HUMAN RIGHTS IN THE DIGITAL ERA: SAFEGUARDING THE RIGHT TO PRIVACY AGAINST PORN TRADERS[1]

***Chinazor Queen Umeobika **Linda Amarachi Oti-Onyema,**

Abstract

The designation/characterization of the genitals as "private parts" epitomizes the profound sense of decency, modesty, and sanctity historically ascribed to them within human societies. While the inadvertent or contextual exposure of other regions of the body may be socially excused or culturally permissible, the deliberate revelation of the genitals has traditionally been regarded as an act of grave indecorum. This stringent reservation is not arbitrary but deeply embedded within the moral and ethical frameworks that govern communal life. It reflects an enduring reverence for bodily integrity and a collective commitment to preserving sexual propriety as a cornerstone of social morality and cultural identity. This article undertakes an examination of the multifaceted impact of digitalization on the privacy rights of individuals and assesses the extent to which existing legal and regulatory frameworks ensure compliance and protection. The analysis reveals a troubling normalization of sexual privacy violations in the digital sphere, where such transgressions have, in many instances, evolved into a form of economic exploitation. Increasingly, individuals illicitly obtain and disseminate intimate images or videos, weaponizing them as instruments of coercion and blackmail for financial gain. This phenomenon not only undermines personal dignity and autonomy but also exposes the inadequacies of contemporary legal mechanisms in addressing the complexities of digital sexual exploitation. A doctrinal approach of research was adopted and based on its findings, it was recommended among others that in addition to the criminalization of non-consensual porn trading, confiscating and recovering any proceeds made from it and possibly be directed to compensate victims for the emotional, social, and financial harm caused by the unlawful sharing or sale of their images. This is based on the principle that no one should profit from a crime.

Keywords: Digital, Right, Sexual Privacy, Trade

1.0 Introduction

The advent of computational technology in the nineteenth century, followed by the inception of the Internet in the latter half of the twentieth century, has fundamentally redefined the modalities of human existence. In contemporary society, digital platforms have become integral to nearly every sphere of human endeavor—ranging from education and commerce to entertainment and social interaction. The relentless advancement of information and communication technologies (ICT) has

[1] * **Chinazor Queen Umeobika, PhD,** Reader and Head, Department of Private and Property Law, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Email: cq.umeobika@unizik.edu.ng; queencumeobika@gmail.com, Tel: +2348035018582.

****Linda Amarachi Oti-Onyema, PhD,** Senior Lecturer, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. Email: la.oti-onyema@unizik.edu.ng; and

engendered a paradigmatic shift in the nature of human communication, rendering it increasingly instantaneous, efficient, and interconnected. The digital transformation has led to unprecedented

reductions in the costs of engaging in international trade, changing how and what we trade, and who can trade.

Notwithstanding these advancements, the digital era has simultaneously precipitated profound challenges to personal privacy. A complex network of state and non-state actors incessantly collects, processes, and disseminates vast quantities of personal data frequently without the knowledge or consent of the individuals concerned.

Concurrently, the commodification of personal information has given rise to novel economic paradigms predicated upon the systematic exploitation of data. In the era of the Fourth Industrial Revolution, personal data has emerged as the principal resource fueling global digital economies. Over the past several decades, the ubiquity of such data processing has occasioned new regulatory challenges that make it more difficult for governments to ensure that the opportunities from digital trade are realised and are not abused or used to the detriment of others.[2]Within this increasingly data-centric environment, individuals—whether as citizens or consumers—have become acutely conscious of the necessity for robust legal safeguards to protect their informational privacy and personal autonomy.

Consequently, the discourse surrounding privacy and data protection has assumed global significance. The ensuing analysis seeks to elucidate the aspect of data privacy and protection that affects the sexual rights of individuals within the digital economic space and the legal protections afforded within international, regional, and domestic legal frameworks applicable in Nigeria.

2.0 Concept of Digital Trading

Trade is the voluntary exchange of goods or services between economic actors, where transactions occur only if both parties find them beneficial.[3]Trade refers to the process of exchanging goods and services, which can occur through various means such as barter or monetary transactions. In its broadest sense, trade encompasses the buying and selling of commodities, as well as the general act of commerce and traffic involving goods. It is a fundamental aspect of economic activity, facilitating the movement of products between individuals and businesses.[4] In *Arbico Ltd v. FBIR*[5]. The Supreme Court laid down two important axioms: • Firstly, that the word 'trade' should be interpreted in its widest sense, in accordance with its common everyday meaning; • Secondly, that an isolated one-off transaction can still constitute a "trade".

[2] Digital trade, <https://www.oecd.org/en/topics/digital-trade.html>accessed on 7/11/2025

[3] Adam Hayes, Trade in Finance: Benefits, Function, and Insights, <https://www.investopedia.com/terms/t/trade.asp>, accessed on 7/11/2025

[4] Trade: A Comprehensive Guide to Its Legal Definition and Scope, https://legal-resources.uslegalforms.com/t/trade, accessed on 7/11/2025

[5] {1996} 2 All NLR 303

While there is no single accepted definition of digital trade, there is growing understanding that it encompasses trade in goods and services that are digitally ordered or delivered. Digital trade

involves digitally ordered but physically delivered trade in goods and services and digitally delivered trade.[6]

Not all trades are permissible. There are domestically prohibited goods which are products that are banned or severely restricted on the domestic market because they are determined to present risks for human, animal or plant life or health, or the environment this includes porn trading which is not consented to or exposes children to immorality.

The "porn trade" (short for *pornography trade*) refers to the industry and commercial activities involved in the production, distribution, and sale of pornographic material — that is, media that depicts sexual acts or nudity intended to arouse viewers. The modern porn trade spans both mainstream commercial enterprises (e.g., adult film studios) and online platforms (like subscription sites, amateur content marketplaces, or adult entertainment networks).[7]

3.0 Sexual Privacy

Sexual privacy is one of the aspects of human right to privacy. Despite numerous scholarly and legal efforts to define the concept of privacy, no universally accepted definition has yet been achieved. Although the aspiration for privacy is a universal human concern, its precise manifestation varies across societies, shaped by distinct social structures, cultural norms, and economic conditions. Consequently, the notion of privacy must be continuously reinterpreted in light of contemporary realities and examined within the evolving socio-technological context. The need for privacy protection, therefore, is not static but dynamically contingent upon changing circumstances. Context plays a decisive role: information regarded as private in one situation may be viewed as public or inconsequential in another. This was the observation of the Supreme Court of Nigeria in *Johnson v The Government of Kaduna State* & ORS[8] where it held that: "the right to dignity of human person and the right to family life or privacy as the case maybe is wide and the applicability of what actions or inactions may be inhumane and a violation of privacy or family life can emanate from a varied of circumstances."

Some scholars attempted to explain the notion of privacy but one of the most referred definitions of privacy was given by D. W. Prosser who explained that, privacy is a group of the following four torts: (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness. Being abstract, privacy encompasses numerous other issues, including the freedom of thought against surveillance; bodily integrity; protection of personal data; seclusion

[6] <https://www.oecd.org/en/topics/digital-trade.html>, accessed on 7/11/2025

[7] Sexual Exploitation of Children over the Internet: The Face of Child Predator and Other Issues
, <https://www.congress.gov/event/109th-congress/house-event/LC12720/text>, accessed on 7/11/2025

[8] – Per Muslim Sule Hassan, J.C.A. (2025-06) LEGALPEDIA 80086 (CA)

in residence; capacity of protecting reputation; safeguard against searches and questionings, etc. In sum, privacy means one's right to keep his/ her personal affairs and relationships away from the

reach of others.[9] A state of being alone, and thus, not to be interrupted or watched by others. In *Sunday Jackson v The State*[10] the Supreme Court of Nigeria defined privacy to mean abstinence from intruding into the private lives of others.

Arguably, in the digital age, this typical definition of privacy cannot ensure the desired protection unless associated with control over information. Hence, many other authors used to define privacy in terms of information control.

All privacy-related discourses acknowledge- privacy is an intrinsic human right that facilitates individuals to exile outsiders from their intimate zones; uplifts the dignity of human beings, along with their other constitutional guarantees. Australian Privacy Charter, for instance, states that 'privacy is such a value that underpins human dignity and other key values, such as the freedom of association, freedom of speech.[11] However, Traditional privacy law's efficacy, however, is eroding just as digital technologies magnify the scale and scope of the harm.[12]

sexual privacy is a distinct privacy interest that warrants recognition and protection. It serves as a cornerstone for sexual autonomy and consent. It is foundational to intimacy. Its recognition would acknowledge the subordinating impact of invasions of sexual privacy.[13]

Sexual privacy involves "the behaviors, expectations, and choices that manage access to and information about the human body, sex, sexuality, gender, and intimate activities." It also encompasses social norms surrounding intimacy and sexuality.[14] In the panoply of privacy values, sexual privacy is paramount because of its importance to intimacy, sexual agency, self-development, and equality. sexual privacy allows an individual to develop and safeguard a core part of his/her personhood.[15]

Sexual privacy violations occur when an individual's body, sexuality, sexual orientation, gender, or sexual history are seen, recorded, photographed, exhibited, revealed, published, disclosed, or circulated offline or online. Online acts that violate an individual's sexual privacy come in many forms: deepfake sex videos, digital voyeurism, and nonconsensual pornography, to name only a

---

[9] Md. Toriqul Islam, "A Brief Introduction to the Right to Privacy – An International Legal Perspective <https://www.nyulawglobal.org/globalex/right_to_privacy_international_perspective.html>, accessed on 7/11/2025

[10] Per Haruna Simon Tsammani, **J.S.C.** (2025-03) LEGALPEDIA 85898 (SC)

[11] Australian Privacy Charter Council – The Australian Privacy Charter, AustLII, [1995] PrivLaw PRpr 31, 1995 2(3) Privacy Law & Policy Reporter 44.

[12] Danielle Keats Citron, Sexual Privacy, 128 Yale Law Journal 1870 (2019), https://digitalcommons.law.umaryland.edu/fac_pubs/1600/

[13] *Ibid*.

[14] Liane M. Jarvis Cooper, "Sexual Privacy and Persecution, 2023", https://www.uclalawreview.org/sexual-privacy-and-persecution/#_ftn8

[15] *Ibid*

few. While some acts are nonconsensual from the outset, other acts may start off as consensual and then mutate into nonconsensual ones. For example, the practice of "revenge porn" involves the nonconsensual, online circulation of (supposedly or seemingly) consensually-taken photographs of an intimate partner.[16]

Online sexual privacy violations harm society. As a result, individuals have retreated from online spaces, reduced their online presence, masked their online identities, and even left the internet entirely thereby destroying or denying them business opportunities in the digital environment amongst other dangers. Due to the great negative impact of sexual privacy violation on the victim, a case is being made in countries like the United States for such violation to be a sufficient ground to seek asylum.

4.0 **The Rampage and Damage of Nudes Trading**

It is no longer news that social media is rampaged with thousands of photographs and a seemingly endless stream of naked or partially undressed people engaging in sexual intercourse. The prevalence of porn videos and photographs is attributable to the big market discovered on the digital space, where the busyness of your social media handle or wall determines your earnings. To meet the required target on posts, views, or shares, internet users have resorted to nude or porn trade where realistically viewers are irresistibly attracted in their numbers.

It was reported that hundreds of anonymous profiles were dedicated to sharing, trading and selling explicit images - and it all appeared to be without the permission of the persons pictured. It seemed like a new evolution of so-called revenge porn, where private sexual material is published online without consent, often by embittered ex-partners. Not only were these intimate images being shared for an audience of thousands, but men - lurking behind the mask of anonymity - were teaming up to expose the real-life identities of these women, a practice known as doxing.

It was once reported that Reddit brands as "the front page of the internet" has built an audience of about 50 million daily users - roughly four million in the UK - by letting people set up and run forums, known as "subreddits", dedicated to all kinds of interests. Reddit has a history of hosting controversial sexual content. In 2014, a huge cache of private images of celebrities was shared on the site, and four years later Reddit shut down a group which was using "deepfake" technology - a kind of artificial intelligence - to superimpose celebrities into porn videos. Responding to these controversies, the US-based company introduced stricter rules and strengthened its ban on posting or threatening to post intimate or sexually explicit media of people without their consent but the ban wasn't working. Dozens of subreddits were still dedicated to sharing intimate images of women from all over the UK. All were being dehumanised as sexual objects in the comments. The men on the subreddit were also sharing and selling naked photos of the women.

On the 16th day of September, 2024, former BBC news presenter Huw Edwards was sentenced for possessing indecent images of children after pleading guilty to three charges of making indecent images of children. A WhatsApp chat between Edwards and another male which was sexual in nature, was detected and it showed that Edwards was giving him gifts and money. Within the chat there were numerous sexually explicit images, including 41 indecent images of children.

[16] Ibid

In the wake of a damning investigative report exposing an underground child pornography syndicate operating across X (formerly Twitter) and Telegram, civil society organisations and global child protection experts are calling for urgent and coordinated action to tackle the crisis of online child sexual exploitation in Nigeria. They also urged the Federal Government to bring the syndicate selling the pornographic content of Nigerian children in plain sight to justice. The two-part report, titled, "Exposed! How teenage boys are lured into selling nudes for cash (1) and (2)", published by PUNCH, revealed the activities of a shadowy figure known as @Hidden_Domain, who has been exploiting young Nigerian boys for profit, sharing explicit content via anonymous social media accounts and protected digital groups. The investigation, which spanned eight months, used technology to uncover not only the syndicate's methods but also identified no fewer than 26 victims and traced some of the financial transactions involved, linked to a tier-one Nigerian bank. "The existence of individuals like @Hidden_Domain underscores the need for stronger enforcement of laws against child exploitation and effective cyber monitoring." [17]

Research has shown that a lot of survivors of porn trading experienced social anxiety and social isolation," The five main consequences the participants shared include fears of going out in public, engaging in relationships, applying to jobs, and seeking help, as well as an increase in depression and anxiety. Victim-blaming is also common and psychologically harmful."[18]This can also cause severe financial consequences; many survivors reported losing their job, or difficulty applying for new jobs, after employers were able to search their names online and view the compromising images.[19]

5.0 Legal Framework for Safeguarding Sexual Privacy Rights Against Porn Trade

The law is not oblivious to the existence of pornography, nor to its production, sale, and distribution within the digital ecosystem. To preserve public decency and moral order, various legal frameworks have been established to regulate and restrict the indiscriminate exposure of pornographic materials. Some of these legal principles manifest as rights conferred upon citizens, ensuring protection from exploitative or harmful content. In contrast, others take the form of prohibitions and criminal sanctions aimed at curbing unlawful conduct. Accordingly, this discussion shall examine both the national and international legal regimes governing the control, dissemination, and regulation of pornographic content in the contemporary digital landscape for monetary benefits.

5.1 International laws

By virtue of the foundational human rights instruments, the United Nations Human, every person is guaranteed the right to his private life and no one shall be subjected to arbitrary interference with

[17] Godfrey George, "Nude trade: CSOs urge FG to prosecute syndicate after PUNCH report", <https://punchng.com/nude-trade-csos-urge-fg-to-prosecute-syndicate-after-punch-report/#google_vignette>, 7/11/2025

[18] Understanding victim blaming and why it's harmful to survivors, <https://welshwomensaid.org.uk/news/understanding-victim-blaming-and-why-its-harmful-to-survivors/ > accessed on 7/11/2025

[19] Jillian McKoy, 'The Social Consequences of Nonconsensual Pornography", <https://www.bu.edu/sph/news/articles/2020/the-social-consequences-of-nonconsensual-pornography/> Accessed on 7/11/2025

his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[20] This same protection is reaffirmed in *Article 17* of the International Covenant on Civil and Political Rights[21], which underscores the universality of the right to privacy by prohibiting arbitrary or unlawful interference with an individual's private and family life, home, or correspondence, and by guaranteeing legal protection against any form of intrusion or attack upon personal honour and reputation. To elaborate on the import of this right, the General Comment No. 16 to Article 17 to the ICCPR emphasized that:

> *The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to, ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.*

The ICCPR went further to obligate states **t**o ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; **t**o ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; and to ensure that the competent authorities shall enforce such remedies when granted. The Convention offers not just the right to privacy but a remedy to be provided in event of breach.

The significance of the right to privacy is further underscored by its explicit extension to children. The Convention on the Rights of the Child[22], drawing from the principles enshrined in the International Covenant on Civil and Political Rights (ICCPR), affirms in Article 16 that: "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks.

At the regional level, the African Charter on Human and Peoples' Rights does not have a direct clause on the right to privacy. Notwithstanding the omission, the African Charter on the Rights and

[20] Article 12

[21] (ICCPR)

[22] (CRC) of 1989

Welfare of the Child[23] provides the child with privacy rights. *Article 10* states: "No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his 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."

Much more than a right, states are encouraged to enact legislations that prohibit commercialization of pornographic materials. For the first time at the international level, issues related to the circulation of goods of a sexual nature were consecrated at the Paris International Conference, as a result of which fifteen states concluded the Agreement for the Suppression of the Circulation of Obscene Publications. The agreement did not contain an official definition of pornography, but focused on a list of items that could be pornographic, namely: writings, drawings, images or other pornographic items. In 1923, the International Convention for the Suppression of the Circulation of and Traffic in Obscene Publications was signed in Geneva. In this Act, pornography is identified through a list of products. In addition, the Convention defines a list of acts for which States Parties undertake to establish responsibility in national legislation: "the production or storage of obscene items for the purpose of selling or distributing or publicly displaying them, transporting obscene personally or through another person for the above purposes, or releasing them in one way or another, conducting or participating in the porn business, advertising or disclosing by whatever means, in order to promote circulation or trade in persecuted items and materials". The Convention is in force and is considered the main international act in the field of combating the trafficking of pornography. [24]

Article 34 of the CRC imposes a duty on states to take all appropriate national, bilateral and multilateral measures to prevent inter alia, exploitative use of children in pornographic performances and materials. Similarly, in *Article 27* of the African Charter on the Rights and Welfare of the Child, States Parties to the Charter shall undertook to protect the child from all forms of sexual exploitation and sexual abuse and shall in particular take measures to prevent; (a) the inducement, coercion or encouragement of a child to engage in any sexual activity; (b) the use of children in prostitution or other sexual practices; (b) the use of children in pornographic activities, performances and materials.

5.2 National Laws

For this discourse, we shall focus on the legal regime on porn trades in Nigeria while making comparisons with other jurisdictions where necessary.

5.2.1 The Constitution of the Federal Republic of Nigeria[25]

The Constitution guarantees the right of every citizen to his private and family life. *Section 37* states that privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected". However, it must be noted that this right is not absolute; some circumstances can legally curtail the exercise of this right as seen in Section 45

[23] 1990

[24] International legal regulation of pornography trafficking and peculiarities of its implementation in Russia Svetlana Viktorovna Sheveleva

[25] 1999(as amended)

of the Constitution **to** the effect that **"**(1) Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health; or for the purpose of protecting the rights and freedoms or other persons.

Furthermore, *section 34* of the Constitution accords to every person respect for the dignity of his person. Accordingly, no person shall be subject to torture or to inhuman or degrading treatment; no person shall he held in slavery or servitude; and no person shall be required to perform forced of compulsory labour.

In a broad and general sense, respect for dignity implies respect for the autonomy of each person, and the right of everyone not to be devalued as a human being or treated in a degrading or humiliating manner.[26]The court has held that any act which amounts to humiliation of a person and an assault to the dignity of his person as a human being is a violation of his right as guaranteed under *Section 34* of the Constitution.[27]

Where there is a violation of the right, section 46 of the Constitution gives the victim the right to approach the high court in the state of violation to seek redress where this right is breached. Where, however, the violation occurred in the workplace, the National Industrial Court shall have jurisdiction to handle same.[28]

5.2.2 The Cyber Crime Act[29]

The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This Act also ensures the protection of critical national information infrastructure, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The Act criminalises the production, distribution, transmission, possession and procurement of child pornography for oneself or for another person in a computer system or on a computer-data storage medium.[30] In other cases, not involving a child, any person who knowingly makes or sends other pornographic images to another computer by way of unsolicited distribution is guilty of an offence.[31] *Section 24* prohibits cyberstalking. It states that "any person who knowingly or

[26] Arthur Chaskalson, 'Human Dignity As A Constitutional Value', <https://brill.com/display/book/edcoll/9789004478190/B9789004478190_s010.xml >, accessed on 7/11/2025

[27] *Igweokolo v Akpoyibo* (2017) Legalpedia (CA) 11415

[28]

[29] 2025

[30] Subsection 1

[31] Subsection 2

intentionally sends a message or other matter by means of computer systems or network that - (a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any

such message or matter to be so sent; or (b) he knows to be false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent: commits an offence.

To realise adequate enforcement of the law, service providers who are usually the custodians and controllers of data supplied by their customers or consumers are under a legal duty to assist and facilitate any process engaged in the investigation or prosecution of cybercrimes. The relevant provisions are found mainly in *Sections 21–26* of the Act. These duties include data retention-service providers (e.g., Internet Service Providers, telecom operators, financial institutions, etc.) must keep all traffic data and subscriber information for a minimum period of two years, assistance and cooperation with the law enforcement agencies in the investigation process of cybercrimes. They must also preserve and release this information when required by law enforcement, subject to proper legal authorization. Refusal or failure to comply may attract criminal liability and fines. Providers are required to preserve the integrity and confidentiality of data they store or transmit. They must take reasonable security measures to protect systems against unauthorized access, alteration, or disclosure. They must promptly report any cyberattacks, intrusions, or other security breaches affecting their systems to the National Computer Emergency Response Team or other designated authority.[32] Service providers are prohibited from disclosing subscriber information except: with the consent of the subscriber, Pursuant to a court order, or for the purpose of national security or crime investigation. [33]Providers must maintain an updated database of subscribers and ensure that communications can be traced to individual users when necessary for law enforcement investigations.[34]

A considerable array of law enforcement and regulatory institutions are statutorily vested with powers under the Act to investigate, apprehend, and prosecute offenders. The enforcement architecture is deliberately multi-agency in scope and includes, inter alia, the Office of the National Security Adviser (ONSA), which serves as the central coordinating authority; the Nigeria Police Force (NPF) through its specialized Cybercrime Unit; the Economic and Financial Crimes Commission (EFCC); and the Department of State Services (DSS).

In addition, sector-specific regulators such as the Nigerian Communications Commission (NCC) and the Central Bank of Nigeria (CBN) are empowered to implement and enforce compliance measures within their respective spheres of oversight, particularly in matters relating to telecommunications infrastructure and financial transactions. The Federal High Court of Nigeria, being the court of exclusive jurisdiction over federal offences, is likewise entrusted with the adjudication of all matters arising under the Act, including the issuance of warrants, preservation orders, and other ancillary judicial authorizations.

[32] Section 24

[33] Section 25

[34] Section 26

Collectively, these bodies form the statutory enforcement framework designed to ensure the effective suppression, deterrence, and prosecution of cybercrimes in Nigeria.

5.2.3 Nigeria Data Protection Act[35]

The objective of the Act, amongst others, is to safeguard the fundamental right of data subjects to the privacy of their information or data as guaranteed under the 1999 Constitution of Nigeria. In furtherance to this, *section 24* of the Act imposes a duty on a Data Controller to ensure that personal data is - (a) processed in a fair, lawful and transparent manner; (b) collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes;(f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach. A data controller and data processor shall use appropriate technical and organisational measures to ensure confidentiality, integrity, and availability of personal data.

One of the significant innovations introduced by the Act is the requirement of a Privacy Impact Assessment (PIA) as a precondition to the processing of personal data to determine the likelihood of any high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purposes. This mechanism is designed to avert potential violations of privacy by ensuring that risks are identified, evaluated, and mitigated before data processing activities are undertaken.[36]

The Act characterises sensitive personal data as encompassing information pertaining to an individual's religious or other beliefs, sexual orientation, health status, race, ethnic origin, political opinions, trade union membership, criminal history, or any other category of personal information deemed intrinsically sensitive. By this classification, the Act accords such data an elevated tier of protection, recognising the heightened risk of harm or discrimination that may arise from its misuse.

In furtherance of this protective regime, the Act prescribes stringent conditions under which sensitive personal data may lawfully be processed. It provides that, without prejudice to the general data protection principles enshrined therein, a data controller—or any data processor acting on its behalf—shall not process sensitive personal data unless one or more of the following legally recognised bases exists:

(a) The data subject has expressly consented to the processing for the specific, clearly defined purpose(s) for which such data is to be utilised, and such consent has not been withdrawn; or

(b) The processing is necessary for the performance of obligations incumbent upon the data controller, or for the exercise of rights vested in the data subject, under employment legislation, social security frameworks, or any analogous statutory regimes.

These conditions underscore the Act's commitment to ensuring that the processing of sensitive data is conducted only under strict, narrowly tailored circumstances, thereby safeguarding individual autonomy, dignity, and privacy.

[35] 2023

[36] Section 28

Section 26 of the Nigerian Data Protection Act (NDPA) imposes a stringent obligation on Data Controllers and Data Processors to ensure the security and protection of all personal data under

their custody or control. This provision underscores the Act's overarching commitment to safeguarding personal data against unauthorized access, alteration, loss, or any form of unlawful processing.

Further strengthening the regulatory framework, *Section 46(3)* empowers the National Data Protection Commission (NDPC) to commence an investigation *suo motu*—that is, on its own initiative—where it has reasonable grounds to believe that a Data Controller or Data Processor has contravened any provision of the Act. This investigative authority is designed to ensure proactive oversight and to prevent violations even in the absence of a formal complaint by a data subject.[37]

6.0 Other Jurisdictions

6.1 Hawai'i Privacy Laws

Hawai'i has some of the strongest privacy protections among U.S. states. Its laws cover physical privacy, communications privacy, digital privacy, intimate-image privacy, and governmental data use. However, for this discourse, we shall restrict ourselves to the 2024 Revised Penal Code Under the 2024 Hawaii Penal Code, it is an offence except in the execution of a public duty or as authorized by law to installs or use in any private place, without consent of the person or persons entitled to privacy, any device for observing, recording, amplifying, or broadcasting another person in a stage of undress or sexual activity in that place; to disclose or threatens to disclose an image or video of another identifiable person either in the nude, or engaging in sexual conduct; or to creates or discloses or threatens to disclose an image or video of a composite fictitious person depicted in the nude, or engaged in sexual conduct, that includes the recognizable physical characteristics of a known person so that the image or video appears to depict the known person and not a composite fictitious person, with intent to substantially harm the depicted person with respect to that person's health, safety, business, calling, career, education, financial condition, reputation, or personal relationships, or as an act of revenge or retribution.

6.2 United Kingdom Online Safety Act[38]

Like Hawai'i, we shall consider only the UK Online Safety Act. The Act provides for a new regulatory framework for the use of internet services. The Act imposes duties on internet service providers to identify, mitigate and manage the risks of harm from illegal content and activity, and content and activity that is harmful to children. thus, the service providers are obligated to secure their services in such a way that users' rights to freedom of expression and privacy are protected.[39]The service providers owe a duty of care to their users to put in place proactive safety measures such as illegal content assessment, child risk assessment and swiftly take down any illegal

[37] Nigerian Data Protection Act 2023 Review, <https://assets.kpmg.com/content/dam/kpmg/ng/pdf/nigeria-data-protection-act2023_kpmg-review.pdf >, accessed on 7/11/2025

[38] 2023

[39] Sections 1 and 33

content upon becoming aware of it;[40] and publish transparent reports on how they protect users.[41] This legal duty goes beyond voluntary codes of practice and establishes binding obligations on tech companies.

The Act expands the law around the non-consensual sharing of intimate images, including deepfakes and manipulated media. This provides stronger legal recourse for victims and reflects a growing recognition that such content can cause severe and lasting significant harm.

A primary priority content area is ensuring that minors cannot access harmful or age-inappropriate material, particularly pornographic content. To achieve this, platforms must implement rigorous age assurance and verification systems capable of reliably preventing under-18s from exposure to such content. In *Free Speech Coalition, Inc. v. Paxton*[42], a landmark decision, the United States Supreme Court allowed states to require Internet pornography websites to verify the age of viewers in order to prevent access by minors

Together, these provisions represent a fundamental shift in responsibility: instead of leaving safety entirely to individual users or parents, the Act places accountability squarely on the platforms that host and distribute harmful content, ensuring they cannot ignore or downplay their role in online risks.

6.0 Enforcement of Sexual Privacy Rights Against Porn Trading in Nigeria

Non-consensual pornography is a relatively new phenomenon, and one that is increasing in today's digital age, and efforts are being made by online service providers to combat incessant infiltration of porn in the digital ecosystem. For example, Meta states that it removes sexual imagery to prevent the nonconsensual distribution of sexual images[43].

Again, laws as seen above have been enacted to regulate commercial transactions in pornography. However, much needs to be desired in terms of enforcement. Notably, countries like the United States are pushing hard on violators of sexual privacy laws. Recently, a Texas jury has awarded a woman $1.2bn (£944m) after ruling that she was the victim of revenge porn**.** The woman, who was named only by the initials DL in court documents, filed a harassment lawsuit against her former boyfriend in 2022. The suit alleged that he posted intimate pictures of her online to "publicly shame" her after a break-up.[44]

In Nigeria, we observe the recklessness with which internet users demand for porn and distribute same without any fear of being sanctioned by law. Unfortunately, some of the porns have been ones generated from Artificial Intelligence through photo shops, etc. to falsely indict their victims and

[40] Section 10

[41] Section 7

[42] 606, US(2025)

[43] Brenda Dvoskin, *Speaking Back to Sexual Privacy Invasions*, 99 Wash. L. Rev. 59 (2024). Available at: https://digitalcommons.law.uw.edu/wlr/vol99/iss1/5

[44] <https://www.bbc.com/news/world-us-canada-66514052>, accessed on 7/11/2025

publicly shame them. These acts have in many cases been reduced to jokes or what they popularly caal comedy without any thought as to the consequences on the life and livelihood of their victims.

While reports have been scarce regarding, this matter, there is no single precedent of prosecution and conviction of any sexual privacy offender in Nigeria.

A man in Anambra State, South-east Nigeria, was once reported to have been arrested for allegedly leaking and selling a nude video clip of an unidentified woman in the state on social media. The suspect, Chinedu Ezeudu, said to be in his 20s, also allegedly used the nude video clip to blackmail the woman. The woman, according to the statement, said, in March, she had lost her memory card, where her nude video clip was saved. She said the suspect, who apparently picked the card, would later chat her up in June via an undisclosed social media platform, where he requested a huge amount of money in order not to leak the nude clip.[45] Regrettably, nothing has been heard about the matter again.

Admittedly, Nigeria does not yet have a specific law dedicated solely to sexual privacy rights. Nevertheless, the existing legal framework is sufficiently robust to support immediate implementation and enforcement efforts. Despite the relative comprehensiveness of these laws, enforcement is hindered by several practical challenges. These include limited technical capacity and inadequate digital forensics expertise within some law enforcement agencies; overlapping and sometimes conflicting mandates among the EFCC, the Nigeria Police Force, the DSS, and other bodies, which often result in jurisdictional disputes; and the persistent underreporting of cyber-related incidents. Collectively, these challenges weaken the effectiveness of the current legal regime and impede timely prosecution.

7.0 Conclusion and Recommendations

The existence of porn trading in Nigeria, as in many other countries, is not in doubt. Although no law outrightly prohibits the trade in pornography, Nigerian law criminalises participation in such activities where consent is absent, where public morals are likely to be corrupted, where minors are exposed, or where the rights of other citizens are infringed. Unfortunately, these legal provisions are more often breached than complied with, and effective deterrence remains weak due to the systemic challenges faced within the Nigerian justice system. Nevertheless, enforcement is achievable if appropriate human and material resources are deployed.

First, drawing inspiration from the UK Online Safety Act, Nigeria should adopt proactive and preventive measures to curb porn trading by holding digital service providers responsible for reporting offenders and facilitating their apprehension and prosecution. However, the economic interests of these providers often make them reluctant to cooperate, a challenge that must be anticipated and addressed.

Second, since many of the digital platforms used to perpetrate these violations are operated by faceless, unidentifiable individuals and entities, stricter regulatory requirements should be incorporated into existing laws. Such regulations should mandate verification processes—such as submission of National Identification Numbers (NIN), Bank Verification Numbers (BVN), or

[45] https://www.premiumtimesng.com/news/more-news/626377-nigerian-man-sells-womans-nude-for-n3000-to-social-media-users-official.html?tztc=1> , accessed on 7/11/2025

similar credentials—before service providers or users are permitted to operate within the digital market. This would greatly enhance traceability and enforcement.

Third, the proceeds of porn trading should be confiscated and channeled toward compensating victims. Adequate rehabilitation services—psychological, emotional, and social—should also be provided to those whose well-being has been harmed. In addition, platforms used in committing such offences should be shut down, and offenders should be denied digital operating licenses for a specified duration.

Lastly, following the example of the Hawai ‘i Penal Code, the installation of digital monitoring devices in private spaces where sexual activities are expected to occur—such as hotel rooms-should be prohibited. Where such installations are necessary, explicit prior notice must be given to customers or guests.