 https://doi.org/10.53982/apblj.2019.0301.05-j

THE RIGHT TO ONLINE DATA PROTECTION OF CHILDREN: EXAMINING THE ADEQUACY OF THE LEGAL FRAMEWORKS TO COMBAT CHILD ONLINE DATA BREACHES IN NIGERIA

By
Thummim Iyoha-Osagie*, Orji Ikechukwu George**,

ABSTRACT

With the rise of digital technology and massive migration to the internet for daily activities, personal data of children is being breached on a large scale by schools, government, online platforms and even parents. It has been estimated that approximately one in three users of the Internet worldwide are under the age of eighteen. In addition to being increasingly active online, children also continue to depend on the Internet for a variety of uses such as play, communication and education. This implies that data belonging to children are frequently being collected through the use of gadgets, applications, and websites, and are sometimes sold or used for criminal activities. Several guidelines regarding children's online data protection have emerged globally such as the United States' Children's Online Privacy Protection Rule ("COPPA"), United Kingdom's ICO Children's Code (or Age Appropriate Design Code), and the General Data Protection Regulation (GDPR). However, there was no adequate provision for the protection of children's data in Nigeria until the enactment of the Nigeria Data Protection Act which is a step in the right direction, but is not without its flaws. This paper seeks to determine the adequacy of the legal frameworks generally in Nigeria to deal with child data breaches. It takes a comparative approach by analysing several legal frameworks in other jurisdictions, and proffers recommendations including amendment of legislations, online safety measures and awareness, privacy and data protection by design approaches for companies and adequate parental control measures.

Keywords*: Children, Data protection, Data privacy, Online data breach*

1. Introduction

Every day we engage in activities that necessitate the collection, processing and storage of personal data, hence the need for reasonable care to protect certain personal information. This process of information processing is further improved with the advancements in technology. All categories of data subjects are affected by this processes including children. The vulnerable nature of children makes them susceptible to abuse and exploitation, hence the need for adequate protection by law. Serious concerns have been raised about how children's right to privacy can be best preserved and protected given the fact that children's data can now be collected from the moment of birth. The sheer amount of digital information generated beginning from the developmental stages of a child's life is alarming[1]. Children have therefore become potential

* Thummim Iyoha-Osagie LL.M (Cyber Law) (Lagos), B.L, LL. B (Lagos). Researcher, Faculty of Law, University of Lagos, Lagos, Nigeria Email address: thummimiyoha@gmail.com, Phone Number: +234 810 1612 874

targets of a wide range of data privacy and protection abusers in the form of marketing, social influencers, sexual predators, criminals, amongst others. While interacting with social networks, a child may easily be manipulated into releasing vital personal information online hence exposing the child's vulnerability more.

According to the UK's Information Commissioner, Elizabeth Denham, 'In an age when children learn how to use an iPad before they ride a bike, it is right that organisations designing and developing online services do so with the best interests of children in mind. Children's privacy must not be traded in the chase for profit'[2]

The complexity of internet data flow remains a herculean task for other data subjects to understand; more so, children's data which presents a peculiar challenge that demands specialized approach. The imperative to closely monitor and protect children from unnecessary personal data exposure and processing is the fulcrum for legislative provision and other institutional framework for the protection of children's data. This paper presents an overview of the nature and types of online data breaches of children in Nigeria and globally. It also presents an examination of the extant laws available for the protection of personal data of children in Nigeria with a view to proffering solutions where gaps exist. It concludes by recommending a multi-stakeholder approach involving the government, parents, online media platforms and children in order to guarantee a seamless data protection of children in Nigeria.

2. Definition of Concepts

2.1 Child

A child is a person who has not reached the age of maturity, whether naturally, culturally or legally[3]. The age limit of children is usually set by provisions of

** Orji Ikechukwu George (Notary Public), LL.M (Cyber Law) (Lagos), B.L, LL. B (Jos). Senior Associate, Bridgeton Partners, Abuja, Nigeria. Email address: geo4iyke@yahoo.com, Phone Number: +234 807 400 8906

[1] A Singh & T Power 'Understanding the privacy rights of the African Child in the digital era' (2021) 21 African Human Rights Law Journal, 100 <http://www.scielo.org.za/pdf/ahrlj/v21n1/07.pdf> accessed 19 December 2023

[2] UK Information Commissioner's Office: <https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/news/15-ways-you-can-protect-children-online/ > accessed 26 November 2023

[3] O. Atoyebi, SAN & Joy Ayara. Omalex Law Firm "An Overview legal rights of a child in Nigeria" (June 7, 2023) <https://omaplex.com.ng/an-overview-legal-rights-of-a-child-in-nigeria/> accessed 9 December 2023

the law. It usually depends on the age the government or society considers that an individual has agency, or has become responsible and is able to make sound decisions.

The United Nations Convention on the Rights of a Child (CRC)[4] defines a child as an individual who had not attained the age of eighteen years unless under the law applicable to the child, majority is attained earlier[5]. Thus, the drafters of the legislation recognised that due to local peculiarities, countries might have varying provisions in their legislation on when majority is attained. The age at which an individual typically attains adulthood in legal terms is known as the age of majority. Most international legislation has eighteen years old as the limit, however, other countries have fourteen, sixteen, or twenty-one. Some countries also make a distinction between the legal age limit, age of majority, minimum age of marriage, sexual consent and criminal responsibility. The African Charter on the Rights and Welfare of the Child (ACRWC) which was enacted to promote the rights and welfare of the African child also recognises a child as one below the age of 18 years[6]. In Nigeria, the Child Rights Act also adopts the age of 18, which is further adopted by the Nigerian Data Protection Act, 2023 by the Interpretation section of the Act[7].
It is also worthy of note that the best interest of the child is to be the paramount consideration in any action taken with regards to a child.[8] A clear definition of the age of a child is necessary in every jurisdiction in order to determine the applicability of child data protection legislations for the purpose of policy formulation.

2.2 Data Protection

The term data protection refers to legal processes and rules that regulate the collection and limitation of usage of personal information of individuals. These rules determine the extent and conditions of usage of personal information.[9] Often used interchangeably with data privacy (though

[4] United Nations Convention on the Rights of a Child (CRC), 1989
[5] Convention on the Rights of a Child 1989, Article 1
[6] African Charter on the Rights and Welfare of the Child 1990, Article II
[7] Nigerian Data Protection Act 2023, Section 65
[8] Convention on the Rights of a Child 1989, Article III, ACRWC 1990, Article IV, Child Rights Act 2003, Section 1
[9] Blume, Peter 'Data protection and privacy – Basic concepts in a changing world' Scandinavian studies in law (2010) :151-164.https://www.scandinavianlaw.se/pdf/56-7.pdf accessed 10 August 2022

different[10]), the need for adequate protection for individuals personal information in commerce, health, education and other spheres have necessitated the enactment of legislation governing use of personal data. Data protection became prominent with the development of computers and its consequent technological advancement over the years with attendant explosion of personal information of natural persons.

> The Nigerian Data Protection Act 2023 (NDPA) defines personal data as:
> any information relating to an individual who can be identified or is identifiable, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual[11]
> While the General Data Protection Regulation defines personal data as:
> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[12].

It therefore follows that any pieces of information about a natural person whether analogue and digitals information that describes and identifies that person are the personal data of that individual. Thus information pertaining a child's date of birth, exam results and grades, medical records, images of pupils etc., are personal data.

Where such personal data relates to genetic and biometric data, race or ethnic origin, religious belief, health status, sex life, political opinions, trade union or such other special personal information, it is called sensitive personal data"

---

[10] There is a philosophical distinction espoused by different schools of thought, that data protection derives from and is same as the right to privacy on the one hand, and those who believe data protection should be detached; Adekemi Omotubora and Subhajit Basu, Next Generation Privacy, (2020) Information and Communications Technology Law, 29 (2) 151-173; Olumide Babalola, Privacy and Data Protection Law in Nigeria (2021) Noetico Repertum Inc.64-67.

[11]Nigeria Data Protection Act 2023, Section 65

[12] General Data Protection Regulation, 2018, Article 4(1)

2.3 **Consent**

The Nigeria Data Protection Act defines 'consent' as "any freely given, specific, informed, and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or to another individual on whose behalf he has the permission to provide such consent"[13]

2.4. **Sharenting**

This is the sharing of children content and information online by parents[14]. Sharenting is a combination of the words "sharing" and "parenting," signifying the behaviour of parents who disclose a lot of potentially delicate information about their kids online. Sharenting has a negative connotation of parents spending time online to share images and other personal details of their children.[15] Parents are considered the most active sharenters. Risks of sharenting include misuse of personal data of children by the sharing adult amongst others [16].

3. Data Protection and the Child

Under this heading, this paper will consider several related principles of data protection set out under various legislation and also the rights of a data subject as it relates to the child.

3.1 Protection of personal data of children

A data subject may be a child, and in such situation, all applicable laws on data protection would be applicable to the child data subject. However, special consideration is had to the child's vulnerability. It is in that circumstance that the law has provided for specific criteria for processing personal data of children. The reasons for these are not far-fetched, given that children often do

[13] Nigeria Data Protection Act 2023, Section 65

[14] Guilia Ranzini, Gemma E. Newlands, & Christopher Lutz, 'Sharenting, Peer Influence and Privacy Concerns: A Study on the Instagram-Sharing Behaviours of parents In the United Kingdom', <https://journals.sagepub.com/doi/pdf/10.1177/2056305120978376>, accessed 3 January 2024

[15] Ayten Dogan Keskin, 'Sharenting Syndrome: An Appropriate Use of Social Media?' <https://journals.sagepub.com/doi/pdf/10.1177/2056305120978376> accessed 23 January 2024

[16] Pamela Ugwudike, Anita Lavogrna and Morena Tartari, 'Sharenting in Digital Society: Exploring the Prospects of an Emerging Moral Panic', <https://www.tandfonline.com/doi/epdf/10.1080/01639625.2023.2254446?needAccess=true> accessed 27 January 2024

not have the requisite knowledge and thinking capacity to analyse situations and comprehend the risks involved in giving out their personal data.

While children's right to data protection are the same as other categories of data subjects, data controllers are expected to establish mechanisms that consider the peculiarity of personal data of children. It is important that the data controller simplifies the procedure for collection of personal data of the child to give room for simple understanding of risks involved and potential consequences of such actions, thus privacy notices for children must be simplified. Statutory and regulatory frameworks have thus established legal mechanisms for fortification of the right of the child to data protection. Section 31 of the Nigerian Data Protection Act, 2023, provides that;

> (1) Where a data subject is a child or a person lacking the legal capacity to consent, a data controller shall obtain the consent of the parent or legal guardian, as applicable, to rely on consent under this Act.
> (2) A data controller shall apply appropriate mechanisms to verify age and consent, taking into consideration available technology.
> (3) For the purposes of subsection (2), presentation of any government approved identification documents shall be an appropriate mechanism[17].

In essence, asides being a data subject who is entitled to the protections conferred by law, a child data subject, enjoys additional protection due his lack of legal capacity to make informed decisions, the data controller shall therefore obtain consent from the parent or legal guardian of the child. It is also a mandatory requirement in law, that the data controller verifies the age and consent particularly considering technological advancements. The duty of verification is one that must be discharged by a data controller by confirming through documentary evidence such as government issued valid means of identification or birth certificates to authenticate the veracity of any claim of age. Exceptions to the need for consent are made in the following situations:

> (a) where the processing is necessary to protect the vital interests of the child or person lacking the legal capacity to consent;
> (b) where the processing is carried out for purposes of education, medical, or social care, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality; or

[17] NDPA 2023; Section 31

(c) where the processing is necessary for proceedings before a court relating to the individual[18]

Clearly, in the absence of any regulations on the processing of data pursuant to the provisions of Section 35(5) of the NDPA, the provisions of the Nigeria Data Protection Regulation, Implementation Framework 2020 takes effect; the said framework makes it the obligation of the data controller and data processor to ensure the existence of a child-friendly privacy policy that enables children and their guardians make informed decisions on whether or not to grant consent based on a clear understanding of the privacy policy .

3.2 Principles of data protection

The processing of personal data must be in compliance with certain basic principles. These principles govern the processing of data of all data subjects including children, they are:

3.2.1 Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner. The data controller and data processor must ensure the existence of a lawful ground for processing personal data, carried out under conditions that are fair and open. Information pertaining the processing of the personal data must clear, unambiguous and easy to understand[19].

The data subject must ab initio, be subjected to a just and equitable procedure, and the imperative of accountability on the part of the data controller. Processing of data by the data controller should pass certain basic tests which includes:

a) granting of consent by the data subject;
b) performance of contractual agreements to which the data subject is party;
c) for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject;
e) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

[18] NDPA 2023, Section 31(4) (a-(c)
[19] General Data Protection Regulation 2018, Article 5(1)(a); NDPR 2019, Article 2.1(a); NDPA 2023, Section 24(1)(a)

f) For the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject[20].

When relying on lawful basis as the main credentials for processing the personal data of a child, the data controller must ensure the child understands clearly, unambiguously, and unequivocally, what he is consenting to. To process the personal data of a child pursuant to reliance on performance of a contract, the child must be competent to enter into the said contract, otherwise it becomes void and unenforceable.

Vital interest of the child entails that the processing shall be in the best interest of the child as envisaged by the Child Rights Act. While acting on legitimate interest, the right of the child to privacy and data protection remains paramount. The data controller must ensure that risks involved and ensuing consequences of every processing of the child's personal data is considered, and appropriate safeguards put in place.

3.2.2 Purpose Limitation

Personal data must be processed for a specific, clear and legitimate purpose[21]. At the commencement of the processing of personal data, the purpose for its collection must be clearly defined. Where circumstances arise in future on the necessity to further process the particular personal data, such further processing must be compatible with the initial purpose. In essence, data collected and processed for educational purposes in a school must not be further processed to include financial data. To determine compatibility with initial purpose, consideration must be taken to the relationship between the original purpose and the purpose of the intended further processing, the nature of the personal data concerned, the consequences of further processing, how the personal data has been collected, and the existence of appropriate safeguards[22].

The only exceptions to this principle is where the further processing of the data is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, no assessment of compatibility of purposes is required as it is considered not to be incompatible with the initial purposes, as provided in Section 24(4)(b) of the Nigeria Data Protection Act, and Article 89 (1) of the GDPR, subject to implementation of guarantees by

[20] GDPR 2018, Article 6.
[21] NDPA 2023, Section 24(1)(b); GDPR 2018, Article 5(1)(b)
[22] NDPA 2023, Section 24(4)

the data controller in order to safeguard the rights and freedoms of the data subject.[23]

Such guarantees are given through the implemented technical and organizational measures, which retain the processed information to the bare necessary minimum.

3.2.3 Data minimization

Collection and processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed[24]. This means that the controller is duty bound to process personal data only when it is adequate and appropriate. He must also ensure the data processed are relevant and crucial for achieving the purpose and without which its realization is not possible.

It is pertinent to state that proper assessment is made to arrive at what is appropriate to the purpose and to avoid irrelevant information. A good example is where the personal data of a child is collected and processed at school, it would be inappropriate to collect the child's data pertaining to ethnicity, religion etc., which might be taken as excessive particularly where the need for the data may be accomplished without the excess data. Such data would also not be collected for the purpose of future speculations or belief that it may come handy in future.

3.2.4 ***Accuracy***

Personal data collected must be accurate, complete, not misleading and where necessary kept up to date[25]. Inaccurate personal data, must erased or rectified without delay. It is the responsibility of the data controller to verify that the source of the data collected is dependable and trusted.

3.2.5 ***Storage Limitation***

Personal data must be stored for a limited duration[26]. They must not be stored for an unreasonably long period. The storage period may be stipulated by law[27]. In the absence of a codified duration of storage, it is reasonable for the

[23] GDPR 2018, Article 89(1), NDPA 2023, Section 24(4)(b)
[24] GDPR 2018, Article 5(1)(c); NDPA 2023, Section 24(1)(c)
[25] NDPA 2023, Section 24(1)(e)
[26] GDPR 2018, Article 5(1)(e); NDPA 2023, Section 24(1)(d)
[27] In Poland for instance, the employer is obliged to store the employee's work file for up to 10-50 years after the termination of the employment agreement, https://www.rsm.global/poland/en/insights/hr-payroll/employee-documentation While in

data controller to store the data for a reasonable time depending on the purpose of collection[28]. Upon the expiration of the expected period of storage and holding of the data, the Data Controller should erase the personal data collected, processed and stored.

In Nigeria, the retention period of personal data is not stated under the NDPA. This may then be attributed to the variation in different circumstances based on contractual terms or other existing laws. Section 27(1) (e) of the NDPA 2023 provides that as part of his duty to the data subject, the data controller shall inform the data subject of the retention period of his personal data. It is incumbent on the data controller to avail the data subject of this information prior to the commencement of the processing of the data, thus it is a condition precedent to the processing activity.

The exception however is only for archiving purposes in the public interest, for scientific or historical research purposes. Such measures may include techniques like data pseudonymisation or anonymisation whose application can lower the risks to the data subject and help data controllers to fulfil their obligations in relation to data protection[29].

3.2.6 *Integrity and Confidentiality*

Processing of personal data must be done in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures[30]. It is incumbent on the controller to ensure that personal data is processed in a way which guarantees an appropriate level of security[31]. Thus such breaches like identity theft, credit card scams, cyber fraud can be averted by adherence to this principle.

3.2.7 *Accountability*

The controller is required to observe all the principles, and be able to demonstrate compliance with them. The law imposes a duty of care on the

---

Bulgaria, Article 12, Accounting Act, allows employers to retain records of employee payroll records for up-to 50 years.

[28] Zhivka Mateeva,'Principles of Personal Data Protection', (2020) Xususi Buraxilis, Special Issue Vol 28 < https://www.researchgate.net/publication/342527554_Principles_of_personal_data_protection > accessed 11 August, 2023

[29] Ibid

[30] GDPR 2018 Article 5(1)(f), NDPA 2023, Section 24(2)

[31] NDPR 2019, Article 2.1(1)(d)

Data Controller and the data processor to demonstrate accountability and responsibility in the enforcement of all the principles[32].

3.3 **Rights of a Child Data Subject**

Data subjects including children, are entitled to certain rights, which are geared towards preventing infractions and violations of the data subject rights. These rights include:

3.3.1 ***The Right to Information***

The law places a fundamental duty on the data controller and data processor, to inform the data subject adequately and timeously of the processing of his personal data. The information must be clear, unequivocal, unambiguous, specific about the nature of the data to be processed, purpose, and the quantum of data involved. In this instance the children or their parents/legal guardians must be adequately informed of the storage period of their personal data, and recipients or potential recipients of their personal data, particularly where the said recipients are in countries outside Nigeria or International organisations[33]. The child must also be availed the opportunity of knowing who the data controller is, with respect to adequate, clear and verifiable information about the controller.[34] Any potential transfer of his personal data to a foreign country or entity must be communicated to the child/parents/legal guardians, as the case may be. Where the personal data had already been transferred to the foreign country or entity, the child data subject has the right to be informed of appropriate safeguards for data protection in the foreign country or entity[35].

3.3.2 Right to Complain

The child data subject is also entitled to make complaints to the appropriate quarters in relevant situations. The data subject is entitled to lodge a complaint before a supervisory authority like the NDPC where breaches occur or likelihood of breaches exist[36].

3.3.3 Right of Objection to processing of personal data:

A child has a right to object to the processing of his personal data, it is immaterial that he had initially given his consent; such consent may be withdrawn by the child data subject and objection raised on the continued processing of his personal data. Such objections may be raised where there is a

[32] NDPA 2023, Section 24(3)
[33] NDPA 2023, Section 34(1)(a) NDPR 2019, Article 3.1(1)
[34] NDPR 2019, Article 3.1(7)
[35] NDPR 2019, Article 3.1(8)
[36] NDPA 2023, Section 34(1)(a)(vi), NDPR, 2019, Article 4.2,

likelihood or actual substantial damage or distress to the child.[37] This right puts the controllers' activities in check. The instances include situations where the accuracy of the personal data processed in school is contested or where medical records of the child is released to third party unlawfully[38].

3.3.4 Right to access personal data:

The opportunity afforded a data subject to access his personal data in the possession of the data controller, is a legal right in law[39]. The said personal data is expected to be in an easily ready and accessible form. A good example of this right would be access to academic records in schools, or access to their data on any online media platform where their data had been shared.

3.3.5 Right to rectify personal data:

It is within the right of the child data subject to rectify his personal data, where the need for accuracy arises and the data controller is duty bound to notify recipients of the child data subjects' data of existence of any rectification[40]. Where a school wrongly records the name of a child, it is his right to request that appropriate step be taken to reflect the correct name.

3.3.6 Right to request erasure of personal data:

Erasure of the data subject' personal data is also a right conferred on the data subject in law. The moment the child data subject makes such a request, the data controller must proceed and delete the affected personal data. The request may be predicated on the grounds that the personal data have served its purpose and therefore need not be retained; or that the child data subject has withdrawn his consent; or the personal data was unlawfully processed; the data subject has raised objection to the processing and there is no overriding legitimate ground for processing same; and where the erasure is in compliance with a legal obligation[41].

3.3.7 Right of data portability:

The data subject has the right of transmission of his data from one controller to another. The data in the instant situation is encouraged to be in an electronic format for easy movement and readability. Where it is impracticable for the data controller to keep the data in machine readable format, perhaps due to cost, the data subject may bear the financial burden[42].

---

[37] NDPA 2023, Section 36(1)
[38] NDPA 2023, Section 36(1), NDPR, 2019, Article 2.3
[39] NDPA 2023, Section 34(1)(b)
[40] NDPA 2023, Section 34(1)(c); NDPR, 2019, Article 3.1(13)
[41] Nigeria Data Protection Act 2023, Section 34(1)(d)(2)
[42] NDPA 2023, Section 38

3.3.8 Right to withdraw consent:

Having granted his consent for the processing of his personal data, the child data subject retains the right to withdraw consent he previously granted. There is also a legal burden placed on the data controller to not only notify the data subject ab initio of the existence of this right, but to ensure that it is as easy to withdraw consent as it is to give[43].

3.3.9 *Right not to be subject to automated decision-making:*

The child data subject shall not be subject to a decision based solely on automated processing of personal data, including profiling, direct marketing etc. Such automated processing may only occur where the data subject gives his consent or where it is necessary for the performance of a contract between the data subject and the data controller or where it is authorized by law provided safeguards are established to avert a breach of the data subject's fundamental rights[44].

3.4 **Parental Consent and Child Data Protection**

Consent of the data subject is any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her. Consent may be made through a written statement, sign or an affirmative action signifying agreement to the processing of personal data. Granting of consent by a data subject who is a child is dependent on the decisions of their parents or legal guardians. This position of the law is geared towards protecting children and ensuring that their best interest is paramount consideration in making these decisions. Determining the legal capacity of children to consent to the processing of their data may not be as easy as it seems on the surface. It is even most difficulty to determine capacity to consent of a child in the digital era where the person behind the screen is anonymous, and in the face of identification challenges.

Giving and obtaining consent is governed by certain principles which include: [45]

a) Transparency: privacy policy must be explicit and unambiguous;
b) Consent must be express and not implied consent; thus silence, pre-ticked boxes or inactivity on the part of the data subject or his legal guardian, do not constitute consent;

[43] NDPA 2023, Section 35
[44] NDPA 2023, Section 37
[45] NDPA 2023, Section 26

c) Consent must not be bundled: There must be consent for different types of data processing activities. Consent request must be separated from the general terms and conditions.

It is the responsibility of the data controller to establish that a data subject's consent was duly obtained. It is the law that such consent must be active; as such silence or inactivity on the part of the data subject shall not be construed as consent. The data controller is duty bound to inform the data subject prior to the granting of consent, of the existence of his right to withdraw consent Request for consent must be in clear, simple language and accessible format. It must be in the affirmative and not based on a pre-selected confirmation; and may be provided in writing, orally, or through electronic means.

One pertinent fact is the understanding that while parents and guardians have been saddled with the responsibility of granting consent on behalf of their children, they may have some handicap of not being tech savvy enough and not necessarily equipped and up-to-date with appropriate information to enable them make right decisions in the child's interest. These may in the long run affect the quality of decision or access of the child to required information and platforms; thereby making the said parental consent a double edged sword, meant to protect on the one hand, but which has become on another hand, a source of restriction of knowledge.

Parents must also be knowledgeable enough to understand the workings of the law of privacy and personal data protection to be better positioned to protect their children. It is also incumbent on the data controller to ensure that parental consent is obtained always. The basis for parental consent is to ensure children are safeguarded from harm, the harm which propensity have exponentially increased in the digital era.

4. The Adequacy of the Legal Framework for Combating Child Online Data Breaches in Nigeria

An overview of the legal frameworks for privacy and child rights in Nigeria generally would reveal that most of the legislation are not adapted to the online environment. In addition, although they provide for general privacy rights, they do not contain specific provisions on child data protection safe the National Data Protection Act, 2023. This Act has saved the day with respect to children's data protection although some amendments to the Act are still desirable to make it suitable for protecting children from online data breaches.

4.1 The Constitution of the Federal Republic of Nigeria, 1999

The Constitution of the FRN is the grund norm and principal legislation in Nigeria from which all other legislation derive their legitimacy, as every other legislation that is inconsistent with the constitutional provisions is void[46]. This means that the right to privacy, dignity and freedom of expression also applies to children. Section 37 of the 1999 constitution provides for the privacy of citizens, homes, correspondences and telephone communications. This constitutional alignment establishes a foundational basis for safeguarding children's data generally. It does not specifically provide for online data protection of children.

4.2 The UN Convention on the Rights of a child / Child Rights Act, 2003

The UN Convention of the Rights of the Child was ratified by Nigeria in 1991. The Child Right's Act was then adopted in 2003 to domesticate the provisions of this convention into our municipal laws. The CRC contains several provisions relating to the child including privacy, but does not contain provisions about personal information or data of children. Article 16 of CRC provides:

> (1) 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.
> (2) The child has the right to the protection of the law against such interference or attacks.

The Child Rights Act in Nigeria is a Federal Law and is only applicable to states who have localised it. As at December 2023, all 36 states and the Federal Capital Territory have passed the Law. The last state to pass the law was Kano state, whose legislature passed it on 24 May 2023.[47]

The Child Rights Act is a very comprehensive piece of legislation dealing with all matters pertaining to the Nigerian child from the protection of the rights of a child. By virtue of section 3 of the Child Rights Act[48], all the fundamental rights provisions contained in Chapter IV of the 1999 Constitution apply to children. Although there is no specific mention of online data protection in the Act, several other provisions could be used to imply the protection of

[46] Constitution of the FRN, 1999 (as Amended), Section 1
[47] Vanguard News, 'Kano Assembly passes Child Right Protection Bill' (May 4 2023) https://www.vanguardngr.com/2023/05/kano-assembly-passes-child-right-protection-bill/ accessed 30 January 2024
[48] Child Rights Act, 2003

children's data online. The right to privacy of the child is covered under the Act. It provides that every child has the right to his or her privacy, family life, home, letters, phone conversations, and electronic communications, and that no child should be exposed to interference with this right[49]. However, it provides that the above provisions do not impede a parent's or legal guardian's ability to exert reasonable oversight and influence over their child or ward's behaviour[50]. This still gives significant control to the child's parents over the child's privacy.

The Act further prohibits publication of a child's name and sensitive personal details where he is being subjected to a judicial process. In order to aid further protection of the child, the Act restricts persons from publishing the name, residence, school, photograph, or anything else that could be used to identify a child whose case is before the Court[51]. This would be very applicable to online data protection due to the prevalence of social media and other online channels (such as Facebook, Twitter, etc.) through which information could be easily disseminated within seconds. The Act penalises the above with a fine of fifty thousand naira or imprisonment for a term of five years or to both. This shows the gravity of such offence as publicising details a juvenile could lead to attacks on the child's reputation, including demeaning treatment for the child and the parents. Such undue exposure could further interfere with the justice process and affect that child's future adversely. Section 205 further reiterates this provision by providing that at all levels of the child justice procedure, all records must be kept confidential and must only be exposed to people who have a connection directly with the case.

4.3 African Charter on the Rights and Welfare of the Child:

The African Children's charter equally states that the best interest of the child is to be considered paramount consideration in any actions taken pertaining to that child[52]. Thus, within the context of our paper, in dealing with children's data or privacy, the best interest of the child is to be considered. The data of the child is to be dealt with in a manner that is not inconsistent with the child's well-being. The protection of the child's privacy is enshrined in Article 10 thus:

> No child shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to the attacks upon his

[49] Child Rights Act, 2003; Section 8(1) (2)
[50] Child Rights Act 2003; Section 8 (3)
[51] Child Rights Act 2003; Section 205
[52] ACRWC 1990, Article 4

> honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.[53]

Although no mention of 'data' is made, we can only envisage that the provisions encompasses children's data. It is recommended that personal information of children be included as this is paramount to their privacy. Concerning the exercise of 'reasonable supervision' by parents, Sillah and Chibanda show concerns that this provision might lead to abuse of privacy rights of children in a bid to reasonably supervise their conduct[54]. However, since the drafters of the charter might not have envisaged this interpretation, parents can create a conducive atmosphere for the protection of the African child where the child is not totally robbed of autonomy with regard to control of their personal data[55]. African children generally have also been taught subjection to parents some times to the detriment of their own rights and expression. Parents should also be weary of sharing excessive personal information of the children on digital platforms in exercise of their oversight rights, otherwise called 'sharenting'.

The African Union Convention on Cyber Security and Personal Data Protection[56] unfortunately contains no provision on processing of children's data. Similarly, the Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime and even the ECOWAS Supplementary Act on Personal Data Protection[57] which makes provision for all member states to set up a legal framework for protection of personal data also contains no specific provision on the processing of personal information of children in the region.

---

[53] African Charter on Welfare and Right of the Child, Article 10

[54] RM Sillah & TW Chibanda 'Assessing The African Charter on the Rights and Welfare of the Child (ACRWC) as a blueprint towards the attainment of children's rights in Africa' (2013) 11 IOSR *Journal of Humanities and Social Sciences* 53.

[55] A Singh & T Power 'Understanding the privacy rights of the African child in the digital era' (2021) 21 African Human Rights Law Journal, 115 <http://www.scielo.org.za/pdf/ahrlj/v21n1/07.pdf> accessed 19 December 2023

[56] Adopted by the 23rd Ordinary Session of the Assembly of the Union, Malabo, 27th June 2014.

[57] Supplementary Act A/SA.1/01/10 On Personal Data Protection Within ECOWAS, 2010

4.4 The Nigerian Data Protection Act (NDPA), 2023:

The NDPA contains some express provision on processing of children's data which is a welcome development for the Nigerian child. Prior to the enactment of the NDPA, the Nigeria Data Protection Regulation (NDPR)[58] and its Implementation Framework[59] mostly governed the processing of child personal data prior to the enactment of the Nigeria Data Protection Act (NDPA) 2023. A person under the age of 13 was considered a child for the purposes of the NDPR[60]. Before obtaining consent, data controllers or processors whose processing activity targeted minors had to make sure that their privacy policies were written in a way that was child-friendly and intended to help children and their guardians understand the nature of the data processing activity. However, the new NDPA has a new age restriction which is a person under 18 years[61].

The Nigeria Data Protection Commission (NDPC) is authorised by the NDPA to formulate regulations concerning the protection of 13-year-olds and older children regarding the provision of information and services through electronic means upon the express request of the child[62]. Hence, with regard to the processing of data from children in the aforementioned age group (13 years and older but under 18), we should anticipate particular guidelines from the regulatory agency. It is instructive to understand that pursuant to Section 64 of the NDPA, regulations made prior to the coming into effect of the NDPA, which are not in conflict with the NDPA, shall continue in effect until they are repealed[63].

Certain domestic frameworks offer children more explicit protection than others. For example, the Data Protection Act, 2012 in Ghana[64] and the Protection of Personal Information Act, 2013, in South Africa forbid processing children's personal information unless one of the exceptions—such as the parent or guardian's consent—can be proven[65]. According to Kenya's Data Protection Act, 2019, processing of children's personal data is prohibited unless the child's parent or legal guardian gives consent and the processing is

[58] NDPR 2019, Article 3.1 (1)
[59] Nigeria Data Protection Regulation: Implementation Framework (2020)
[60] Ibid, Article 5.5
[61] NDPA 2023, Section 65; A Child has the same meaning ascribed under the Child Rights Act, No. 26, 2003
[62] NDPA 2023, Section 31(5)
[63] NDPA 2023, Section 64 (2)(f)
[64] Ghana Data Protection Act 2012; Section 37, Section 39, Section 40
[65] Protection of Personal Information Act, 2013; Section 11(1); Section 35(1)(a)

done in a way that upholds the child's rights and best interests[66]. In order to process the data, a data controller or processor must also include the necessary procedures for age verification and consent.

5. Comparison of the legal framework for combating child online breaches in other jurisdictions: United Kingdom, European Union and the United States

5.1 The General Data Protection Regulation

The EU GDPR is the data protection regulation available in the European Union. It contains detailed principles for data processing, consent, marketing, right of access and withdrawal amongst several other rules. Since the Brexit, the United Kingdom has both the UK Data Protection Act, 2018 and the UK GDPR which is not too different from the EU variation.

The GDPR contains specific provisions in relation to children's data and provides for fair processing. The rationale is captured in the recital which provides that specific protection should be accorded to the processing of children's personal data since they might be less knowledgeable of the risks, consequences and their rights in this regard.

> Children require 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. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child [67]

Article 8 of the GDPR first states the age of consent. The default age for a child to provide their own consent for information society services is set at 16 years. Member states have the discretion to lower this age, but it must not be below 13 years. It further makes provision for Parental Consent where it states that If a child is below the defined age of consent, processing of their personal data is only lawful if consent is given or authorized by the child's parent or legal guardian. On verification of consent, it provides that service providers are required to make reasonable efforts to verify that consent is given or authorized by the holder of parental responsibility for the child, taking into account available technology.

[66] Kenya Data Protection Act 2019; Section 33(1)
[67] Recital 38 of the GDPR

The GDPR further provides that information addressed to children regarding data processing should be in clear and easy to understand language[68]. The right to rectification or erasure also applies to children. The GDPR provides that where the data subject had initially given consent to processing of their data as a child, and chooses to withdraw such content such right should be given them. This relates to personal data of such a child available on the internet[69].

5.2 UK Age appropriate design: a code of practice for online services (Children's code)

The code lays out the expectations for all companies that design, develop, or manage online services, such as educational websites, social networking platforms, online games, apps, internet connected toys, and streaming services. It provides instructions on data protection measures that guarantee children's data protection when accessing online services. It does not apply to schools who are engaged in the processing of children's data under the age of 18 years, but it applies to edTech companies[70]. These companies are also enjoined by the code to comply with the provisions of the UK GDPR and DPA 2018.

The code contains fifteen standards that designers of children's online services are to comply with in processing of children's data. Firstly, the best interest of the child is to be of paramount consideration in the use of children's personal data. It should not be processed in such a manner as to expose the children to any form of abuse, or interfere with their physical, mental or emotional development. They are also to acknowledge the duty of the parents in safeguarding their data and provide all necessary support in this role. We agree that the acknowledgment of the parental control or supervision particularly for younger children who may not comprehend the importance of data protection is paramount. It would safeguard them from online harms. The code also provides for Data Protection Impact Assessment (DPIA) to evaluate and reduce risks that the data processing poses to the rights of children who are likely to use the service. The code further makes provision for transparency in information given to users, high privacy by default standards, data minimisation, and parental controls.

---

[68] GDPR 2018, Recital 58
[69] GDPR 2018, Recital 65
[70] ICO: Introduction to the Children's Code < https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/> accessed 24 December 2023

Several African countries needs to take a leaf from the UK Children's code and provide specific legislation for children's online data protection. Although some efforts have been made by some African countries such as Zambia, Ghana and South Africa to create policies or amend legislation to include children's internet safety are also. In Zambia, the Ministry of Transport and Communication launched a 'Child online protection strategy'[71] in 2020 whose aim is to protect children from online abuse, regulate online content and ensure a safe cyberspace generally for children.

In South Africa, the Children's Amendment Bill[72] was released in 2020 which was to the amend the provisions of the Children's Act, 2005 in providing protection for children's personal information in alliance with the Protection of Personal Information Act, 2013. Prior to this amendment, the Act made no provisions for the protection of personal information of children.
In Nigeria, the National Information Technology Development Agency (NITDA) released a Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries in 2022 which recognises the need to protect children online, as they are present online without supervision. It aims to protect children from sexual abuse, illicit content and exploitation but makes no specific reference to child privacy.

5.3 The United States Children's Online Privacy Protection Act[73]

The Children's Online Privacy Protection Act (COPPA) contains several provisions aimed at protecting the privacy of children online. According to the Act, a person under the age of 13 is considered a "child," and personally identifiable information gathered online about such an individual is considered personal information. This entails first and last name, address, phone number, email address, social security number, screen name, and other information that could be combined with other information to identify a person are all considered personal information. The key provisions include:

5.3.1 Parental Consent**:**

Websites and online services directed towards children under 13, or those with actual knowledge that they are collecting personal information from children, must obtain verifiable parental consent before collecting, using, or disclosing

[71] Zambia launches national strategy to protect children online (27 August 2020) https://dig.watch/updates/zambia-launches-national-strategy-protect-children-online accessed 28 January 2024
[72] Children's Amendment Bill (B19–2023)
[73] 15 U.S.C. 6501–6505, 1998

personal information[74]. This consent can be obtained through a signed consent form, use of a credit or debit card or through the telephone.

5.3.2 Notice and Transparency:
Operators of websites or online services must provide clear and understandable notice of their information practices, including the types of information collected, how it will be used, and the disclosure practices[75].

5.3.3 Access to Parents:
Parents have the right to review the personal information collected from their children, and they can also request that the information be deleted[76].

5.3.4 Data Security:
Operators must take reasonable steps to ensure the security of children's personal information, including protections against unauthorized access, disclosure, and use[77].

The provisions of the Act are also enforced by the Federal Trade Commission in the US which imposes high penalties for defaulting companies. It is a commendable step that the Act could be enforced by the commission.

5.4 Breaches and Consequences of breaches of children's online data.
In Nigeria, breaches of personal data of data subjects has become rampant. In October 2023, for instance, a group of freshly graduated students of the University of Ilorin received the shock of their lives, when after celebrating their graduation, they received personal messages from a serving senator congratulating them on their graduation, this without giving consent for such information as contacts be shared.[78] Also in July 2022, the Plateau State Contributory Health Care Management Agency(PLASCHEMA), experienced a major breach of over 75,000 data subjects including children[79]. In 2023

[74] COPPA 1998, Section 6504
[75] COPPA 1998, Section 6502
[76] COPPA 1998, Section 6503
[77] COPPA 1998, Section 6506
[78] Usman Aliyu, News Agency of Nigeria (NANS) 'Data breaches and Nigerians right to privacy' (23 December 2023) <https://nannews.ng/2023/12/23/data-breaches-and-nigerians-right-to-privacy/, accessed 26 January 2024
[79] People's Gazette 'Nigerian agency data breach exposes 75,000 personal details of citizens online' (19 July 2022) <https://gazettengr.com/nigerian-agency-data-breach-exposes-75000-personal-details-of-citizens-online/,> accessed 23 January 2024

alone, financial institutions in Nigeria were fined over 200 Million Naira, for various degrees of data processing infractions.[80]

Violations of the protections over a child's personal data as enshrined in law may result in severe consequences, such as sexual exploitation, cyber bullying, identity theft, financial crimes against the child and even death. These violations may come in different forms such as surveillance, online sexual exploitation, automated processing, unintended disclosures, sharenting amongst others[81].

The NDPA places a burden on the data processor under whose watch a personal data breach occurred, to immediate notify the data controller of the breach, with details of the breach with respect to nature and number of person affected[82]. He must also communicate every information required by the data controller for purposes of compliance. The controller has a statutory obligation to ensure it notifies the NDPC within 72 hours of his knowledge of the said breach, with a description "where feasible" of the nature of data affected and the number of persons involved[83].
The data controller must also inform the data subject of the said breach and its potential risks in a clear and precise language; and shall offer advice on how to mitigate the effects of the said breach[84]. Where the personal data of a child has been breached, he may through his parents/guardian lodge a complaint at the NDPC[85]. The NDPC shall in turn investigate and where appropriate, impose penalties on the data controller or data processor[86]. Such penalties may be compensation for injury and loss suffered.[87] This step does not preclude the right of the child to seek redress in court[88]. Thus the child may sue through their legal guardian in a court of competent jurisdiction

[80] Staff Writer, TechPoint Africa 'Nigerian banks and institutions fined over N200 million for data privacy violations' (20 June, 2023) <https://techpoint.africa/2023/06/20/nigerian-banks-fined-200-million-data-privacy-violations/ > accessed 26 January 2024
[81] UNICEF - Legislating for the digital age; Global Guide on improving legislative frameworks to protect children from online sexual exploitation and Abuse, (10 May 2022) <https://www.unicef.org/reports/legislating-digital-age> accessed 1 December 2023.
[82] NDPA 2023, Section 40(1)(a)
[83] NDPA 2023, Section 40(2)
[84] NDPA 2023, Section 40(3)
[85] NDPA 2023, Section 46
[86] NDPA 2023, Section 47
[87] NDPA 2023, Section 48(2)
[88] NDPA 2023, Sections 50, 51

The consequences of child data breaches can be devastating and even life threatening. In what experts described as the worst known hack aimed at children, V Tech Holdings, a manufacturer of digital toys, announced that 6.4 million children's personal information had been compromised. The company revealed that more children were impacted by the hack on the databases for the Learning Lodge app store 4.9 million adults it earlier revealed on a dark web site by the perpetrator[89]. In another child data breach report, school files from hacker's websites were replete with children's personal information. Data from about 1,200 American K–12 schools was leaked by ransomware gangs in 2021[90]. The analysis also added that delicate personal information, such as health issues or family financial situations was contained on these websites. A child may be at risk of identity theft for the rest of their life if their personal information, like their birthdays or social security numbers, is stolen. These emphasises the need for protection of children's data in Nigeria and globally. Other consequences include reputation damage, economic exploitation, sexual exploitation, and exposure to cybercrimes.

5.5 **Necessity of Data Protection Impact Assessments**

Data Protection Impact Assessments(DPIA) is a process designed to identify the risks and impacts of proposed or envisaged processing of personal data.[91] It places a burden on the data controller to assess and mitigate potential risks that may occur in the course of processing personal data of certain individuals to their rights and freedom.[92] By their nature and vulnerable state, children data clearly fall under this category of data. Thus a controller must identify the need for a DPIA at the beginning of the process, describe the processing i.e if children would be affected, assess the necessity and proportionality of the processing by consulting children and their parents, identify and assess the risk such as online sexual grooming etc, explain the necessity for compliance, and state measures taken to address the risks. The Data Controller is also under obligation to consult the NDPC where the propensity for high risks are still present after taking all necessary mitigating steps.

---

[89] CNBC, Cybersecurity "VTech hack: Data of 6.4M kids exposed", (2 December 2015) https://www.cnbc.com/2015/12/02/vtech-hack-data-of-64m-kids-exposed.html accessed 28 November 2023

[90] NBC News, "Hackers are leaking children's data — and there's little parents can do" (10 September 2021) https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926 accessed 28 November 2023

[91] Nigeria Data Protection Act, Section 28(4)

[92] Nigeria Data Protection Act, Section 28(1)

6. Conclusion

The right to online data protection and privacy of the child is paramount in the child's overall development including their independence, intellectual capacity and general exploration. It also guarantees other rights of the children such as their right to freedom of expression, association and education. Where the child is assured of the protection of their data, they would be free to express themselves and associate with their peers without fear of surveillance. Also, they would perform better in schools, and would also be able to avoid cyber criminals who are out to trace or harm children through gathering their data online. Specific legislation addressing children's data needs to be enacted in Nigeria to enhance accountability and enforceability of the right.

6.1 Recommendations

The proper approach towards safeguarding the privacy rights of children is a multi-stake holder approach from the government, parents, online platforms, civil societies, and the children themselves. This paper proposes the following recommendations for an improved data protection regime for children.

6.1.1. The Role of the Government

6.1.1.1 Amendment of the Child Rights Act and the NDPA or the enactment of specific online data protection law for children:

Our legal regime needs to be updated to come in tune with realities and exposure of children online. Extant laws must also be enforced and regulatory agencies adequately funded to guarantee due implementation of existing laws. The United States Children's Code should serve as a useful example to Nigeria and other African countries. It focuses on how to incorporate data privacy measures into online services including games, applications and social media services in the child's best interest. Although, there are several approaches the legislature in Nigeria can take. The first approach can be to amend the provisions of the Child Right's Act to incorporate online data protection of children as is the case of South Africa, or enact specific legislation or guidelines on online child data protection.

6.1.1.2 Digital literacy and sensitisation campaigns for children, parents and educational Institutions:

A clue can be taken from digital literacy and online safety campaigns from Facebook, TikTok and other service providers. The government through its agencies such as the Ministry of Education, National Orientation Agency and the National Data Protection Commission can undertake child online data

protection and safety campaigns. In addition to this, there should be collaboration on ethical processing of data between government, industry practitioners, educators and child representatives.

6.1.1.3 Avoidance of online surveillance by online platforms or other technology:

The state also has a duty to ensure that there is no unwarranted surveillance of children's data by government agencies or private organizations through the enforcement of online safety measures such as encryption and anonymisation. Due to the proliferation of digital technologies in the form of learning analytics, child monitoring apps and online media platforms, dataveillance of children has become rampant. [93] The law needs to regulate this unwanted surveillance to make surveillance possible only where there is an overriding educational, public interest or security concern.

6.1.2 The Role of the Online Platforms

Companies should ensure they have data security measures and safeguards in place to prevent unintentional or unlawful disclosures and other processing of children's personal data. They should also integrate a security by design approach in their designs. The emphasis on privacy by default and design is pertinent because it encourages a proactive approach to data protection by ensuring that protection is in-built, rather than as an after-though.[94] Thus children would be exposed to systems that have privacy by default and do not necessarily need to take further actions to activate protection of their data.
The use of encrypted data while in transit or otherwise, the implementation of secure access controls, routine security audits and vulnerability assessments, and the establishment of incident-response plans for alleged breaches are a few examples of appropriate precautions. All systems should receive regular upgrades and fixes to protect against known security flaws.

The platforms used by Internet service providers and electronic service providers must be safe and should not endanger minors. Implementing security and privacy by design should be the default for service providers. By

[93] Lupton, D., & Williamson, B. 'The Datafied child: The Dataveillance of children and implications for their rights' (2017) New Media & Society, 19(5), 780-794. https://doi.org/10.1177/1461444816686328 accessed 4 January 2024
[94] Ellis Stewart, Enterprise Management 360 'What is Privacy by Design and Default? Definition, Principles, Examples' (13 September 2023) < https://em360tech.com/tech-article/what-is-privacy-by-design-and-default > accessed 26 January 2024

controlling material and successfully handling abuse, platform misuse, and unapproved communication with minors, they will need to go above and beyond in order to provide and guarantee age-appropriate content. Data collection should also be curtailed and should not be used for other purposes different from which they have been gathered.

6.1.3 The Role of the Parents/Guardians

Parents have the responsibility of providing a conducive environment for safeguarding the privacy of children. The use of parental control or safety tools is paramount. These tools assist parents and guardians to better supervise their children's device usage, shield them from harmful internet content, and keep their personal information private. Parents should also not participate in violating the rights of their children by indiscriminately exposing private information of children online such as their names, pictures, schools and others.

6.1.4 The Role of the Civil society

The Civil society acts as a watchdog for the society and can hold the government and online platforms accountable to provide an enabling environment for the protection of children's data. They can mount pressure on the legislature to amend the existing legislations or provide specific laws for online protection of the Nigerian child. The civil society can also actively participate in sensitisation and awareness campaigns. There are several privacy rights NGO's in Nigeria such as Paradigm Initiative, Internet society and Privacy International among other children rights NGOs. For instance, the Internet society, France in a class action in 2021 sued Facebook for violating privacy of users despite the enactment of the new EU privacy legislations[95]. This action resulted in a payment of over $100 million. This is an example of how the civil society can keep government and online media platforms dealing with users' data accountable.

6.1.5 The Role of the Children

Children should be taught online safety techniques in order to keep themselves and their data safe online. They should be encouraged to speak up and actively participate online as they are entitled to freedom of expression. Children should also be able to seek redress where their rights have been infringed in this regard. They should be taught to report any infringement, or request that

[95] France 24 News 'French NGO threatens Facebook with privacy lawsuit' (9 November 2018) https://www.france24.com/en/20181109-french-ngo-threatens-facebook-with-privacy-lawsuit; accessed 4 January 2024

 https://doi.org/10.53982/apblj.2019.0301.05-j

personal information collected or released concerning them without their consent be withdrawn. This would encourage them to engage freely in the online environment without fear or inhibition and ultimately improve their educational performance and quality of life.