THE MENACE OF ONLINE POSTS, VIS-A-VIS THE VIOLATION OF HUMAN RIGHTS OF THE SUSCEPTIBLE

AMAAYENEABASI INI ENANG
(LL.M) (LL.B) (BL) (AIcmc) (ACiarb)
Maryland School Street, off Idoro Road,
Uyo, Akwa Ibom State
Amaayeneabasienang2@gmail.com
09026430979

ABSTRACT
Online posts can take any form. It can be through the use of social media platforms, news platforms, or the internet generally. Posts include videos, Graphic Interchange Formats (GIFs), images and write-ups. Thus, while freedom of expression and free speech are basic human rights, these have been used in such a way that has occasioned a breach of the human rights of others. Now, while online posts cannot and should not be stopped, there should be a way of curbing sensitive posts and the negative impacts which have resulted from their use. This issue is not to be confused with defamatory posts, but the negative after-effects these posts have on humans. This work will explain further and in detail, how human rights have been breached as a result of the use of the internet. It will also recommend solutions to these issues and achieve better use of the internet.

***KEYWORDS**: Human rights, online posts, negative impacts.*

INTRODUCTION

The introduction of the internet and social media has been a blessing to mankind because among other things, it aids the access to and dissemination of information across the world thereby making the world a global village and easy to navigate without actually being present anywhere. Despite this feat, social media has had its downsides ranging from privacy issues to hacking issues, problems with the owners of the platforms, to the users themselves thereby occasioning several violations of human rights and lawsuits especially as social media also encourages the practice of freedom of information and speech which most often than not have been practiced in breach and have facilitated other breaches of human rights. Susceptibility or vulnerability, as will be seen in this work cuts across everyone who uses or has been used by social media.

This work will critically examine who are the susceptible or vulnerable, what makes them vulnerable, and human rights infringements on them occasioned by the use of social media.

The Concept of Susceptibility

To be susceptible means to be defenceless, vulnerable, helpless, and to be in danger. For the purpose of humans, it means where a person is more or most likely to be exposed to the chance of being attacked or harmed either physically or emotionally.[1] Ordinarily, women, children, the sick, old and injured are placed in this category, but for the purpose of this paper, everyone is a victim one way or the other and the vulnerability of humans will be brought to the fore.[2] This work is simplified in these questions- Is it safe or ethical to publish something about someone who *cannot* or have not given their consent? Or to use their content knowing they are vulnerable and exploiting same? These questions and more will be discussed below.

a. Sharenting and Human Rights Violations

In the course of sharenting which will be discussed hereunder, several breaches of human rights and other laws occur to include the following.

i. Right to Privacy Violations

[1]Valkenburg, P. M., Pouwels, J. L., Beyens, I., Driel, I. I. van, &Keijsers, L. (2021). Adolescents' Social Media Experiences and Their Self-Esteem: A Person-Specific Susceptibility Perspective. Technology, Mind, and Behavior, 2(2). https://doi.org/10.1037/tmb0000037 accessed 1 December 2022.

[2]Hazel Biggs, Caroline James, 'Legally Vulnerable: What is Vulnerability and Who is Vulnerable?' In Michael Freeman, Sarah Hawkes & Belinda Bennett (eds), *Law and Global Health: Current Legal Issues.* (Oxford Academic 2014) <https://doi.org/10.1093/acprof:oso/9780199688999.003.0009> accessed 21 December, 2022.

Due to the widespread accessibility of technology and internet access, the average child has a digital footprint before their first birthday, typically in the form of an ultrasound image or birth announcement photos.[3] This information is not restricted to images, with birthdays, names, geographical locations and schools all susceptible to data brokers who very often sell personal information to advertisers.[4]

Though these children may become aware of their digital footprint and online identity at an early age, they remain powerless in asserting their rights, especially with parents assuming the dual role of parent and publisher. Babies and young children cannot give informed consent to the reproduction of a photo and while adults can set their parameters when sharing their personal information in the virtual world, children are not afforded such control over their digital footprint. Nonetheless, one needs to think about privacy issues, particularly as children grow older.

In some legal systems, such as France and Germany, children possess the rights to their images.[5]Under *Article 226(1) French Penal Code 2020*, the fine for posting images of one's child is €35,000.[6]In *Von Hanover v Germany*,[7] the court held that, "a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image thus presupposes the individual's rights to control the use of that image, including the right to refuse the publication thereof." Parents are only recognised as stewards, not owners, of that right.[8]

Sharenting has been described as any instance where an adult in charge of a child's well-being transmits private details about the child via digital channels.[9] Though the term is conventionally used to refer to social media and common telecommunications channels, children's information can also be input into other data tracking tools such as fertility applications, smart toys or personal cloud servers. Sharing the wrong type of content on social media can also make children feel like they do not have ownership over their bodies or their own values. Most times, children do not have the opportunity to disagree with their parents posting bath time and other sensitive photos on social media. Some parents go as far as using their babies' nude images to solicit votes in order to win baby competitions. They also have no say in whatever political or social messages their parents press on them. For example, in the future, it is imaginable how some children will feel about seeing a picture of them wearing campaign t-shirts of a presidential candidate who subsequently turned out to become unpopular after the elections, or being used as political statements on their parents' social media pages.

Sharenting breaches the right to privacy of children as contained in *Article 10* of the *African Charter on Rights and Welfare of the Child, Section 8* of the *Child Rights Act,*[10] as well as *Article 16* of the *Convention on Rights of the Child*. *Article 10* provides thus:

> No child shall be subject to ...unlawful interference with his privacy, family home or correspondence, or to attacks upon his honour or reputation, provided their parents or legal guardians shall have the right to protection of the law against such interference or attacks.

It is unclear the intention of the draftsmen in the proviso part of the section, however, it seems to mean that so long

---

[3]Vanessa Cezarita, 'Children's rights and Digital Technologies: Children's Privacy in the Age of Social Media- The Perils of "Sharenting"'. (2021) <https://www.humanium.org/en/childrens-rights-and-digital-technologies-childrens-privacy-in-the-age-of-social-media-the-perils-of-sharenting> accessed 21 December 2022.

[4]Kathleen Morf, 'Children's Online Privacy and Freedom of Expression.' (2018) <http://www.unicef.org> accessed 1 June 2022.

[5]*Section 201a (1) German Criminal Code* prohibits taking and transmitting of photographs or other images of another person in private, thus violating the intimate privacy of the person depicted.

[6]Jess Staufenberg, 'French parents could face prison for posting photos of their children on Facebook'. (2016) <https://www.google.com/amp/s/www..independent.co.uk/news/world/eurpoe/renchfrench-parents-told-their-children-might-sue-them-for-pictures-put-on-facebook-a6906671.html%3famp>

[7](no2) Grand Chamber Judgment of 7 February 2012, pg. 96.

[8] Dan Reimold, 'USA Today: Professor Explores Why Things Go viral.' (2014) <https://ischool.uw.edu/news/2014/01/usa-today-professor-explores-why-things-go-viral> accessed 1 June 2022

[9] Aisha Sultan and Jon Miller, ''Facebook Parenting Is Destroying Our Children's Privacy' (2012) <http://www.cnn.com/2012/05/25/opinion/sultan-miller-facebook-parenting/> accessed 1 November 2022.

[10]*Cap c50 LFN 2004*

as the parents of the children have protection from breach of privacy, the children also are accorded such protection. It could also mean that the parents have the right to be protected where they occasion a breach of their children's privacy. *Article 16* of the *Convention on Rights of the Child* carefully omitted that proviso part and replaced it with subsection 2 to read, '...the child has the right to the protection of the law against such interference or attacks.' This seems to be more comprehensible and better protects the child from this breach.

It has been argued that these rights to privacy provisions birth an inherent conflict between a child's right to privacy and a parent's right to freedom of expression thereby, putting children and their development at risk.[11] However, it should be noted that a man's right stops where another man's right begins. *Section 8* of the *Child Rights Act* goes further to provide for sealing of records and privacy of child offenders. *Section 157*of the same Act also prohibits the publication of the name, address, school, photograph, or anything likely to lead to the identification of a child whose matter is before the Court.

The *Nigerian Data Protection Regulations Framework 2020* defines a child as any person below thirteen (13) years. It goes further to state that a data controller or processor whose processing activity targets children shall ensure its privacy policy is made in a child-friendly form with the aim of making children and their guardians have clear understanding of the data processing activity before grant of consent.[12] While this section is commendable, it does not however make provision for situations where parents are the data controllers or processors, nor what happens in the case of infants who are incapable of giving their consent by reason of their age.

ii. Exposure to Paedophiles and Loss of the Right to Life, Right against Rape and Slavery

Photos and videos of children shared by their parents on social media sometimes turn up on disturbing websites and forums, some of them dedicated to child pornography, in some cases the children's heads are cropped off and used in such websites.[13] Moreover, perverts who have information about these children as displayed on the internet can stalk these children and violate them.

Also, it is easy to forget that social media posts can provide little indicators that can help people identify where a child lives, plays, and goes to school. Posts with information like location tags and landmarks give strangers as well as known aggressors the ability to locate a child and other family members. This is especially dangerous for families who are trying to manage custody disputes and escape domestic violence situations. Even if these photos are taken down from the internet, how about those already saved in people's phones and other devices? This makes sharenting all the more dangerous.

Where these girls are stalked, they can be raped, killed, sold into sexual slavery or kidnapped for ransom.[14] These various acts of rape; importation, publication, selling, hiring, letting, printing of harmful publications,[15] using computers for production of child pornography,[16] cyber stalking,[17] sexual slavery and kidnapping are in breach of human rights instruments such as the *Child Rights Act*[18] and the *African Charter on Rights* and *Welfare of the Child*.[19]

iii. Identity Theft and Breach of Privacy

As has been pointed out earlier, over-sharing parents who post sensitive information such as their children's full names, date, and place of birth, alongside photos could make it easier for fraudsters to steal their children's identities. Child identity theft happens when a child's sensitive personal information is obtained and used to get services or benefits or to commit fraud.[20] In the nearest future, it may be responsible for almost two-thirds of all

[11](n 3)

[12]*Section 5.5*

[13]Ilana Donna, 'The Dangers of Posting your Children's Photos Online.' (2019). <https://patch.com/new-york/rivertowns/dangers-posting-your-childrens-photos-online> accessed 1 November 2022.

[14]Adam Bulger, 'This Is Why You Should Think Twice Before Posting Photos of Your Kids Online' (2021) <https://www.yahoo.com/lifestyle/why-think-twice-posting-photos-231836508.html> accessed 2 June 2022

[15]*Section 35 Child Rights Act*.

[16]*Section 23 Cyber Crime Prohibition Prevention Act 2015*

[17]*Section 24 Cyber Crime Prohibition Prevention Act 2015*

[18]*Sections 27, 30-32*.

[19]*Article 27; Article 29; Article 16*.

[20]Federal Trade Commission: Consumer Information 'How to Protect Your Child from Identity Theft.' (2021) <https://www.consumer.ftc.gov/articles/how-protect-your-child-identity-theft> accessed 1 November 2022.

identity fraud cases affecting today's children[21]. There also exists synthetic media or deep fakes as they have also been called. This is where facial recognition and machine-learning are used to combine images creating new footage of things that never actually happened. It is a computer-generated video but it looks genuine and convincing that it can be extremely difficult for the naked eye to spot that it is false. Fake videos can be created using a machine learning technique called a generative adversarial network.[22]

This is part of the negative effects of displaying one's children online. It also constitutes a breach of privacy,[23] crime of impersonation,[24] and identity theft.[25]

iv. Cyber Bullying and Inhumane Treatment

Some of the sensitive information shared on social media may lead to a child being made fun of, insulted, and even bullied in school especially as the child grows older. Peers could even share or create memes and stickers of such nude photos or videos on their school networks thereby making the child a laughing-stock in school. Sometimes, it extends beyond school and these memes and stickers so created may go viral into the wider cyberspace.[26] These acts constitute inhumane and degrading treatment contained in the *International Convention on Civil and Political Rights*[27].

b. Vulnerability of Females and Privacy Right Violations

In some relationships, young females therein are encouraged by their significant others to send nude pictures of themselves or send photos of their sensitive body parts. The problem usually arises in event of a breakup when the male in the relationship shares these pictures on the internet or for some other reason, they go viral. This constitutes a violation of privacy.[28]

c. Health Concerns and Right to Life

Another issue has to do with posting photos of the sick in need of financial support for medical treatment. While posting to raise funds is not bad in itself, the end for some of those who post is to achieve financial gain as well. Thus, from whatever amount is raised, it is split to also benefit those who posted it. Sometimes the money does not get to the vulnerable victim thereby leading in most cases to loss of life. Previously, this was done on the streets but with the aid of social media, it is rampant on the internet. At times the vulnerable sick people posted are unaware of their photos being used, they may have a genuine page and bank details supplied online for that purpose but it so happens that fraudsters also open donation platforms for the same cause and at times raise funds higher than that of the sick person because some contributed to the fraudsters' bank accounts instead of contributing to the authentic one. In the end, this fraud could occasion the loss of life[29] as the funds raised in the genuine account may not be sufficient to treat the patient, in other cases, the health of the patient may worsen.

d. Data Privacy Issues

The use of the internet has occasioned several breaches of privacy. In this case, everyone is vulnerable as it affects men, women and children, educated or not educated. Sensitive information supplied on the internet includes full names, mothers' maiden names, home and work addresses, phone numbers, email addresses, bank verification numbers (BVNs), ID cards and national identity numbers (NIN). These pieces of information if entered into the wrong hands can cause harm to the owners of the information.

Data privacy issues also affect online financial transactions which include online bank transfers where one is asked to supply sensitive information regarding debit or credit card details and personal identification number (PIN). These online financial transactions make everyone vulnerable.

---

[21]Sean Coughlan, 'Sharenting Puts Young at Risk of Online Fraud.' (2018) <https://www.bbc.com/news/ education-44153754> accessed 1 June 2022

[22] (n 10)

[23]*Article 10 African Charter on Rights and Welfare of the Child. Section 8, Child Rights Act.*

[24]*Section 484 Criminal Code Act, LFN 2004.*

[25]*Section 22(3) Cyber Crime Prohibition Prevention Act 2015.*

[26]Stacey Steinberg, 'Sharenting Children's Privacy in the Age of Social Media.' (2017) *Uf Law Faculty Publication*<http://scholarship.law.ufl.edu/facultypub> accessed 2 November 2022.

[27]*Article 7 International Convention on Civil and Political Rights; Article 16 African Charter on Rights and Welfare of the Child. Section 34 (1)(a) Constitution of the Federal Republic of Nigeria 1999 as amended.*

[28]*Article 12 Universal Declaration of Human Rights. Section 37 CFRN 1999 as amended.*

[29]*Section 33.*

Vulnerability also extends to accepting cookies on websites and some social media platform's terms and conditions. A paragraph in the 'provide, improve and develop services' section under the privacy policy of Meta Platforms Inc (formerly Facebook) states that, 'when we have location information, we use it to tailor our services for you and others like helping you check-in, ...and telling your friends you are nearby'.[30] It should be noted that telling one's Meta friends that he or she is nearby or in the same locality constitutes a breach of one's privacy and personal information simply because one's Meta location is turned on. In a subsequent lawsuit, Meta Platforms Inc. can argue that it sought the user's permission before turning on such a location, and that will be a good argument. This situation is worse when a user's account is hacked which is a common trend, thus the locations of the original user's friends are disclosed to the hacker by Facebook (Meta) which may not be safe. Cookies on the other hand, if accepted, grant the owner of the website permission to access content on the phone of users, and monitor their browsing histories, among other things.

In the locus classicus United States case of *Specht v Netscape Communications Corp*,[31] the plaintiffs brought a class action against the defendant, claiming that the software they downloaded from the defendant's website to enable them to browse the internet, violated their right to privacy as the plaintiffs had without their knowledge embedded spyware cookies in the software enabling it to carry out electronic surveillance on their online activities. The defendant sought to rely on terms in its user's licence agreement stipulating that such disputes were to be settled by arbitration and that by downloading the software, site visitors were thereby agreeing to the installation of cookies. The defendant's instruction to visitors to review and agree to these terms before downloading the software and the hyperlink to the terms was not prominently displayed and became visible only after scrolling past the download button. The Court of Appeal held that these terms did not bind the plaintiffs as they had insufficient notice of them when downloading the software.

Under the *Central Bank of Nigeria Consumer Protection Framework of 2016*, which serves as a guide to the effective regulation of consumer protection practices of Financial Institutions, with the aim of protecting consumers of financial services and treating them well, *section 2.3* provides that, contract terms should contain adequate information that will enhance consumers' decision-making process prior to execution of the contract. Financial institutions should also inform consumers of the possibility of variations in terms and conditions of contracts due to changes in economic conditions before such contracts are executed. This section further stipulates that contractual agreements posted should be clear and precise. The information must be legible and in simple language to avoid misinterpretation. Technical terms should be explained. While this is commendable in that, it addresses contracting concerns between financial institutions and customers, there is need for a law to extend a similar provision to other electronic commercial and social media websites.

In Nigeria, there is in existence, the *Nigerian Data Protection Regulation 2019* as well as the new *Data Protection Act 2023* which among other duties aims at safeguarding the rights of natural persons to data privacy.[32]The Act provides for among other things, consent under *section 26(1)* of the Act and states that the data processor[33] has the burden of proofing that consent of the data subject was obtained first. Also, silence or inactivity of the data subject shall not constitute consent.[34]*Section 26* further provides that

> (4)Where the processing of personal data is based on the consent of the data subject, the data subject shall be informed of the right to withdraw consent, prior to the granting of consent.
> (5) The withdrawal of consent under subsection (4) shall not affect the lawfulness of data processing that occurred before the withdrawal of the consent.
> (6) A request for consent shall be in clear and simple language and accessible format.
> (7) Consent-
> (a) shall be in the affirmative, and not based on a pre-selected confirmation; and
> (b) may be provided in writing, orally, or through electronic means.

[30]'Facebook Privacy Policy'<https://m.facebook.com/about/privacy/previous> accessed 2 November 2022.
[31]*(2002)306 F, 3d 17*
[32] This is in addition to *Article 12 Universal Declaration of Human Rights*; *Section 37 CFRN 1999 as amended*.
[33]A data processor has been defined under *section 65* of the *Nigeria Data Protection Act 2023* as an individual, private entity, public authority or any other body, who processes persona data on behalf of, or at the direction of a data controller or another data processor.
[34]*Section 26(3)*

The Act also provides for processing of sensitive data, [35]On children and persons lacking the legal capacity to consent, the Act provides in *Section 31* as follows-

> (1) Where a data subject is a child or a person lacking the legal capacity to consent, a data controller[36] 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.
> (4) Subsection (1) shall not apply, where the processing is--
> (a) necessary to protect the vital interests of the child or person lacking the legal capacity to consent;
> (b) 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
> (c) necessary for proceedings before a court relating to the individual.

This section provides that parental consent or consent of a legal guardian of a child or of a person lacking the legal capacity to consent shall be obtained before processing of their data can occur. While a child under this Act is a person under the age of 18 years,[37] there is no provision stating how to determine a person lacking the legal capacity to consent. Furthermore, *subsection (4)(a)* can be interpreted to mean that parental consent can be forfeited where the vital interests of the child or the person lacking the legal capacity to consent need to be protected. Thus, arguably, it may be safe to say that the issue of sharenting has been addressed in this section. Similarly, parental consent may not be necessary where educational, medical or social care professionals owe the duty of confidentiality to the child or person lacking legal capacity.

Section 35 provides that consent can be withdrawn at any time.[38] It further provides that the data controller shall ensure that it is as easy for the data subject to withdraw consent, as to give consent.[39]

In the UK, there exists the *Data Protection Privacy and Electronic Communications Regulations 2019* aimed at providing protection of data and data privacy of its citizens. Its equivalent in the EU is the *General Data Protection Regulation 2018*.

The *Credit Reporting Act 2017* was enacted to promote access to credit information and enhance risk management in credit transactions.[40] It provides for right to privacy, confidentiality and protection of all data subjects regarding their credit information, and where such information needs to be shared, it shall be done with the consent of the data subject.[41] However, there are exceptions to this rule, for example, where a data subject is involved in the issuance of a dishonoured cheque owning to lack of funds or financial and credit related malpractices, and disclosure of credit information is required, the consent of the said data subject shall not be required.[42]

Under the *Freedom of Information Act, 2011, section 14* prohibits public institutions from accepting applications for information that contains

(a) files and personal information maintained with respect to clients, patients, residents, students, or other individuals receiving social, medical, educational, vocation, financial, supervisory or custodial care or

[35]*Section 30 Nigeria Data Protection Act, 2023*
[36]*Section 65* of *Nigeria Data Protection Act 2023*, defines a data controller has been defined as an individual, private entity, public commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data.
[37]*Section 65*
[38]*Section 35(1)*
[39]*Section 35(2)*
[40]*Part 1, Section 1*
[41]*Part 5, section 1*
[42]*Part 5, section 3(b)*

services directly or indirectly from public institutions;

(b) personnel files and personal information maintained with respect to employees, appointees or elected officials of any public institution or applicants for such positions;

(c) files and personal information maintained with respect to any applicant, registrant or licensee by any government or public institution cooperating with or engaged in professional or occupational registration, licensure or discipline;

(d) information required of any tax payer in connection with the assessment or collection of any tax unless disclosure is otherwise requested by the statute; and

(e) information revealing the identity of persons who file complaints with or provide information to administrative, investigative, law enforcement or penal agencies on the commission of any crime.

Exception to this section will occur where the owner of the information consents, it is in the public domain already[43] or where disclosing it will be in public interest.[44]

The *Nigerian Data Protection Regulations Implementation Framework 2020*, was issued by the NITDA to clarify provisions of the NDPR and relevant laws applicable to it. On handling of personal data, the Regulations provides that, where a Data Controller wishes to further process Personal Data initially collected for a defined or limited purpose, the Data Controller shall consider among other things, the nature of the Personal Data; the possible impact of the new processing on the data subject; and the existence of requisite safeguards for the Personal Data.[45] These have to be provided to the Data Subject before further processing is done.[46] The further processing may be done if among other things, the Data Subject gives consent based on the new information; and the further processing is required in compliance with a legal obligation.

The regulations define consent as any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, 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.[47]

On the principles guiding consent, the Regulations states that;

a) There must be an explicit privacy policy stating the type of Personal Data collected, how the Personal Data is processed, who processes the Personal Data, the security standard implemented etc.[48]
b) Consent must be implied; thus, silence, pre-ticked boxes or inactivity do not constitute consent; and
c) Consent must not be bundled, as such; consent request from general terms and conditions should be separated from consent request. There must be consent for different types of data uses.

Furthermore, consent is required for among other things, the processing of sensitive personal data[49] and for processing the personal data of a minor.[50]

On cookies, the use of cookies on a website or other digital platforms requires consent. The consent must be freely given, informed and specific.[51] Consent for cookies does not necessarily need the ticking of a box or similar methods; the continued surfing of a website upon a clear notice indicates consent. It goes further to provide that, in deploying cookies, website owners are required to:

i. Make cookie information clear and easy to understand;
ii. Notify users of the presence and purpose of the cookies;

[43] *Section 14(2)*
[44] *Section 14(3)*
[45] *Section 4.1.1*
[46] *Section 4.1.2*
[47] *Section 5.1*
[48] *Section 5.2*
[49] *Section 5.3.1(b)*
[50] *Section 5.3.1(d)*
[51] *Section 5.6*

iii. Identify the entity responsible for the use of the cookies; and provide information on how to withdraw consent from the use of the cookie.

While this is commendable, the Regulations should also provide for an option to reject cookies ab initio as well.

Section 10(2) of the *Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011* provides that

> (2) Subscriber information shall not be released to a licensee, Security Agency or any other person, where such release of Subscriber Information would constitute a breach of the Constitution or any other Act of the National Assembly, for the time being in force in Nigeria or where such release of subscriber information would constitute a threat to national security.
> (3) Licensees shall not release personal information of a subscriber to any third party without obtaining the prior written consent of the subscriber.

A licensee in this context means a provider of communications services that utilises a subscription medium in Nigeria.[52]

Section 9(2) of the Regulations provides that subscribers' information contained in the Central Database shall be held on a strictly confidential basis and no person or entity shall be allowed access to any subscriber information on the Central Database. It also prohibits Licensees, Independent Registration Agents and Subscriber Registration Solution Providers from retaining, duplicating, dealing in or make copies of any Subscriber Information or store in whatever form any copies of the subscriber information for any purpose.[53]

The Regulations further provide that Licensees, Independent Registration Agents, Subscriber Registration, Solution Providers and the Commission must each take all reasonable precautions in accordance with international practises to prevent any corruption, loss or unauthorised disclosure of subscriber information obtained and ensures that they take steps to restrict unauthorized use of the Subscriber Information by their employees who may be involved in the capturing or processing of such subscriber information. Personal information retained by Licensees are to be used solely for their operations.[54]

RECOMMENDATIONS

This work has outlined several statutes that have addressed concerns on violation of rights of vulnerable persons through online posts, including those that have prohibited these breaches. In addition to these statutes, the right of erasure also addresses some of these concerns because the erasure of a user's information from the internet and databases solves much of the problem.

The concept of the right to be forgotten or right of erasure first arose in the case of *Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez*.[55] This right was established in May 2014 by the European Court of Justice (ECJ).[56] The Court found that European data protection law gives individuals the right to ask search engines like Google to delist certain results for queries related to a person's name. In deciding what to delist, search engines must consider if the information in question is 'inaccurate, inadequate, irrelevant or excessive,' and whether there is a public interest in the information remaining available in search results. In 2018, the EU adopted the *General Data Protection Regulation* (GDPR). *Article 17* of the GDPR sets out a 'right to erasure' similar to the right the European Court of Justice had recognised under the older law that the GDPR replaced. Some countries outside the European Union have adopted similar laws as well. To give a few examples, in July 2015, Russia passed a law that allows citizens to delist a link from Russian search engines if it 'violates Russian laws or if the information is false or has become obsolete'[57]and Turkey and Serbia have also established their

[52]*Section 1 of the Registration of Telephone subscribers Regulations 2021 Draft*
[53]*Section 9(3)*
[54]*Section 9(4)*
[55]*(2014) C-131;12*
[56]'Right to be forgotten overview'. *Google support*. <https://support.google.com/legal/answer/10769224?hl=en>accessed 1 November 2022.
[57]*Article 19, On the Activities of Foreign Entities on the Internet Telecommunications Network in the Territory of the Russian Federation 2021.Federal Law No. 1176731-7*

versions of the right to be forgotten since.[58] In Nigeria, *section 3.1(9)* of the *Nigerian Data Protection Regulations 2019* (NDPR) provides for the deletion of the personal data of a data subject under certain circumstances.

1. Where the Personal Data is no longer necessary in relation to the purposes for which they were collected or processed. Thus, for example, where information was collected as a result of membership of an association and the Data Subject later leaves that association, the former member could request that certain data relating to his membership be expunged[59] or where for instance, information was collected for employment purposes and the data subject subsequently leaves the organisation, the former employee can request that certain information regarding his employment that is no longer necessary be deleted;[60]
2. Where the Data Subject withdraws consent on which the processing is based. For instance, most websites make use of cookies where one can click on consent or opt-out by unticking the consent box;
3. Where the Data Subject objects to the processing and there are no overriding legitimate grounds for processing. Overriding legitimate grounds may include public interest;
4. Where the personal data has been unlawfully processed (most likely without the consent of the data subject or processed beyond the consent obtained);[61] and
5. Where the personal data must be erased for compliance with a legal obligation in Nigeria.

This provision, therefore, gives a legal backing of this right to Nigerians and enforceability in the Nigerian courts. It also solves most of the above-mentioned issues. The *Nigeria Data Protection Act 2023*, under *section 34(1)(d)* also provides that a data subject has the right of erasure of personal data without undue delay. *Section 34(2)* further provides that the data controller shall erase the personal data of a data subject without undue delay where the personal data of the data subject is no longer necessary in relation to the purposes for which it was collected or processed, and where the data controller has no other lawful basis to retain the personal data. The *Google Spain* case, being a landmark case has brought enlightenment around the world in that, between July 2019 and December 2019, Google received over 925,944 content removal requests from governments and courts in 19 countries.[62]

This right of erasure may not be completely attained or achieved in situations where the data in question, be it videos or documents, had already been saved in people's devices prior to the erasure or had already been printed out in hard copies, thus the erasure is limited. Moreover, the erasure does not extend to erasing such data from the minds of people who had already seen it, and as such, people may not forget the data erased.

Lastly, the Disabling Regulation, provided for in the *Protection from Internet Falsehood and Manipulation Bill (The Social Media Bill, 2019),*[63] if passed into law can among other things, disable access by end users in Nigeria, as well as disable access to identical copies where a false declaration of fact has been transmitted via the internet.

CONCLUSION

This work has undertaken a discourse on how social media publications have violated several rights of vulnerable and susceptible humans in addition to exploiting the data content of users of websites. It has also brought to the fore the fact that everyone is vulnerable to the way social media and websites have used the freedom of expression and access to information to violate other rights. Thus, parents should be careful of the content they post online about their children; visitors and users of website pages and applications should always read all information, whether policies or cookies or other sensitive information including location information before accepting and lastly, sensitive photos of females and exploitation of the sick should be avoided. In as much as these recommendations are made, the laws aforementioned in this work equally serve to curtail much of these breaches and sanction violators of these rights. That way, everyone is adequately protected.

---

[58](n 56)

[59]Ijeamaka Nzekwe, 'Should we Forget the Right to be Forgotten.' (2020) *Templars*<https://www.templars-law.com/should-we-forget-the-right-to-be-forgotten/> accessed 3 June 2022

[60] Florence Balogun and Opeyemi Adeleke, 'The Right to be Forgotten-Realities under the Nigerian Data Protection Legislation.' (2020) *Mondaq*<https://www.mondaq.com/nigeria/privacy-protection/926926/the-right-to-be-forgotten-realities-under-the-Nigerian-data-protection-legislation> accessed 3 November 2022.

[61]*Ibid*

[62]*Ibid*

[63]*Section 18*