

**NON-CONSENSUAL INTIMATE IMAGE DISSEMINATION
UNDER CRIMINAL LAW: A DOCTRINAL AND
COMPARATIVE ANALYSIS OF CONSENT, PRIVACY AND
EXTRATERRITORIAL JURISDICTIONS.**

By

Osawaru A. Erimwinorosee, Esq*

Abstract

This article examines Non-Consensual Intimate Dissemination (NCID) under criminal law through a rigorous doctrinal and comparative analysis of consent, privacy, and extraterritorial jurisdiction. The study is situated within the context of a widely reported incident involving a foreign national who recorded consensual sexual encounters with African nationals and subsequently disseminated the intimate recordings on social media without their consent, thereby raising complex questions concerning the limits of sexual autonomy, digital privacy, reputational harm, and cross-border criminal accountability in the digital age. Employing a doctrinal research methodology, chosen because the study principally involves the analysis, interpretation, and evaluation of existing rules and judicial authorities, the article analyses relevant statutory provisions, constitutional guarantees, and judicial authorities within Nigeria, while drawing comparative insights from selected common law and international jurisdictions that have developed specific legislative responses to image-based sexual abuse. The findings reveal significant doctrinal ambiguities between consent to dissemination, alongside fragmented privacy protections, evidentiary challenges, and inadequate statutory recognition of image-based abuse as a distinct and aggravated criminal harm. The study further identifies structural challenges relating to territoriality and enforcement, particularly where offenders, victims, and digital platforms operate across multiple jurisdictions, thereby complicating investigation, prosecution, and victim

*.LLB(Hons)(Uniben),LLM(Uniben),PhD(RSU),ACIarb(UK),Dr.FCHIRM,ACTI,MIAR,AIS DS,MILAN,AICMC,MICI Arb,FNILA,BL.Lecturer,Nigerian Law School, Port Harcourt Campus, Port Harcourt, Rivers State; Notary Public of Nigeria of the Supreme Court of Nigeria.

redress. It argues that traditional criminal law principles concerning mens rea, harm, and jurisdiction require principled recalibration to effectively address technologically facilitated sexual exploitation. The article recommends the enactment of clear and comprehensive offences criminalizing non-consensual dissemination, the articulation of a rights-based and autonomy-centered understanding of consent and reasonable expectation of privacy, and the strengthening of extraterritorial jurisdiction and mutual legal assistance frameworks. It concludes that a coherent, victim-centered criminal justice response is imperative to safeguard dignity, equality, autonomy, and digital integrity.

Key words: *Non-Consensual Intimate Dissemination (NCID), Image-Based Sexual Abuse, Consent and Mens Rea, Digital Privacy Rights, Extra territorial Criminal Jurisdiction.*

1.0. Introduction

The proliferation of digital technologies and social media platforms has fundamentally transformed the regulation of intimacy, privacy, and personal autonomy within contemporary criminal law. In an era where mobile devices enable instantaneous recording and global dissemination, private sexual encounters may be converted into permanent digital artefacts capable of inflicting enduring reputational, psychological, and socio-economic harm. Non-consensual Intimate Dissemination (NCID), increasingly conceptualized as image-based sexual abuse, represents one of the most pressing manifestations of technology-facilitated exploitation. It exposes the inadequacy of traditional criminal law doctrines that were developed in a pre-digital context and that often fail to capture the distinct and aggravated harm occasioned by the unauthorized circulation of intimate material.

The urgency of doctrinal clarity is underscored by the widely reported incident involving an alleged Russian national who engaged in sexual relations with Ghanaian and Kenyan women, recorded the encounters, and subsequently uploaded the intimate videos to social media platforms without their consent. Although the underlying sexual activity was reportedly consensual, the subsequent dissemination was not. This distinction is central to contemporary criminal law debates: does consent to sexual intercourse imply consent to recording? Does consent to recording imply consent to dissemination? And to what extent should criminal liability attach where the dissemination occurs across digital platforms accessible in multiple jurisdictions? The incident not only highlights the vulnerability of victims to digital exploitation but also exposes the jurisdictional complexities that arise when offenders, victims, and hosting platforms are located in different states.

Within Nigeria and many other jurisdictions, existing legal responses remain fragmented. Provisions addressing cyber stalking, obscenity, defamation, or invasion of privacy offer partial remedies but lack conceptual coherence and specificity. The absence of an express statutory offence tailored to NCID creates uncertainty regarding the elements of the crime, the requisite mens rea, evidentiary standards concerning consent, and the scope of victim protection. Moreover, traditional territorial principles of criminal jurisdiction are strained where dissemination occurs through global networks, raising questions about extraterritorial competence, mutual legal assistance, and the enforcement of judgments against foreign nationals.

Comparatively, several jurisdictions have enacted targeted legislation criminalizing image-based sexual abuse, recognizing that the harm lies not merely in reputational injury but in the violation of sexual autonomy, dignity, and informational privacy. These developments reflect an evolving understanding of consent as context-specific and revocable, particularly in digital environments where control over personal data is central to autonomy. Yet significant doctrinal divergences remain regarding the threshold of intent,

the requirement of proof of harm, and the permissible reach of extraterritorial jurisdiction.

This article therefore undertakes a doctrinal and comparative analysis of NCID under criminal law, focusing on three interrelated pillars: the conceptual boundaries of consent; the scope and protection of privacy as a criminal law interest; and the reach of extraterritorial jurisdiction in transnational digital offences. By interrogating statutory provisions, judicial authorities, and comparative legislative models, the study seeks to determine whether existing frameworks adequately address the normative and practical challenges posed by NCID. It argues that a coherent and victim-centered criminal law response-grounded in a principled understanding of consent, reinforced privacy protections, and robust jurisdictional mechanisms-is essential to safeguarding dignity, autonomy, and digital integrity in an increasingly interconnected world.

2.0. Conceptual and Theoretical Framework

The phenomenon of non-consensual intimate image dissemination (NCIID) has emerged as a significant challenge within contemporary criminal law jurisprudence. It refers to the distribution or publication of sexually explicit or intimate images of a person without that person's consent, often through digital platforms or electronic communication technologies. The concept is sometimes colloquially described as "revenge pornography" although scholars increasingly reject that term because it narrowly frames the offence as motivated by revenge, whereas many cases arise from coercion, harassment, financial exploitation, or malicious humiliation¹. The conceptual foundation of the offence is therefore rooted in the protection of personal autonomy, privacy, dignity, and sexual integrity within the digital environment.

From a doctrinal perspective, NCIID intersects with several established legal concepts, including consent, privacy, dignity, and informational autonomy. Consent, within criminal law, operates as a normative threshold determining the legitimacy of conduct affecting another person's bodily or personal integrity. The absence of consent is therefore central to criminal liability in offences involving sexual autonomy. The courts have long emphasized the importance of genuine consent in determining the legality of acts affecting personal dignity. In *R v Brown*,² the House of Lords affirmed that consent does not always operate as a complete defence where conduct causes harm or undermines public policy. This reasoning has influenced contemporary debates concerning digital sexual exploitation, particularly where the dissemination of intimate images causes serious psychological harm even where the images were originally produced consensually.

1 Danielle Keats Citron and Mary Anne Franks, 'Criminalizing Revenge Porn'(2014) 49 *Wake Forest Law Review* 345.

2 [1994] 1 AC 212 (HL).

It is instructive to state that the conceptualization of privacy in the context of NCIID draws from both constitutional and common law principles. Privacy has been defined as the right of an individual to control the disclosure and use of personal information relating to his or her private life.³ In many jurisdictions, courts have recognized that the publication of intimate images without consent constitutes a grave invasion of privacy. For example, in *Campbell v MGN Ltd*,⁴ the House of Lords recognized that the unauthorized publication of private information can amount to a violation of an individual's reasonable expectation of privacy. Similarly, the European Court of Human Rights in *Von Hannover v Germany*,⁵ affirmed that the right to respect for private life under Article 8 of the European Convention on Human Rights extends to protection against intrusive media publication. These authorities illustrate the broader normative framework within which NCIID is increasingly criminalized.

Another important conceptual element is the principle of informational self-determination, which refers to an individual's ability to control the dissemination of personal data or information concerning their private life.⁶ In the digital era, intimate images constitute highly sensitive personal data, and their dissemination without consent undermines the individual's control over personal identity and reputation. The harm caused by such dissemination often includes reputational damage, psychological trauma, harassment, and social exclusion. Consequently, modern criminal law frameworks increasingly recognize NCIID as a form of technology-facilitated gender-based violence. The theoretical framework underpinning the criminalization of NCIID may be analyzed through several legal theories. One prominent perspective is the harm principle, articulated by John Stuart Mill, which posits that the state is justified in restricting individual liberty only where such conduct causes harm to others.⁷ The dissemination of intimate images without consent causes significant emotional, psychological, and reputational harm to victims and therefore falls squarely within the domain of conduct that criminal law is justified in prohibiting.

A related theoretical justification is the dignitarian theory of criminal law, which emphasizes the protection of human dignity as a fundamental value underlying criminal prohibition. The unauthorized distribution of intimate images objectifies victims and reduces them to instruments of humiliation or sexual exploitation. *a fortiori*, this is inconsistent with the constitutional and human rights principle that individuals must be treated as ends in themselves rather than as mere means.⁸ In many jurisdictions, such as England and Wales

3 Alan Westin, *Privacy and Freedom* (Atheneum Press 1967) 7.

4 [2004]UKHL 22;[2004] 2 AC 457.

5 (2004) 40 EHRR 1.

6 Paul M Schwartz, 'Internet Privacy and the State' (2000) 32 *Connecticut Law Review* 815.

7 John Stuart Mill, *On Liberty* (Oxford University Press 1859) 14.

8 Jeremy Waldon, *The Harm in Hate Speech* (Harvard University Press 2012) 105.

under the Criminal Justice and Courts Act 2015 and Canada under section 162.1 of the Criminal Code, this principle has informed legislative responses that criminalize the dissemination of intimate images as an offence against personal dignity, privacy and sexual autonomy.

The feminist legal theory perspectives also provide a critical analytical lens for understanding NCIID. Feminist scholars argue that such conduct disproportionately affects women and is often used as a mechanism of coercion, intimidation, or control within intimate relationships.⁹ The non-consensual dissemination of intimate images therefore reflects a broader structural inequalities in digital spaces and reinforces gender-based violence. Consequently, feminist legal scholars advocate for robust criminalization, victim protection mechanisms, and platform accountability.

Another theoretical consideration is the transnational nature of digital communication, which raises complex issues of jurisdiction and enforcement. The internet enables images to be disseminated instantaneously across national borders, making it difficult for domestic criminal laws to effectively regulate such conduct. This has led to increasing reliance on principles of extraterritorial jurisdiction, particularly where harmful digital conduct originates outside the territorial boundaries of the victim's state but produces harmful effects within that state. As a necessary corollary, Courts have recognized that states may assert jurisdiction over extraterritorial conduct where there exists a substantial connection or harmful effect within the territory.¹⁰ This doctrinal approach is increasingly relevant in addressing NCIID offences committed through global online platforms.

Within the Nigerian context, the conceptual framework for addressing NCIID is gradually evolving through statutory provisions addressing cybercrime, privacy violations, and electronic harassment.

The **Cybercrimes (Prohibition, Prevention, etc.) Act 2015** contains provisions that criminalize certain forms of online harassment and the distribution of obscene or offensive content through computer systems.¹¹

Although the statute does not expressly define NCIID as a separate offence, its provisions provide a partial legal basis for prosecuting individuals who disseminate intimate images without consent through digital platforms.

In sum, the conceptual and theoretical framework of non-consensual intimate image dissemination rests on the interrelated principles of consent, privacy, dignity, informational autonomy, and protection from harm. Theoretical justifications for criminalization draw from the harm principle, dignitarian theory, feminist legal scholarship, and the evolving doctrine of extraterritorial

9 Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 *Oxford Journal of Legal Studies* 534.

10 175 F Supp 2d 367 (D Conn 2001).

11 Cybercrimes (Prohibition, Prevention. etc.) Act 2015, SS 24 and 26.

jurisdiction in cybercrime regulation. These conceptual foundations provide the analytical basis for examining how different jurisdictions structure criminal liability for NCIID and how domestic legal systems may develop more effective mechanisms to protect victims in the digital age.

3.0. Non-Consensual Intimate Image Dissemination (NCIID),

Non-Consensual Intimate Image Dissemination (NCIID), commonly described as “revenge pornography” or image-based sexual abuse, has emerged as a significant contemporary challenge within domestic criminal law systems. The phenomenon involves the distribution, publication, or threat to distribute sexually explicit or intimate images of an individual without their consent, often with intention to humiliate, harass, intimidate, or exploit the victim. Although historically unaddressed by traditional criminal statutes, many domestic jurisdictions have progressively recognized NCIID as a distinct form of sexual exploitation and privacy violation requiring criminal sanction.

Under domestic criminal law frameworks, the criminalization of NCIID generally rests upon the protection of fundamental legal interests such as privacy, dignity, sexual autonomy, and psychological integrity. These interests are increasingly recognized as components of broader constitutional or human rights protections. For instance, the right to privacy, which is protected under section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended), provides a normative basis for criminal liability where intimate images are shared without authorization.¹² Courts have consistently interpreted the right to privacy to extend to personal communications and private life. In *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo*¹³, the Supreme Court affirmed that personal autonomy and privacy constitute integral aspects of constitutional protection.

In Nigeria, although there is no single statute expressly titled as prohibiting “revenge pornography”, the conduct is addressed through a combination of statutory provisions under cybercrime and criminal legislation. The principal statute is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, which criminalizes various forms of online harassment, cyberstalking, and unlawful publication of offensive or harmful content. Section 24 of the Act criminalizes the transmission of messages or materials through computer systems that are grossly offensive, indecent, obscene, or intended to cause annoyance, inconvenience, danger, insult, or emotional distress.¹⁴ Where intimate images are disseminated online to humiliate or intimidate a victim, such conduct may fall squarely within the ambit of cyberstalking or offensive communication under this provision.

12 Constitution of the Federal Republic of Nigeria 1999 (as amended) S 37.

13 (2001) 7 NWLR (Pt 711) 206 (SC).

14 Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 24

Furthermore, domestic criminal liability may also arise under traditional criminal law provisions governing obscenity and defamation. The Criminal Code Act applicable in Southern Nigeria criminalizes the publication of obscene materials capable of corrupting public morals.¹⁵ Although historically directed at pornography or indecent publications, such provisions have occasionally been invoked to prosecute individuals who circulate sexually explicit materials without authorization. However, scholars have criticized the reliance on general obscenity provisions because they tend to frame the harm primarily in moralistic rather than victim-centered terms.¹⁶

As an additional corollary, civil and quasi-criminal remedies may arise under the law of defamation and invasion of privacy where the dissemination of intimate images damages the reputation or dignity of the victim. In *Okedara v Attorney-General of the Federation*,¹⁷ the court emphasized the need to protect individuals from unlawful intrusions into their private lives in the context of modern technological communication. Although the case did not directly concern NCIID, it illustrates the willingness of Nigerian courts to recognize privacy violations in the digital sphere.

Beyond Nigeria, many domestic jurisdictions have enacted specific legislation targeting NCIID. For example, the Criminal Justice and Courts Act 2015 in the United Kingdom introduced the offence of disclosing private sexual photographs and films without consent and with intent to cause distress.¹⁸ Similarly, in the United States, several states have enacted statutes criminalizing the non-consensual dissemination of intimate images. Courts have generally upheld such laws as legitimate restrictions designed to protect privacy and prevent harassment. In *People v Austin*,¹⁹ the Illinois Supreme Court upheld the constitutionality of the state's revenge pornography law, emphasizing that the law protects victims from severe emotional and reputational harm caused by unauthorized dissemination of intimate images.

Domestic criminal law responses to NCIID therefore reveal a gradual transition from reliance on traditional offences such as obscenity, harassment, and defamation toward the creation of specific image-based abuse offences. This shift reflects a growing recognition that the harms caused by NCIID are distinct, involving violations of sexual autonomy, dignity, and digital privacy. More importantly, the widespread use of smartphones, social media platforms, and encrypted messaging applications has significantly increased the scale and speed at which intimate images can be disseminated, thereby intensifying the need for robust criminal law interventions.

15 Criminal Code Act, Cap C38 Laws of the Federation of Nigeria 2004, ss 233-235.

16 Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 *Oxford Journal of Legal Studies* 34.

17 (2011) 12 NWLR (Pt 1261) 165.

18 Criminal Justice and Courts Act 2015 (UK), S. 33.

19 155 NE 3d 439 (Illinois Supreme Court, 2019).

Nevertheless, the enforcement of NCIID laws under domestic criminal systems continues to face several challenges. These include evidentiary difficulties in proving lack of consent, jurisdictional complications arising from cross-border dissemination, and the anonymity often associated with digital communication platforms. Moreover, where legislation relies on general cybercrime or obscenity provisions, prosecutors may encounter interpretative uncertainties regarding whether such statutes adequately capture the specific harms of image-based abuse.

Consequently, legal scholars and policy advocates increasingly argue that domestic criminal law frameworks should adopt explicit NCIID offences that clearly define the prohibited conduct, recognize the centrality of consent, and incorporate extraterritorial enforcement mechanisms where dissemination occurs through transnational digital networks. Such reforms would enhance legal certainty and provide stronger protection for victims whose privacy and dignity are violated through the non-consensual distribution of intimate images.

4.0. Comparative Jurisprudence: South Africa and the United States of America

4.1. South Africa

South Africa has taken significant legislative steps to address the growing problem of image-based abuse through the enactment of the Cybercrimes Act 19 of 2020, which introduced explicit criminal provisions targeting the unlawful disclosure of intimate images. Section 16 of the Act criminalizes the disclosure of a data message containing an intimate image of another person without their consent where the individual depicted retains a reasonable expectation of privacy.²⁰

The Act further criminalizes threats to distribute such images, thereby recognizing the coercive and exploitative nature of image-based sexual abuse. The South African approach is deeply rooted in constitutional principles. The Constitution of the Republic of South Africa, 1996, guarantees the right to privacy under section 14 and the right to dignity under section 10, both of which have been interpreted by courts as extending to the protection of personal autonomy and private information. In the landmark decision of *National Media Ltd v Jooste*,²¹ the court recognized that the publication of private information without consent may constitute an actionable invasion of privacy. Although the case did not specifically concern intimate images, its reasoning laid an important doctrinal foundation for later developments concerning digital privacy and image-based abuse.

²⁰ Cybercrimes Act 19 of 2020, S. 16

²¹ 1996 (3) SA 262 (A).

Similarly, in *S v I*,²² the Western Cape High Court addressed the criminal implications of distributing explicit images without the victim's consent. The court emphasized that such conduct undermines both dignity and privacy, particularly in circumstances where the images were originally shared within the context of an intimate relationship. The judgment underscored the principle that consent to create or share an image privately does not automatically extend to consent for wider dissemination.

South Africa's statutory framework also incorporates extraterritorial dimensions where offences are committed through digital platforms. The Cybercrimes Act allows prosecution where the harmful data message either originates within South Africa or produces substantial harmful effects within the jurisdiction.²³ This approach recognizes the inherently transnational nature of online image dissemination and reflects broader international trends toward expanding jurisdictional reach in cybercrime regulation.

Overall, the South African model demonstrates a rights-based approach to NCIID, grounded in constitutional protections for dignity and privacy while simultaneously recognizing the need for specific criminal offences addressing digital sexual abuse.

4.2. United States of America

In contrast to South Africa's unified federal legislative approach, the United States has developed a more fragmented yet extensive legal framework through state-level legislation. While there is currently no comprehensive federal statute specifically criminalizing revenge pornography, the majority of U.S. states have enacted laws addressing the non-consensual distribution of intimate images.

One of the most influential judicial decisions in this area is the case of *People v Austin*,²⁴ in which the Illinois Supreme Court upheld the constitutionality of the state's revenge pornography statute. The defendant challenged the law on the grounds that it violated the First Amendment protection of freedom of speech. However, the court rejected this argument and held that the statute served a compelling governmental interest in protecting individual privacy and preventing severe emotional and reputational harm. The court emphasized that individuals possess a legitimate expectation that intimate images shared privately will not be publicly disseminated without consent.

Similarly, the Vermont Supreme Court in *State v VanBuren*,²⁵ upheld the constitutionality of Vermont's non-consensual pornography statute. The court reasoned that the law was narrowly tailored to address a specific form of harm

22 (2016) ZAWCHC 126.

23 Cybercrimes Act 19 of 2020 (South Africa), S. 3.

24 155 NE 3d 439 (Ill 2019).

25 214 A 3d 791 (Vt 2019).

arising from the abuse of private sexual images and therefore did not infringe upon constitutionally protected expression.

In the absence of a federal statute specifically targeting NCIID, U.S. federal authorities sometimes rely on broader criminal laws addressing cyberstalking, harassment, and extortion. For instance, the Violence Against Women Act,²⁶ provides mechanisms for addressing online harassment and stalking that may overlap with revenge pornography cases. Additionally, federal prosecutors have occasionally invoked provisions of the **Computer Fraud and Abuse Act**,²⁷ Where intimate images were obtained through unauthorized access to digital accounts.

From a constitutional perspective, the American legal system must carefully balance the criminalization of NCIID against the robust protection of free speech guaranteed by the First Amendment. Courts have generally upheld revenge pornography statutes where they are narrowly framed to target non-consensual dissemination of private sexual images rather than general speech. Judicial reasoning often emphasizes that such laws regulate conduct that violates privacy rather than suppressing legitimate expression.

Comparative Observations

A comparative assessment of South Africa and the United States reveals both convergences and divergences in their legal responses to NCIID. Both jurisdictions recognize the serious harms caused by the non-consensual dissemination of intimate images and have developed criminal law mechanisms to address such conduct. However, the normative foundations and institutional structures differ significantly.

South Africa's approach is heavily influenced by constitutional rights to dignity and privacy, resulting in a relatively cohesive statutory framework within the Cybercrimes Act. The emphasis on human dignity reflects the broader transformative constitutionalism that characterizes South African jurisprudence.

The United States, by contrast, adopts a decentralized model in which individual states enact legislation tailored to local policy considerations. Judicial scrutiny under the First Amendment ensures that such laws must be carefully drafted to avoid unconstitutional restrictions on speech. Despite this constitutional constraint, courts have increasingly recognized that revenge pornography laws serve a legitimate and compelling governmental interest.

From a doctrinal perspective, both jurisdictions reinforce the principle that consent to the creation or private sharing of intimate images does not constitute consent to public dissemination. This distinction has become a central element of modern NCIID jurisprudence and reflects a broader shift

26 Violence Against Women Act 1994 (as amended).

27 18 U.S.C. SS 1030 (1986) (as amended).

toward recognizing digital sexual autonomy and informational privacy as protected legal interests.

Cumulatively, the comparative experiences of South Africa and the United States illustrate the gradual emergence of a global legal consensus that non-consensual intimate image dissemination constitutes a serious violation of privacy, dignity, and personal autonomy. Their respective legal frameworks provide invaluable insights for jurisdictions seeking to strengthen domestic criminal law responses to image-based sexual abuse, particularly in the context of rapidly evolving digital technologies and cross-border online communication.

5.0. Consent and Privacy in Criminal Law Doctrine.

5.1. The Concept of Consent in Criminal Law

Consent operates as a central justificatory principle in criminal law, determining the boundary between lawful and unlawful conduct. However, in the context of non-consensual intimate image dissemination (NCIID), consent is highly contextual and purpose-specific.²⁸ Thus, consent to the creation or possession of an intimate image does not extend to its distribution.²⁹

This doctrinal distinction has been affirmed in several jurisdictions. Under the UK's Criminal Justice and Courts Act 2015, liability arises where:

- ❖ private sexual photographs are disclosed;
- ❖ without the consent of the individual depicted; and
- ❖ with knowledge or recklessness as to that lack of consent.³⁰

The emphasis on knowledge or recklessness reflects a shift from subjective intent to a broader culpability standard.³¹

Similarly, in the United States, legislative efforts such as the Intimate Privacy Protection Act adopt a “reckless disregard” standard, thereby expanding criminal liability beyond intentional harm.³²

Judicial reasoning also supports this distinction. In *R v Brown*³³ although not directly on image-based abuse, the court underscored that consent is not absolute and may be limited where public policy or harm is implicated. This reasoning has been extended to digital sexual offences where harm is significant and enduring.

28 A. Ashworth and J. Horder, *Principles of Criminal Law* (7th edn, OUP 2013) 25.

29 D. Ormerod and K. Laird, *Smith, Hogan and Ormerod's Criminal Law* (15th edn, OUP 2018) 329.

30 Criminal Justice and Courts Act 2015 (UK), S. 33.

31 *Ibid.*, s 33(2).

32 Intimate Privacy Protection Act (2016)

33 [1994] 1 AC 212.

6.0. Privacy as a Protected Legal Interest

Historically, privacy was not recognized as an independent interest within criminal law. The decision in *Kaye v Robertson*,³⁴ illustrates this limitation, where the court lamented the absence of a general right to privacy under English Law.

However, modern jurisprudence has significantly evolved. Privacy is now understood as encompassing:

- ❖ informational control;
- ❖ sexual autonomy; and
- ❖ protection against humiliation and exposure.³⁵

In the United States, constitutional jurisprudence, particularly *Stanley v Georgia*,³⁶ affirms that individuals possess a sphere of private autonomy free from state intrusion, including control over intimate materials.

Furthermore, in *Katz v United States*,³⁷ the Supreme Court articulated the doctrine of reasonable expectation of privacy, which has become foundational in assessing privacy violations in digital contexts.

Thus, privacy has transformed from a civil remedy-based concept to a criminally enforceable legal interest, particularly in cases involving sexual exploitation and digital abuse.³⁸

At its normative core, privacy protects an individual's autonomy, dignity, and control over personal information, including the ability to determine when, how, and to what extent intimate aspects of one's life are disclosed to others. The non-consensual dissemination of intimate images constitutes a profound invasion of this protected sphere because it deprives the individual of informational self-determination and transforms inherently private material into a source of public exposure, humiliation, and exploitation.

Consequently, contemporary human rights jurisprudence increasingly recognizes privacy not merely as a negative right against unwarranted intrusion, but as a positive legal interest that imposes obligations upon the State to provide effective legal and remedial mechanisms against digital violations of personal intimacy and autonomy.

7.0. The Intersection of Consent and Privacy

Consent and privacy are intrinsically connected in the regulation of non-consensual intimate image dissemination. Privacy safeguards an individual's autonomy, dignity, and control over personal information, while consent determines the circumstances in which such information may be accessed,

34 [1991] FSR 62.

35 R Wacks, *Privacy and Media Freedom* (2nd edn, OUP 2013) 56.

36 394 US 557 (1969).

37 389 US 557 (1969).

38 N Moreham and M Tufal (eds), *Privacy and Media Law* (3rd edn, OUP 2017) 112.

used, or disclosed. In the context of intimate images, consent to the creation or private sharing of an image does not imply consent to its subsequent dissemination.

Accordingly, the authorized disclosure of intimate images constitutes both a violation of the individual's reasonable expectation of privacy and infringement of personal autonomy and sexual integrity.

The intersection of these concepts underscores the principle that individuals retain continuing control over the disclosure and circulation of intimate material concerning them.

Consequently, contemporary jurisprudence increasingly recognizes that consent in the digital environment must be specific, informed, and contextual, and that the absence of such consent transforms the dissemination of intimate images into a serious violation of privacy and human dignity, warranting legal and, where appropriate, criminal sanction.

7.1. Reasonable Expectation of Privacy

Courts evaluate whether the victim had a legitimate expectation that the image would remain private.³⁹ Even where images are voluntarily shared, further dissemination outside the agreed context constitutes a violation.

In *AMP v Persons Unknown*,⁴⁰ the court granted injunctive relief to restrain dissemination of intimate images, holding that prior consensual sharing did not negate the claimant's expectation of privacy.

Similarly, Canadian jurisprudence in *R v Jarvis*,⁴¹ recognized that privacy is not extinguished merely because an individual is visible or has shared information in limited context.

7.2. Autonomy and Sexual Dignity

Modern criminal law increasingly frames NCIID as an infringement of sexual autonomy and dignity.⁴²

In *KS v AM*,⁴³ the court held that the non-consensual dissemination of intimate images constitutes a profound violation of dignity and privacy, warranting judicial protection.

This approach aligns with constitutional jurisprudence in *Teddy Bear Clinic for Abused Children v Minister of Justice*,⁴⁴ where privacy was linked to dignity, bodily integrity, and personal development.

In the UK, the decision in *Campbell v MGN Ltd*,⁴⁵ further reinforced that misuse of private information engages both privacy and dignity interests.

39 *Ibid.*

40 [2011] EWHC 3454 (TCC).

41 2019 SCC 10.

42 C MacKinnon, 'Pornography as Defamation and Discrimination' (1991) 71 *Boston University Law Review* 793.

43 [2017] ZAGPJHC 297.

44 [2013] ZACC 35.

7.3. Harm-Based Justification

The criminalization of NCIID is grounded in the harm principle, which justifies state intervention where conduct causes substantial injury.⁴⁶

Courts and legislatures recognize that non-consensual dissemination results in:

- ❖ severe psychological trauma;
- ❖ reputational harm; and
- ❖ permanent digital exposure.⁴⁷

South African statutory law, particularly the Criminal Law (Sexual Offences and Related Matters) Amendment Act, criminalizes the non-consensual sharing of intimate images, emphasizing both actual and potential harm.⁴⁸

Similarly, several U.S. state laws criminalize “revenge pornography” based on harm to emotional well-being and privacy.⁴⁹

8.0. Extraterritorial Jurisdiction

8.1. Concept and Basis of Extraterritorial Jurisdiction in Criminal Law

Extraterritorial jurisdiction refers to the authority of a State to prescribe, adjudicate, and enforce criminal law beyond its territorial boundaries.

In the context of non-consensual intimate image dissemination (NCIID), this doctrine has become increasingly significant due to the borderless nature of digital communication technologies⁵⁰

Classical principles of jurisdiction include:

- ❖ Territorial principle (offence committed within the State);
- ❖ Passive personality principle (victim’s nationality);
- ❖ Protective principle (threats to State interests); and
- ❖ Universality principle (for grave international crimes).⁵¹

In NCIID cases, jurisdiction is often asserted based on territorial effects, where harm occurs within the forum State, even if the act of dissemination originated elsewhere.⁵²

The decision in *R v Smith (Wallace Duncan)*⁵³ illustrates this approach, where jurisdiction was upheld because the harmful effects of the defendant’s conduct were felt within England.

45 [2004] 2 AC 547.

46 (1859) ch.1

47 C McGlynn, E Rackley and R Houghton, ‘Beyond “Revenge Porn”’ (2017) 25 *Feminist Legal Studies* 25.

48 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007 (South Africa).

49 D Citron and M Franks, ‘Criminalising Revenge Porn’ (2014) 49 *Wake Forest Law Review* 345.

50 M Shaw, *International Law* (8th edn, CUP 2017) 469.

51 S Brenner, *Cybercrime and the Law* (Northeastern University Press 2012) 89.

52 *Ibid*, 90.

8.2 Extraterritorial Regulation of NCIID

(a) United Kingdom

The UK adopts a limited extraterritorial approach. Under the criminal Justice and Courts Act 2015, jurisdiction may be established where there is a substantial link to the UK, such as the victim's presence or the occurrence of harm within the jurisdiction.⁵⁴

Furthermore, the courts have demonstrated flexibility in asserting jurisdiction over cross-border digital offences. In *R v Sheppard and Whittle*,⁵⁵ the court upheld jurisdiction over online publications hosted abroad but accessible within the UK, emphasizing the location of harm.

(b) United States

The United States adopt a broad extraterritorial framework, particularly in cyber-related offences. Statutes such as the Computer Fraud and Abuse Act and the Violence Against Women Act provide mechanisms for addressing cross-border harms, including image-based abuse.⁵⁶

Judicial authority for extraterritorial application is well established. In *United States v Al Kassar*,⁵⁷ the court affirmed that jurisdiction may be exercised where there is a sufficient nexus between the conduct and the US interests.

Additionally, in *United States v Ivanov*,⁵⁸ jurisdiction was upheld over a foreign hacker whose actions caused harm within the United States, reinforcing the effects doctrine in cybercrime.

(c) South Africa

South Africa has adopted a hybrid jurisdictional model, combining territorial and extraterritorial elements. The cybercrimes Act 2020 allows for jurisdiction where:

- ❖ the offence is committed within South Africa
- ❖ the accused is a South African citizen; or
- ❖ the harmful effects are experienced within the Republic.⁵⁹

This approach reflects constitutional commitments to dignity and privacy, as seen in *KS v AM*,⁶⁰ where the court recognized the serious harm caused by non-consensual dissemination of intimate images.

53 A Aust, *Handbook of International Law* (2nd edn, CUP 2010) 45.

54 [2004] EWCA Crim 631.

55 Criminal Justice and Courts Act 2015 (UK), S 33-35.

56 [2010] EWCA Crim 65.

57 Computer Fraud and Abuse Act 18 USC § 1030; Violence Against Women Act 34 USC SS 12291.

58 660 F3d 108 (2d Cir 2011).

59 175 F Supp 2d 367 (D Conn 2001).

60 Cybercrimes Act 19 of 2020 (South Africa), S 25.

(d) Nigeria

Nigeria's legal framework on cybercrime, particularly the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, provides for extraterritorial jurisdiction where:

- ❖ the offence is committed by a Nigerian citizen outside Nigeria; or
- ❖ the offence has substantial effects within Nigeria.⁶¹

Although Nigerian courts have yet to develop extensive jurisprudence specifically on NCIID, the statutory framework allows for prosecution of cross-border digital offences.⁶²

The Supreme Court in *Federal Republic of Nigeria v Ibori*,⁶³ recognized the increasing relevance of transnational criminal conduct and the need for cooperative enforcement mechanisms.

8.3. Enforcement Challenges in NCIID Cases

(a) Jurisdictional Conflicts

Jurisdictional conflicts constitute a significant enforcement challenge in cases of non-consensual intimate image dissemination (NCIID). Given the borderless nature of digital communication, the perpetrator, victim, digital platform, and data servers may be located in different jurisdictions, thereby creating uncertainty as to which state possesses the authority to investigate and prosecute the offence. Traditional territorial principles of criminal jurisdiction are often inadequate to address such transnational offending.

The challenge is further compounded by disparities in domestic legal frameworks, as some jurisdictions, such as England and Wales under the Online Safety Act 2023 and Singapore under the Penal Code have enacted specific legislation criminalizing non-consensual intimate dissemination and providing, in appropriate circumstances, for extraterritorial jurisdiction, while others continue to rely on general criminal offences that inadequately address the unique nature of image-based sexual abuse.

Conflicts arise where multiple States assert jurisdiction over same conduct.⁶⁴ This may lead to:

- ❖ duplication of proceedings;
- ❖ forum shopping; and
- ❖ inconsistent legal outcomes.

61 [2017] ZAGPJHC 297.

62 Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Nigeria), S 41.

63 *Ibid.*

64 (2014) 15 NWLR (Pt 1425) 1.

The absence of harmonized legal standards on NCIID exacerbates these challenges.⁶⁵

(b) Evidentiary Difficulties

Evidentiary difficulties represent a significant challenge in the investigation and prosecution of non-consensual intimate image dissemination (NCIID). The digital nature of the offence means that crucial evidence is often stored on electronic devices, cloud servers, or social media platforms, where it may be deleted, altered, encrypted, or located outside the prosecuting jurisdiction. Moreover, proving the identity of the perpetrator and establishing the absence of consent can be particularly difficult, especially where anonymous accounts or digital concealment techniques are employed.

These challenges are further compounded by delays in obtaining electronic evidence from service providers and by differing rules governing the admissibility and authentication of digital evidence.

Consequently, the effective prosecution of NCIID requires robust digital forensic capabilities, prompt preservation of electronic evidence, and enhanced cooperation between law enforcement agencies and technology companies.

Digital evidence is often:

- ❖ located in multiple jurisdictions;
- ❖ controlled by private technology companies; and
- ❖ subject to differing legal standards for admissibility.⁶⁶

The case of *Microsoft v United States*,⁶⁷ highlights the complexities of cross-border data access, particularly where data is stored on servers located outside the requesting State.

(c) Anonymity and Identification of Offenders

The anonymity afforded by digital technologies presents a significant challenge in NCIID cases. Perpetrators often use pseudonymous accounts and encrypted platforms to conceal their identities and evade detection.

Consequently, effective investigation depends largely on digital forensic techniques and cooperation between law enforcement agencies and online service providers.

Perpetrators frequently exploit anonymity tools, making identification difficult.⁶⁸ Even where identified, extradition may be hindered by :

- lack of bilateral treaties; or
- differences in criminalization standards.⁶⁹

65 Shaw (n 1) 478.

66 Brenner (n 2) 102.

67 *Ibid*, 110.

68 584 US -----(2018).

69 Brenner (n 2) 115.

(d) Enforcement Against Digital Platforms

Enforcement against digital platforms remains a significant challenge in NCIID cases, as online platforms often facilitate the dissemination of intimate images. Delays in content removal and difficulties in obtaining user information frequently impede effective enforcement.

Accordingly, digital platforms are increasingly expected to remove unlawful content promptly and cooperate with law enforcement authorities. Many NCIID offences involve dissemination through global platforms such as Meta Platforms or X Corp.

Regulating such entities presents challenges due to:

- jurisdictional limitations;
- varying national laws; and
- platform immunity doctrines.⁷⁰

In *Google LLC v Equustek Solutions Inc.*,⁷¹ the court ordered a global de-indexing injunction, illustrating attempts to impose transnational obligations on digital intermediaries.⁷²

(e) Inadequate International Cooperation

Inadequate international cooperation poses a significant challenge in NCIID cases. The transnational nature of digital offending requires cross-border access to electronic evidence and coordinated investigations.

However, differences in domestic laws and delays in mutual legal assistance frequently impede effective prosecution.

Effective enforcement depends on mutual legal assistance and extradition frameworks.⁷³ However, delays and bureaucratic obstacles often undermine timely intervention in NCIID cases, where harm is immediate and ongoing.⁷⁴

8.4. Emerging Responses and Doctrinal Developments

Recent years have witnessed significant doctrinal and legislative developments in response to non-consensual intimate image dissemination.

Several jurisdictions, including England and Wales, Canada, and Singapore, have enacted specific offences criminalizing image-based sexual abuse and have strengthened victim-protection measures, content-removal mechanisms, and extraterritorial enforcement frameworks. These developments reflect a growing recognition of NCIID as a serious violation of privacy, dignity, and sexual autonomy warranting a distinct and comprehensive legal response.

⁷⁰ Aust (n4) 52.

⁷¹ D kaye, *Speech Police: The Global Struggle to Govern the Internet* (Columbia University Press 2019) 134

⁷² 2017 SCC 34.

⁷³ Shaw (n 1) 485.

⁷⁴ Brenner (n 2) 120.

States and international bodies are increasingly adopting measures to address these challenges:

- Expansion of extraterritorial provisions in cybercrime legislation;⁷⁵
- Strengthening of mutual legal assistance treaties (MLATs);⁷⁶
- Development of platform accountability frameworks;⁷⁷
- Recognition of transnational harm-based jurisdiction.⁷⁸

Regional instruments such as the Budapest Convention on Cybercrime promote harmonization of cybercrime laws and facilitate cross-border cooperation.⁷⁹

9.0. Recommendations and Reform Proposals

Against the Backdrop of the foregoing, Effective regulation of non-consensual intimate image dissemination (NCIID) requires a combination of legislative clarity, institutional capacity, and technological responsiveness. A key reform priority is the enactment or refinement of laws that clearly criminalize the creation, distribution, and threatened distribution of intimate images without consent. Such laws should adopt a broad and contextual definition of consent, recognizing that permission to create or share an image privately does not extend to further dissemination.

There is also a need to move away from overly restrictive fault elements, such as requiring proof of intent to cause distress, toward objective standards like recklessness or negligence. This ensures that liability reflects the foreseeable harm caused by the conduct, rather than the subjective motive of the offender.

Given the cross-border nature of digital platforms, States should strengthen extraterritorial jurisdiction provisions and enhance international cooperation mechanisms. Faster procedures for cross-border evidence gathering, data sharing, and enforcement are essential to ensure timely intervention and accountability.

Regulation of digital platforms is equally important. Governments should impose clear legal obligations on social media companies to promptly remove non-consensual content, preserve evidence, and implement preventive technologies. At the same time, such measures must be carefully balanced with the protection of legitimate expression and due process rights.

Victim-centered reforms are crucial. Legal frameworks should provide swift and accessible remedies, including expedited takedown procedures, confidentiality protections, and access to support services such as counselling

⁷⁵ Cybercrimes Act 2020(South Africa); Cybercrimes Act 2015(Nigeria).

⁷⁷ Aust (n4) 60.

⁷⁷ Kaye (n 22) 140.

⁷⁸ Brenner (n2) 130.

⁷⁹ Budapest Convention on cybercrime (Convention on Cybercrime),opened for signature 23 November 2001,ETS No 185(entered into force 1 July 2004).

and legal aid. This helps to mitigate the ongoing harm associated with the widespread and persistent nature of online dissemination.

Ultimately, there is a need for public education and normative change. Awareness campaigns and digital literacy initiatives can play a significant role in reshaping societal attitudes toward privacy, consent, and responsive online behavior. In the long term, harmonization of legal standards across jurisdictions will further strengthen the global response to NCIID and improve enforcement outcomes.

10.0. Conclusion

Against this backdrop, this article has demonstrated that the non-consensual dissemination of intimate images presents a profound challenge to contemporary criminal law, engaging fundamental rights to privacy, dignity and sexual autonomy in an increasingly digital society. Although the Nigerian legal framework provides limited avenues for redress, it remains fragmented and insufficiently equipped to address the distinctive harms associated with image-based sexual abuse. The comparative analysis further reveals that several jurisdictions have adopted bespoke legislative responses that offer more comprehensive protection for victims and more effective mechanisms for offender accountability. The study therefore underscores the urgent need for a coherent and comprehensive legal framework capable of responding effectively to technology-facilitated sexual abuse.

Of equal importance, the findings of this study carry significant implications for law and policy reform in Nigeria. There is an imperative for the enactment of specific legislation criminalizing the non-consensual dissemination of intimate images, accompanied by clearer statutory guidance on consent in digital interactions, stronger privacy safeguards, and effective procedures for the prompt removal of offending content and the prosecution of perpetrators. Equally necessary are strengthened international cooperation, enhanced judicial capacity, and the provision of accessible support services for victims in order to ensure a rights-based and victim-centered response to image-based sexual abuse.

From a forward-looking standpoint, the rapid evolution of digital technologies, particularly artificial intelligence and deepfake technologies, is likely to generate new challenges for criminal law and regulatory enforcement. Future research should therefore examine the implications of these emerging technologies for criminal liability and victim protection, as well as undertake empirical studies on the prevalence and impact of image-based sexual abuse in Nigeria to facilitate evidence-based law reform and the development of a more adaptive and resilient legal framework

Bibliography

Books

- Ashworth A and Horder J, *Principles of Criminal Law* (7th edn, Oxford University Press 2013).
- Aust A, *Handbook of International Law* (2nd ed, Cambridge University Press 2010).
- Brenner SW, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (Northeastern University Press 2012).
- Enabulele, AO, *Human Rights Law and Practice in Nigeria* (Revised edn, Malthouse Press Ltd 2021).
- Kaye D, *Speech Police: The Global Struggle to Govern the Internet* (Columbia University Press 2019).
- Moreham N and Tufal M (eds), *Privacy and Media Law* (3rd edn, Oxford University Press 2017).
- Ormerod D and Laird K, *Smith, Hogan and Ormerod's Criminal Law* (15th edn, Oxford University Press 2018).
- Wacks R, *Privacy and Media Freedom* (2nd edn, Oxford University Press 2013).

Journal Articles

- Citron DK and Franks MA, 'Criminalizing Revenge Porn' (2014) 49 *Wake Forest Law Review* 345.
- MacKinnon CA, 'Pornography as Defamation and Discrimination' (1991) 71 *Boston University Law Review* 793.
- McGlynn C, Rackley E and Houghton R, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25 *Feminist Legal Studies* 25.
- Powell A and Henry N, 'Policing Technology-Facilitated Sexual Violence against Adult Victims: Police and Service Sector Perspectives' (2017) 17 *Policing and Society* 523.

Legislation

Nigeria

- Cybercrimes (Prohibition, Prevention, etc.) Act 2015.
- Constitution of the Federal Republic of Nigeria 1999 (as amended).
- Violence Against Persons (Prohibition) Act 2015.

United Kingdom

- Criminal Justice and Courts Act 2015.
- Data Protection Act 2018.
- Human Rights Act 1998.

United States of America

Computer Fraud and Abuse Act, 18 USC § 1030.

Violence Against Women Act, 34 USC 4 12291.

Intimate Protection Act 2016.

South Africa

Cybercrimes Act 19 of 2020.

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.

Constitution of the Republic of South Africa 1996.

Cases

Nigeria

Federal Republic of Nigeria v Ibori (2014) 15 NWLR (Pt 1425) 1 SC.

United Kingdom

Kaye v Robertson [1991] FSR 62 (CA).

R v Brown [1994] 1 AC 212 (HL).

R v Smith (Wallace Duncan) [2004] EWCA Crim 631.

R v Sheppard and Whittle [2010] EWCA Crim 65.

AMP v Persons Unknown [2011] EWHC 3454 (TCC).

Campbell v MGN Ltd [2004] 2 AC 457 (HL).

United States of America

Stanley v Georgia 394 US 557 (1969).

Katz v United States 389 US 347 (1967).

United States v Ivanov 175 F Supp 2d 367 (D Conn 2001).

United States v Al Kassab 660 F 3d 108 (2d Cir 2011).

Microsoft Corp v United States 548 US---(2018).

South Africa

KS v AM [2017] ZAGPJHC 297.

Teddy Bear Clinic for Abused Children v Minister of Justice [2013] ZACC 35.

Canada

R v Jarvis 2019 SCC 10.

Google LLC v Equustek Solutions Inc 2017 SCC 34.

International Instrument

African Charter on Human and Peoples' Rights (ACHPR), 1981

Budapest Convention on Cybercrime 2001.

Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979.

European Convention on Human Rights 1950.

Non-Consensual Intimate Image Dissemination Under Criminal Law: A Doctrinal And Comparative Analysis Of Consent, Privacy And Extraterritorial Jurisdictions.

International Covenant on Civil and Political Rights (ICCPR), 1966.

The African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) adopted on June 24, 2014.

The Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (the Istanbul Convention) opened for signature on May 11, 2011.

Universal Declaration of Human Rights (UDHR), 1948.