regulations and of Rules On Information Society Services art 1

[81] Lenka Tomanova, 'What Is an Information Society Service' <*https://stentors.eu/articles/what-is-an-information-society-service*>accessed 6 July 2022

[82] GDPR recital 38

[83]ibid art 8 (1)

[84] ibid recital 71 and 75

[85]Ibid recital 65

In the People's Republic of China (PRC), the Regulations on the Protection of Children's Personal Information Online of 2019[86]applies to the collection, storage, processing, transfer and disclosure of personal data of children who are under the age of 14 by network operators within the PRC.[87]This regulation provides specific protection for children within the larger context of the Chinese Cybersecurity Law (CSL),which defines network operators as network owners, managers, and network service providers.[88]This phrase extends to every company that provides services or does business via a computer networkand therefore includes the collection and processing of children's data via websites, internet connected devicesand applications.[89]

The regulation requires network operators to notify and obtain theclear consent of guardians before they collect, use, transfer, or disclose the personal data of children younger than 14.[90]They are also required to appoint a dedicated person to protect children's personal data.[91]When obtaining consent, guardians must be given an option to withdraw the consent and they must be informed amongst other things of the consequences for refusal, the security measures in place, means to file complaints and the purpose for collection.[92]This purpose must not violate laws, administrative regulations or the scope of use agreed on by both parties.[93]

Network providers are prohibited from keeping children's personal datafor longer than is required to fulfil the purpose for which it was collected. When they do so,children or their guardians can explicitly request the deletion of data they have

[86]Regulations on the Protection of Children's Personal Information Online, 2019 <*http://www.cac.gov.cn/2019-08/23/c_1124913903.htm*>accessed 21 August 2022
[87]ibid art 2 and 3
[88]Cybersecurity Law of the People's Republic of China (CSL) (Effective June 1, 2017) art 76 (3)
[89]Jeff Edwards, 'Everything You Need to Know About China's Cybersecurity Law' <*https://www.ipswitch.com/blog/everything-you-need-to-know-about-chinas-cybersecurity-law*>accessed 21 July 2022; Gil Zhang and Kate Yin, 'China has released its version of COPPA'<*https://iapp.org/news/a/china-has-released-its-version-of-coppa/*>accessed 21 August 2022
[90]Regulations on the Protection of Children's Personal Information Online, 2019 art 9
[91] ibid art 8
[92] ibid art 10
[93] ibid art 11

collected.Furthermore network operators must also delete personal data when consent is withdrawn or the product or service is no longer used.[94]

The law does not provide any exemptions for when consent of a guardian will not be needed and neither does the CSL. So in practice, theprovisions of the Chinese Personal Information Security Specification of 2019[95](CPIS) which provides detailed consent standards is often resorted to.[96] Paragraph 5.6 of the CPIS provides a few exemptions to consent in situations such as when complying with laws, performance of a contract and processing in the national and public interest. Network operators are also mandated to employ encryption or other security measures to protect personal data that they have collected from children.[97]The law further directs network operators to ensure access to children's personal data is kept at a minimum and toimpose strong access controls on employees allowed to handle the personal data of children.[98]Before a third party can be contracted to handle children's personal information, security assessments must be conductedand parties must sign data-processing agreements.[99]

In the event that personal data of children leaks, gets damaged or lost, network operators are to immediately take remedial measures and if the situation is serious, they are to report to the relevant competent authorities and notify the children and the guardian who the information relates to.[100]Those who breach the law are subject to sanctions, including criminal penalties, under other applicable laws and regulations, such as the CSL.[101]

4.4 Nigeria

In Nigeria, the NDPR is the primary law on data protectionand while the data protection standards which it creates, undoubtedly extends to children, it does not give special attention to the peculiar nature of children and the need to adapt the guarantees covering them under law to protection of their personal data. The NDPR does not designate children as vulnerable and save for twoinstances within

[94] ibid art 20
[95]Personal Information Security Specification of 2019, GB/T 35273-2020(CPIS) <*https://www.tc260.org.cn/front/postDetail.html?id=20200918200432*>accessed 21 July 2022
[96] Zhang and Yin (n 89)
[97]Regulations on the Protection of Children's Personal Information Online, 2019 art 12 and 13
[98] ibid art 15
[99] ibid art 16 and 17
[100] ibid art 21
[101] ibid art 26

its provisions, it does not contain enough provisionstailored to protect the personal data of children. The relevant provisions are regulation2.4 (a) which forbids the seeking, giving or acceptance of consent in circumstances that may lead to atrocities and child rights violations and regulation 3.1 (1) which gives DS a right to have any information relating to processing of personal data provided to them by the data controller in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Where the DS is a child, such informationis tobe provided in writing, or by other means, including, where appropriate, by electronic or oral means.

Forbidding data controllers and processors from seeking consent in circumstances that may lead to atrocities and child rights violations is laudable and offers protection to the personal data belonging to children. Also, when information relating to processing is provided in a clear manner, it is expected that any inconsistency willalert the DS (in this case the child, their parent or guardian) to the possibility of violation of the rights of the child in any way. These provisions are however insufficient to combat the risks data collection, processing and storage pose to the privacy of children, particularly in light of the level of protection afforded children in the other jurisdictions highlighted.

The NDPR is silent on the age of giving valid digital consent and recourse has to be made to paragraph 5.5 of its Implementation Framework for guidance on who is even considered a child under the NDPR. The paragraph provides that a child for the purpose of the NDPR is any person younger than 13 and for businesses offering services to children to make sure they have child friendly privacy policies to enable children and parents be informed about the processing activity before granting consent. Neither the NDPR nor its Implementation Framework makes any mention of whether data controllers must take reasonable steps to confirm that permission has been granted or approved by a parent or legal guardian. There is also an absence of a provision on special protection that should be provided in relation to the handling and processing of children's data.

The absence of special provisions on the handling of children’s data coupled with the already existing deficiency of provisions on profiling as noted prior, could adversely affect the protection of personal data of children because the use of datain profiling and targeting activitiescan be biased, lead to discrimination,

exclusion, and marginalization.[102] Through profiling, more sensitive conclusions on children can be made. An example of this is given by Hildebrandt[103] when he describes how big data[104]may be analysed with the aid of computers to reveal patterns, trends, and associations, especially relating to human behaviour and interactions.[105]

When the shortcomings of the NDPR are considered alongside the growing rates at which children in the country use ICT for educational and social activities, it raises the question as to how the personal data which is collected during these activities is protected and safeguarded, because at the end of the day, unregulated processing of personal data belonging to children has human right implications and touches upon the right to privacy.Consequently, while the NDPR is a ground breaking regulation that set data protection standards and created data privacy rights for children, it is plagued with shortcomings and fails in more than one instance to adequately provide for the protection of personal data belonging to children.

5.0 Recommendations

Effective data protection in Nigeria will requirelaws as well as coordinated campaigns spreading awareness and ensuring implementation. While children will benefit from the protection afforded the general public, there is the need to consider their circumstance as a vulnerable group so that they are protected accordingly. To improve the level of protection afforded the personal data of children in Nigeria, the article makes the following recommendations:

i. The passing of a comprehensive law with protection tailored to children

Although the NDPR applies generally, it is not comprehensive, it does not provide for all the variables in data protection and has had to be supplemented by

[102]Solon Barocas and Andrew Selbst, 'Big Data's Disparate Impact' *California Law Review* (2016) (104) 671 <*https://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf*> accessed 12 March 2022

[103] M Hildebrandt,'Defining Profiling: A New Type of Knowledge?', inM Hildebrandt and S Gutwirth (eds),*Profiling the European Citizen*(Springer, 2008) 17-45

[104] ibid, big Data is an extremely large collection of data

[105] S Wachter and B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' *Columbia Business Law Rev*iew (2019) (2) (49)1

an Implementation Framework.The comprehensive law which the article recommendslaw should designate children as vulnerable inconsideration of their peculiarity and the need for special provisions protecting their personal data. The law should alsoclarifythe age of giving valid digital consentbecause it determines the point at which the data of children can be lawfully processed like that of adults.

There is uncertainty on the age at which children in Nigeria can give valid digital consent. Is it the age of 13 which the NDPR Implementation Framework sets as the age for children under the NDPR?If that is the case, this article puts forth an argument against it because there is no evidence to show that the drafters of the implementation framework conducted neither an analysis of children in Nigeria to understand their comprehension abilities nor anassessment of the age bracket that can understand standard privacy policies before setting that age. In light of this, there is the danger that children who do not have the maturity nor mental capacity to comprehend terms of service and privacy notices, have been given the right to consent and are therefore likely to be exposed to risks and threats to their personal data.

It is recommended the NDPB or the NITDA carry out a study to gauge the average comprehension abilities and levels of digital literacy among children in Nigeria and then based on the findings from that study, the age of digital consent in Nigeria can be set in this comprehensive law.The comprehensive lawshould alsorequirethat parental consent be gotten for children below the age of consent with an additional responsibility to verify such consent. The rules for verifying consent under the COPPA can be looked at as a guide in this regard. Provisions such as these, will make it easy to incorporate the other safeguards to protect the personal data of children.

Other safeguards are necessary because children might have ways to bypass consent thresholds[106] and individuals holding parental responsibility may not be digitally literate, therefore making them less than ideal persons to give consent to the processing of their child/wards personal data.

An additional safeguard that can be utilised is for the comprehensive law to direct data controllers and processors to design systems that consider the vulnerability of children. The law in China can serve as a guide here to require data controllers

[106] By lying or falsifying age credentials

to appoint a dedicated person to protect children's personal data. A provision on data protection by design also needs to be introduced into data protection law in Nigeria. The current requirement for data protection by design that can be found in the NDPR and its implementation framework only directs that systems are built and maintained with data protection in mind, so as to make requests, access and transfers seamless for DS.[107]

Data protection by designcan be utilized as a mechanism to ensure that systems are built in consideration of the vulnerability of children. To do this, a leaf can be taken from the GDPR which requiresorganizations to adopt special measures to protect children's rights[108] and also to implement appropriate technical and organisational measuresto ensure that, by default, only personal data which are necessary for each specific purpose are processed.[109]This can help level the gap between children's rights and ICT development in the country.

There is also a need to require everybody involved in processing to conduct compulsory Data Protection Impact Assessment (DPIA) before deploying technology that will process the personal data of children on a large scale. The closest the NDPR comes to providing for a DPIA, is the requirement for audits by organizations to state the policies and procedures of the organization for assessing the impact of technologies on privacy and security policies.[110] Moreover, while the GDPR utilises the word 'shall' in directing data controllers to carry out a DPIA, the NDPR implementation framework which is supposed to assist compliance with the NDPR, provides that a 'DPIA may be required' by the NITDA for processing which involves profiling, sensitive or highly personal data.[111] The implementation framework however provides that data controllers and administrators will need to carry out a DPIA as part of compliance.[112]

The comprehensive law also needs to address the issue of penalties as the penalties contained in the NDPR will fail to serve as deterrent because they are too meagre, the comprehensive law should contain more punitive penalties.Implementation of this comprehensive law should be also be supported

[107] NDPR reg 2.6, NDPR Implementation Framework para 3.2
[108] GDPR recital 38
[109] ibid art 25(1)
[110] NDPR reg 4.1 (5)
[111] NDPR Implementation Framework para 4.2
[112] ibid para 3.2

by a mechanism to inspect and gather data about violations and apply appropriate sanctions as necessary. Sanctions in the form of fines or custodial sentences must be pecuniary, to serve as deterrence while establishing and raising public confidence as well as trust in the enforcement mechanisms.

ii. An update and review of the NDPR to include protection tailored to children

This article acknowledges that the process of planning, drafting and passing a comprehensive legislation will take considerable time and effort. So in the meantime, it is recommended that a review and subsequent update of the NDPR be conducted, taking into consideration the paucity of provisions protecting children inherent side by side the vulnerability of children, the ubiquitous nature of technology and how much access children have to mobile devices and computers. The uncertainty regarding age of children can be addressed and provisions for dataprotection by design can be included so as to give children a higher level of protection.

6.0 Conclusion

This article has discussed data protection and how children have long been considered candidates for special protection as a vulnerable group. With a focus on Nigeria, this article argues that the special status afforded children ought to be no different in the protection of their personal data.

With the proliferation of different devices that can collect and process the personal data of children, there is the need for data protection law in Nigeria to better protect the personal data of children because of the risks posed to the privacy and indeed the entire wellbeing of children. To achieve this, the article has made some recommendations both long term and immediate.