Appraisal of Digital Age Challenges: Cyber Torts and Privacy Rights in Nigerian Law

Adekunle Ademola Aminu* and Morayo Kafilat Sholaja Bello Abdulquddoos*****

Abstract

The rapid advancement of digital technologies has transformed socio-economic interactions while generating complex legal challenges in protecting privacy and regulating civil wrongs in cyberspace. This study critically examines cyber torts and privacy rights within the Nigerian legal framework, assessing the extent to which existing laws address harms such as online defamation, cyberstalking, identity theft, and unauthorised data disclosure. Adopting a doctrinal and comparative methodology, the paper analyses relevant constitutional, statutory, and judicial authorities in Nigeria, drawing on insights from the United Kingdom, the United States, and South Africa. It also engages emerging issues, including artificial intelligence, big data, surveillance capitalism, cross-border jurisdiction, and platform liability. The findings reveal that Nigeria's legal framework remains fragmented, predominantly regulatory and criminal in orientation, and deficient in providing effective civil remedies. The absence of a coherent doctrine of cyber torts and limited judicial innovation further weakens protection for victims of digital harm. The study recommends recognising cyber torts, developing a comprehensive civil liability regime, and strengthening institutional and international cooperation to ensure effective privacy protection in the digital age.

Keywords: Cyber Torts; Digital Privacy; Data Protection; Civil Liability; Platform Liability; Nigerian Law.

1. Introduction

The rapid advancement of digital technology in the twenty-first century has significantly transformed human interactions, commerce, governance, and communication. The emergence of an interconnected

* Adekunle Ademola Aminu, Ph.D, BL, a lecturer at the Faculty of Law, Federal University, Lokoja, Nigeria, adekunle.aminu@fulokoja.edu.com, +2347035236789

** Morayo Kafilat Sholaja, B.Sc (Hons) Political Science, LLB (Hons) morayo0003@yahoo.com, +2347083008803

*** Bello Abdulquddoos, LLB, BL, LLM, PhD In View, Lecturer, Faculty of Law, Federal University Lokoja. Belloabdulquddoos8885@gmail.com, 08066266755

digital ecosystem has enabled the instantaneous creation, storage, and dissemination of information across borders. In Nigeria, the expansion of internet access, largely driven by mobile telephony and increasing smartphone penetration, has facilitated economic development and social engagement. However, this technological progress has also given rise to complex legal challenges, particularly regarding the protection of personal data, online reputation, and individual privacy. The increasing prevalence of digital interactions has exposed individuals to new forms of civil wrongs, commonly described as cyber torts. Unlike traditional torts, cyber torts are characterised by their transnational nature, anonymity of perpetrators, and the rapid dissemination of harmful content. Consequently, conventional tort law principles, developed in an analogue context, often prove inadequate for addressing injuries arising in cyberspace.

As scholars have observed, the architecture of the internet fundamentally alters the nature of harm, thereby necessitating a re-evaluation of existing legal doctrines.[1] The conceptual foundation of privacy law can be traced to the seminal work of Warren and Brandeis, who articulated privacy as "the right to be let alone."[2] This formulation has since influenced the development of privacy jurisprudence across jurisdictions, evolving into a fundamental human right recognised under international law. Instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights affirm the protection of individuals against arbitrary interference with their privacy, family, home, or correspondence.[3] In the digital age, however, the scope of privacy has expanded beyond mere physical intrusion to encompass informational privacy, data protection, and autonomy over personal data.[4] In response to these developments, the European Union, for instance, has established a comprehensive regulatory framework through the General Data Protection Regulation (GDPR), which emphasises accountability,

1 R Crootof, 'The Internet of Torts' (2019) 69 *Duke Law Journal* 583.

2 SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

3 Universal Declaration of Human Rights 1948, Art 12; International Covenant on Civil and Political Rights 1966, Art 17.

4 DJ Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477; NM Richards, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934.

transparency, and individual control over personal data.[5] In the United Kingdom, the decision in *Campbell v MGN Ltd,*[6] marked a significant development in the recognition of the tort of misuse of private information. In the United States, the evolution of privacy torts, particularly as articulated by Prosser, has provided a framework for addressing various forms of informational and reputational harm.[7] Despite these global developments, the Nigerian legal framework remains relatively underdeveloped in addressing civil liability for cyber-related harms. The absence of a clearly articulated doctrine of cyber torts in Nigeria creates significant challenges for victims seeking redress for online harms. Traditional torts such as defamation, negligence, and breach of confidence may, in theory, apply to digital contexts. Nevertheless, their practical application is hindered by jurisdictional issues, evidentiary complexity, and the anonymity inherent in cyberspace.

2. Conceptual and Theoretical Framework

A rigorous analysis of cyber torts and privacy rights requires clarity of key conceptual terms, particularly given the fluidity and overlap that characterise legal discourse in the digital age. Cybercrime generally refers to unlawful acts committed using computers, digital devices, or networks as instruments, targets, or environments of criminal conduct.[8] These include offences such as hacking, identity theft, cyberstalking, and online fraud, which are primarily addressed within criminal law frameworks. In contrast, cyber torts denote civil wrongs committed through digital means, giving rise to private causes of action.[9] Unlike cybercrimes, which attract penal sanctions, cyber torts focus on compensatory remedies for harm suffered by individuals. Such harms include reputational damage (online defamation), emotional distress (cyberbullying), economic loss (data breaches), and violations of personal autonomy (unauthorised data disclosure).[10] The distinction is critical, as many jurisdictions, including Nigeria, have

---

5 C Kuner, L Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020).

6 *Campbell v MGN Ltd* [2004] UKHL 22.

7 WL Prosser, 'Privacy' (1960) 48 *California Law Review* 383.

8 MT Ladan, *Legal Regimes on Cybercrimes and Electronic Evidence in Nigeria and Africa* (2020).

9 R Crootof, (fn.1).

10 D Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014).

developed criminal responses to cyber harms without corresponding civil liability frameworks.

Privacy rights refer to the legal entitlement of individuals to control access to their personal information, communications, and private life.[11] In the digital context, this extends to informational privacy, data protection, and autonomy over digital identity. Privacy is both a constitutional right and a tort-based interest in many jurisdictions, although its doctrinal recognition varies significantly across legal systems. Data protection, while related to privacy, is conceptually distinct. It concerns the regulatory framework governing the collection, processing, storage, and dissemination of personal data.[12] Data protection regimes, such as those found in modern statutes, focus on compliance obligations for data controllers, whereas privacy rights emphasise individual autonomy and dignity.

Contemporary scholarship has expanded the concept of privacy beyond physical intrusion to include informational control. Solove argues that privacy should be understood as a set of related problems, including information collection, processing, dissemination, and invasion.[13] This taxonomy is particularly relevant in the digital age, where harm often arises from data aggregation and misuse rather than direct intrusion. Similarly, Richards emphasises the relationship between privacy and intellectual freedom, arguing that surveillance undermines autonomy, creativity, and democratic participation.[14] This perspective highlights the broader societal implications of privacy violations in digital environments. From a regulatory standpoint, scholars such as Schwartz and Cohen have emphasised the importance of data governance frameworks that balance individual rights with technological innovation.[15] These theories underpin modern data

[11] SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

[12] C Kuner, L Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020).

[13] DJ Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477.

[14] NM Richards, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934.

[15] P Schwartz and J. Cohen, 'Privacy and Data Protection Law' (various works, OUP).

protection regimes and reinforce the need for legal systems to adapt to evolving technological realities.

The interaction between law and technology has also been examined through the lens of regulatory theory. Lessig's influential proposition that "code is law" suggests that the architecture of digital systems can regulate behaviour as effectively as legal rules.[16] This insight is particularly relevant in the context of cyber torts, where platform design, algorithms, and data practices shape the occurrence and impact of harm. Crootof further argues that the internet has fundamentally altered the nature of tortuous conduct, creating what she describes as an "Internet of Torts," where traditional legal categories struggle to accommodate new forms of harm.[17] This underscores the need for doctrinal evolution in tort law.

Privacy is increasingly recognised as a fundamental human right grounded in human dignity. International instruments affirm protection against arbitrary interference with privacy, family, and correspondence.[18] This dignity-based approach has been particularly influential in European jurisprudence, where courts have prioritised personal autonomy and reputation. In comparative African jurisprudence, courts have also adopted a rights-based approach. In *NM v Smith*, the South African Constitutional Court recognised the unauthorised disclosure of private medical information as a violation of privacy, warranting an award of civil damages.[19]This reflects a progressive application of constitutional values to private law disputes, an approach that remains largely underdeveloped in Nigeria.

The convergence of these theories reveals that cyber torts occupy a complex intersection between tort law, constitutional law, and regulatory frameworks. While traditional tort principles provide a foundation, they are insufficient to address the scale, speed, and transnational nature of digital harm. In jurisdictions such as the United Kingdom, courts have responded by developing new doctrines, as seen in *Campbell v MGN Ltd*, where the tort of misuse of private

---

16 L Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).
17 Crootof (fn. 1).
18 Universal Declaration of Human Rights 1948, Art 12; ICCPR 1966, Art 17.
19 *NM v Smith* 2007 (5) SA 250 (CC).

information was recognised.[20] In the United States, courts have applied existing torts to digital contexts, including claims for intentional infliction of emotional distress in cases of online harassment.[21]In Nigeria, however, the absence of similar doctrinal development highlights a significant gap. Although courts have addressed elements of defamation and privacy in cases such as *Ozo Ejeke v Anthony*, the application of these principles to digital environments remains limited.[22]This underscores the need for a coherent theoretical and doctrinal framework to address cyber harms within the Nigerian legal system.

3. Evolution of Privacy and Cyber Torts: A Comparative Perspective

The modern legal conception of privacy has its origins in the late nineteenth century, particularly in the influential work of Samuel D. Warren and Louis D. Brandeis, who articulated privacy as "the right to be let alone."[23] Their intervention was prompted by concerns about technological advancements, such as photography and mass media, which enabled unprecedented intrusions into private life. This foundational articulation laid the groundwork for the recognition of privacy as a distinct legal interest in common law jurisdictions. In the United States, courts began to recognise privacy-based claims, culminating in Prosser's doctrinal classification, which identified four distinct privacy torts: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of likeness.[24]

This framework significantly shaped American jurisprudence and continues to influence contemporary approaches to privacy law. In the twentieth century, particularly after the Second World War, privacy became a fundamental human right under international law. The United Nations recognised privacy in the Universal Declaration of Human Rights, which provides that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence.[25] This protection was further reinforced in the

---

20 *Campbell v MGN Ltd* [2004] UKHL 22.
21 *Doe v Hofstetter* (2012) (US District Court).
22 *Ozo Ejeke v Anthony* (2009) (CA)
23 SD Warren and LD Brandeis ‘The Right to Privacy’ (1890) 4 *Harvard Law Review* 193.
24 WL Prosser, ‘Privacy’ (1960) 48 *California Law Review* 383.
25 Universal Declaration of Human Rights 1948, Art 12.

International Covenant on Civil and Political Rights, which imposes binding obligations on state parties to safeguard privacy rights.[26] This rights-based approach has had a profound influence on domestic legal systems, particularly in jurisdictions that incorporate international human rights norms into their constitutional frameworks. In Europe, privacy is closely linked to human dignity and personal autonomy, forming the basis for extensive legal protections in both constitutional and statutory regimes.[27]The advent of digital technologies has fundamentally altered the scope and nature of privacy. Unlike traditional forms of intrusion, digital privacy concerns arise from the collection, processing, and dissemination of personal data on a massive scale. Scholars such as Solove have argued that modern privacy harms are better understood as a constellation of interrelated problems involving data aggregation, surveillance, and information misuse.[28]

In response, several jurisdictions have adopted comprehensive data protection frameworks. The European Union's General Data Protection Regulation (GDPR) is among the most advanced regulatory regimes, establishing principles such as data minimisation, purpose limitation, and accountability.[29]The GDPR also introduces enforceable rights for individuals, including the right to access, rectify, and erase personal data, thereby strengthening individual control over digital identity. Similarly, courts have adapted traditional legal doctrines to address digital harms. In *Campbell v MGN Ltd*, the House of Lords recognised the tort of misuse of private information, marking a significant departure from the traditional breach-of-confidence framework.[30] This development was further reinforced in *PJS v News Group Newspapers Ltd*, where the UK Supreme Court emphasised the importance of protecting privacy even in the context of widespread online dissemination.[31] In the United States, the evolution of privacy law has been closely tied to tort principles. Building on Prosser's framework, courts have applied traditional tort doctrines to emerging digital harms.

---

26 International Covenant on Civil and Political Rights 1966, Art 17.

27 CKuner, .L Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

28 DJ Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania Law Review* 477.

29 Kuner, Bygrave and Docksey (fn. 27).

30 *Campbell v MGN Ltd* (2004) 2 AC 457 (HL).

31 *PJS v News Group Newspapers Ltd* (2016) UKSC 26.

For instance, claims for intrusion upon seclusion and public disclosure of private facts have been extended to cases involving online surveillance and unauthorised dissemination of personal information.[32]Additionally, American courts have addressed issues of online harassment and harmful speech through doctrines such as intentional infliction of emotional distress. In *Elonis v. United States,* the Supreme Court considered the criminal implications of threatening speech on social media, highlighting broader legal challenges in regulating online conduct.[33] While this case arose in a criminal context, it underscores the difficulties of applying traditional legal standards to digital communication. Scholarly contributions have further advanced the discourse on cyber torts. Citron, for example, has extensively analysed the inadequacy of existing legal frameworks in addressing cyber harassment and abuse, advocating for stronger civil remedies to protect victims.[34]

In Africa, the development of privacy law has been uneven, though some jurisdictions have made significant progress. South Africa, in particular, has adopted a robust constitutional approach to privacy. In *NM v Smith*, the Constitutional Court held that the unauthorised disclosure of an individual's HIV status constituted a violation of privacy, thereby affirming the availability of civil remedies for such harm.[35] This case illustrates the application of constitutional values to private law disputes, a principle known as horizontal application. Kenya has also made strides in data protection through the enactment of the Data Protection Act 2019, which establishes a comprehensive framework for regulating the processing of personal data. Although judicial interpretation is still developing, the legislation reflects a growing recognition of privacy as a critical legal issue in the digital age. In contrast to these developments, the legal framework in Nigeria has evolved more slowly.

While the Constitution guarantees the right to privacy under section 37, judicial interpretation has remained largely conservative, focusing

[32]PM Schwartz and DJ Solove, *Information Privacy Law* (6th edn, Wolters Kluwer, 2018).
[33]*Elonis v United States* 575 US 723 (2015).
[34]D.K. Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).
[35]*NM v Smith* 2007 (5) SA 250 (CC).

on physical and communicational privacy rather than the broader implications of digital technology.[36] Legislative interventions such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and the Nigerian Data Protection Act 2023 represent important steps toward regulating cyberspace. However, these frameworks are primarily criminal and regulatory in nature, with limited emphasis on civil liability. As a result, victims of cyber harms often lack effective tort remedies.Compared with jurisdictions such as the United Kingdom, the United States, and South Africa; Nigeria lacks a clearly defined doctrine of cyber torts, placing it at a disadvantage as courts in these jurisdictions have demonstrated greater willingness to adapt legal principles to technological change.

4. Legal Framework on Privacy and Cyber Torts in Nigeria

The right to privacy in Nigeria is primarily rooted in the Constitution of the Federal Republic of Nigeria 1999 (as amended), which guarantees the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications.[37] This provision establishes privacy as a fundamental right enforceable against the state. However, judicial interpretation of this right has traditionally been narrow, often limited to physical intrusions and state surveillance, with limited extension to digital environments. Nigerian courts have, in several instances, affirmed the importance of privacy as a constitutional safeguard.

In *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo*, the Supreme Court emphasised the autonomy of individuals in matters of personal decision-making, reinforcing the broader concepts of personal liberty and privacy.[38] Although the case did not directly address digital privacy, it reflects a judicial willingness to protect personal autonomy, which could be extended to informational privacy in appropriate circumstances. Despite this constitutional foundation, there is a noticeable absence of jurisprudence directly addressing digital privacy rights.

---

[36] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

[37] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

[38] *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo* (2001) 7 NWLR (Pt 711) 206 (SC).

The failure to interpret section 37 in light of technological developments has created a gap between constitutional guarantees and contemporary realities. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 represents Nigeria's principal legislative response to offences committed in cyberspace. The Act criminalises a wide range of conduct, including unlawful access to computer systems, identity theft, cyberstalking, and electronic fraud.[39] Notably, section 24 of the Act addresses cyberstalking and the use of electronic communication to harass, threaten, or cause emotional distress. While the Act provides a robust framework for criminal enforcement, it is largely silent on civil liability.

The enactment of the Nigerian Data Protection Act 2023 marks a significant development in the regulation of personal data in Nigeria. The Act establishes a comprehensive framework governing the collection, processing, and storage of personal data, and creates the Nigeria Data Protection Commission (NDPC) as the primary regulatory authority.[40] The Act introduces key data protection principles, including lawfulness, fairness, transparency, purpose limitation, and data minimisation. It also grants individuals enforceable rights, such as the right to access, rectify, and erase personal data. These provisions align Nigeria with global standards, particularly those reflected in the European Union's GDPR.

However, the Act remains primarily regulatory in nature. While it provides for administrative sanctions and compliance obligations, it does not clearly establish a tort-based mechanism for compensating victims of data breaches or privacy violations. As a result, individuals seeking redress must rely on indirect or alternative legal avenues. The Evidence Act 2011 plays a crucial role in the adjudication of cyber-related disputes by recognising the admissibility of electronic evidence. Section 84 of the Act provides the conditions under which computer-generated evidence may be admitted in Court.[41]This provision represents an important step in modernising Nigeria's legal system, as it facilitates the use of digital evidence in both civil and criminal proceedings. The Nigerian judiciary has yet to develop a

[39] Cybercrimes (Prohibition, Prevention, etc.) Act 2015.
[40] Nigerian Data Protection Act 2023.
[41] Evidence Act 2011, s 84.

robust body of case law addressing cyber torts and digital privacy. Existing decisions on privacy and defamation are largely grounded in traditional legal principles, with limited adaptation to digital contexts.

For instance, in *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo*, the Supreme Court recognised the importance of individual autonomy, which is closely linked to privacy rights.[42] Similarly, Nigerian courts have addressed defamation in various cases, establishing principles that could potentially be applied to online publications. However, there is little direct authority on cyber defamation or other digital torts. When viewed in comparative perspective, Nigeria's legal framework reveals significant gaps. Jurisdictions such as the United Kingdom and South Africa have demonstrated greater willingness to adapt legal principles to technological change, recognising new forms of liability and providing effective remedies for victims.

5. Doctrinal Gaps and Challenges in the Regulation of Cyber Torts and Privacy in Nigeria

A central weakness in Nigeria's legal framework is the absence of a clearly articulated doctrine of cyber torts. While traditional tort law provides remedies for civil wrongs such as defamation, negligence, and breach of confidence, these principles have not been systematically adapted to address harms arising in digital environments.[43] The concept of cyber torts, civil wrongs committed through electronic means, remains largely undefined in Nigerian jurisprudence. Unlike jurisdictions such as the United Kingdom, where courts have developed the tort of misuse of private information, Nigerian courts have yet to recognise an equivalent cause of action.[44] This doctrinal vacuum creates uncertainty for litigants and limits the availability of civil remedies for victims of online harm.

Furthermore, the reliance on inherited common law principles without corresponding judicial innovation has constrained the development of a modern tort framework capable of addressing the realities of cyberspace. As a result, victims of digital harm are often unable to fit their claims within existing legal categories. Another significant

---

42 *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo* (n 2).
43 R Crootof, 'The Internet of Torts' (2019) 69 *Duke Law Journals* 583.
44 *Campbell v MGN Ltd* (2004) 2 AC 457 (HL).

challenge lies in the predominance of criminal law in addressing cyber-related harms. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 provides a comprehensive framework for prosecuting offences such as cyberstalking, identity theft, and online fraud.[45]

However, the Act is primarily punitive in nature and does not provide adequate avenues for civil redress.This over-reliance on criminal law creates a structural imbalance, prioritising punishment over compensation. Victims of cyber harm often seek remedies such as damages, injunctions, or the removal of harmful content, reliefs that are not readily available under criminal proceedings.[46] Consequently, the absence of a parallel civil liability regime undermines the effectiveness of legal protection in the digital space. Although traditional torts such as defamation and breach of confidence may, in theory, apply to cyber contexts, their practical application is fraught with challenges. In Nigerian law, the tort of defamation requires proof of publication, falsity, and reputational harm.[47]

While these elements can be established in cases of online defamation, issues such as anonymity, rapid dissemination, and jurisdiction complicate enforcement. In *Guardian Newspapers Ltd v Ajeh*, the Court of Appeal reaffirmed the essential elements of defamation, emphasising the need for clear identification of the defamatory statement and its publication to a third party.[48] However, the application of these principles to digital platforms, where content can be shared instantly and globally, remains underdeveloped. Similarly, the tort of breach of confidence may be relevant in cases involving unauthorised disclosure of personal data. However, Nigerian courts have not fully explored their applicability to modern data protection issues. In contrast, jurisdictions such as the United Kingdom have developed robust mechanisms for civil redress. In *Campbell v MGN Ltd*, the Court recognised the availability of damages for misuse of private information, thereby providing a remedy for privacy

[45]Cybercrimes (Prohibition, Prevention, etc.) Act 2015.
[46]R. Rabin, 'Perspectives on Privacy, Data Security and Tort Law' (2016) 66 *DePaul Law Review* 313.
[47]*Guardian Newspapers Ltd v Ajeh* (2011) 10 NWLR (Pt 1255) 574 (CA).
[48]ibid.

violations.[49] Similarly, courts have granted injunctions to prevent the publication of sensitive information, even in digital contexts.

The absence of similar remedies in Nigeria leaves victims without practical means to address the harm. Procedural complexities, high costs, and delays in the judicial process further hinder litigation.[50] These barriers discourage victims from pursuing legal action and contribute to a culture of impunity in cyberspace. Cyber torts are inherently transnational, often involving multiple jurisdictions. Content published in one country may be accessed globally, creating complex questions of jurisdiction and applicable law. In Nigeria, the legal framework for addressing cross-border disputes remains underdeveloped.

The difficulty of asserting jurisdiction over foreign defendants and digital platforms poses a significant challenge. In addition, the lack of effective mechanisms for international cooperation limits the Nigerian authorities' ability to investigate and enforce legal rights.[51] The absence of clear rules on the territorial scope of Nigerian law in cyberspace compounds these challenges. As a result, victims of cross-border cyber harm face significant obstacles in seeking redress. The anonymity afforded by digital platforms presents another major obstacle to the enforcement of cyber torts. Perpetrators can conceal their identities through pseudonyms, virtual private networks (VPNs), and encrypted communication channels. This makes it difficult to identify defendants and establish liability.

There is limited institutional support for civil litigation or victim compensation.[52]Moreover, public awareness of privacy rights and cyber harms remains low, leading to underreporting and limited utilisation of available legal remedies. The Nigerian judiciary has generally adopted a conservative approach to legal interpretation, particularly in emerging areas such as cyber law. Courts have been reluctant to extend traditional tort principles to digital contexts or to

---

[49] *Campbell v MGN Ltd* (n 2).

[50] MT Ladan, *Legal Regimes on Cybercrimes and Electronic Evidence in Nigeria and Africa* (Ahmadu Bello University Press 2020).

[51] GA Gilmore, 'Suing the Surveillance State: The (Cyber) Tort Exception' (2014) 46 *Columbia Human Rights Law Review* 227.

[52] Nigerian Data Protection Act 2023.

recognise new causes of action. This conservatism has resulted in a lack of judicial precedents addressing cyber torts and digital privacy. Without authoritative guidance from the courts, legal practitioners face uncertainty in framing claims, and victims are discouraged from pursuing litigation. In contrast, courts in other jurisdictions have demonstrated greater willingness to engage in doctrinal innovation. The development of new torts and the expansion of existing principles have played a crucial role in addressing digital harms.[53]

The Nigerian legal framework is characterised by fragmentation. Privacy and cyber-related issues are addressed across multiple legal instruments, including the Constitution, the Cybercrimes Act, the Nigerian Data Protection Act, and the Evidence Act. However, these instruments operate independently, without a unified or coherent structure. This fragmentation creates gaps and overlaps, leading to inconsistencies in enforcement and interpretation. It also complicates the legal landscape for individuals seeking to understand and assert their rights.

6. Comparative Jurisprudence on Cyber Torts and Digital Privacy

A comparative analysis of cyber torts and digital privacy reveals significant divergences in how legal systems respond to technologically mediated harm. While some jurisdictions have proactively adapted their legal frameworks through judicial innovation and legislative reform, others, such as Nigeria, continue to rely on traditional doctrines that are ill-suited to the complexities of cyberspace. Historically, English law did not recognise a general right to privacy. However, the incorporation of the European Convention on Human Rights through the Human Rights Act 1998 catalysed a significant transformation in judicial reasoning. In *Campbell v MGN Ltd*, the House of Lords recognised the tort of misuse of private information, thereby marking a decisive shift from the traditional doctrine of breach of confidence.[54]

The case involved the publication of details concerning the claimant's medical treatment, and the Court held that such disclosure constituted an unjustified interference with her privacy. This decision established a two-stage test: first, whether the claimant had a reasonable

[53] DK Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014).
[54] *Campbell v MGN Ltd* (2004) 2 AC 457 (HL).

expectation of privacy; and second, whether that expectation was outweighed by competing interests, particularly freedom of expression. Subsequent decisions have refined and expanded this doctrine.

In *PJS v News Group Newspapers Ltd*, the Supreme Court granted an injunction restraining the publication of private information, notwithstanding the widespread dissemination of the material on the internet.[55] In the United States, the development of privacy law has been shaped by both tort principles and constitutional considerations. Building on the foundational work of Prosser, American jurisprudence recognises four distinct privacy torts: intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of likeness.[56] These categories have been widely adopted and adapted to address digital harms. American courts have extended these torts to cover various forms of online misconduct, including unauthorised data collection and dissemination.

The Restatement (Second) of Torts provides a doctrinal foundation for these developments, particularly in the areas of intrusion upon seclusion and public disclosure of private facts.[57]However, the expansion of privacy torts in the United States is constrained by the constitutional protection of freedom of speech under the First Amendment. Courts must balance privacy interests against the public interest in free expression, particularly in cases involving media publications or matters of public concern. In *Cox Broadcasting Corp v Cohn*, the Supreme Court held that the publication of truthful information obtained from public records could not give rise to liability, thereby limiting the scope of privacy protection.[58] Similarly, in *Snyder v Phelps*, the Court prioritised freedom of speech over claims for emotional distress arising from offensive expression.[59]

Despite these constraints, American scholarship has played a crucial role in advancing the discourse on cyber torts. Scholars such as

---

55 *PJS v News Group Newspapers Ltd* (2016) UKSC 26.
56 WL Prosser, 'Privacy' (1960) 48 *California Law Review* 383.
57 *Restatement (Second) of Torts* (American Law Institute 1977).
58 *Cox Broadcasting Corp v Cohn* 420 US 469 (1975).
59 *Snyder v Phelps* 562 US 443 (2011).

Danielle Keats Citron have highlighted the inadequacy of existing legal frameworks in addressing cyber harassment and online abuse, advocating for stronger civil remedies and legislative reform.[60] South Africa offers a particularly instructive model for the development of privacy law within a constitutional framework. The Constitution of the Republic of South Africa explicitly guarantees the right to privacy, which the courts have interpreted expansively.

In *NM v Smith*, the Constitutional Court held that the unauthorised disclosure of an individual's HIV status constituted a violation of privacy, warranting the award of damages.[61] The Court emphasised the importance of dignity and autonomy, recognising privacy as a fundamental component of human rights. A distinctive feature of South African jurisprudence is the horizontal application of constitutional rights, whereby constitutional values directly influence private law relationships. This approach has facilitated the development of privacy-based claims within the law of delicts (tort), enabling courts to adapt legal principles to contemporary challenges. South Africa has enacted comprehensive data protection legislation, the Protection of Personal Information Act (POPIA), which establishes a regulatory framework for the processing of personal data. This dual approach, combining constitutional protection with statutory regulation, provides a robust model for addressing digital privacy.

The evolution of cyber torts and privacy law is increasingly shaped by rapid technological developments, particularly in the domains of artificial intelligence (AI), big data analytics, and platform-based digital ecosystems. These developments have not only intensified traditional privacy concerns but have also generated novel forms of harm that challenge existing legal frameworks. This section examines key emerging issues with significant implications for civil liability and regulatory intervention. Artificial intelligence has transformed data processing by enabling large-scale automated profiling**,** predictive analytics, and behavioural inference. AI systems can aggregate vast datasets to generate detailed profiles of individuals, often without their knowledge or meaningful consent.[62]Data profiling raises profound

[60] D.K Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014).
[61] *NM v Smith* 2007 (5) SA 250 (CC).

[62] European Data Protection Board, *Opinion 28/2024 on AI Models* (2024).

concerns for privacy and autonomy, particularly where algorithmic decision-making affects access to employment, credit, healthcare, or public services. The opacity of AI systems, often described as "black box" technologies, complicates accountability and undermines transparency.[63]

Recent regulatory developments in Europe reflect growing concern over these risks. The European Data Protection Board has emphasised the need for safeguards in AI-driven data processing, particularly in relation to automated decision-making and profiling.[64] Similarly, emerging scholarship highlights that AI not only predicts behaviour but may actively shape and influence it, thereby blurring the line between observation and manipulation. For Nigeria, the absence of clear legal standards governing AI-driven profiling creates significant risks. Without regulatory intervention, individuals remain vulnerable to opaque and potentially discriminatory algorithmic practices. The rise of big data has given birth to what scholars describe as *surveillance capitalism*, an economic model in which personal data is commodified and exploited for profit.[65]

Digital platforms collect vast amounts of behavioural data from users, including browsing habits, location data, and social interactions, which are then analysed to predict and influence behaviour. This model has been significantly enhanced by AI technologies, enabling real-time data analysis and behavioural prediction at unprecedented scale.[66] As noted in recent scholarship, surveillance capitalism operates by extracting "behavioural surplus" and converting it into predictive products for commercial gain.[67]

The activities of data brokers further exacerbate this problem. These entities aggregate personal data from multiple sources to create detailed profiles, which may be sold to advertisers, corporations, or

---

63 F Pasquale, *The Black Box Society* (Harvard University Press 2015).

64 European Data Protection Board (n 1).

65 K Lipartito, 'Surveillance Capitalism: Origins, History, Consequences' (2025) *Histories*.

66 U Reviglio, 'Data Brokers and Surveillance Capitalism' (2022) *Internet Policy Review*.

67 S Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).

even government agencies.[68] This raises serious concerns about consent, transparency, and the erosion of individual autonomy. Recent developments have highlighted the extent of these risks. Reports indicate that government agencies increasingly rely on commercially available data to conduct large-scale surveillance, thereby circumventing traditional legal safeguards. For legal systems, surveillance capitalism presents a fundamental challenge: traditional privacy doctrines are ill-equipped to address harms arising from systemic data extraction and algorithmic manipulation. Cyber torts are inherently transnational, raising complex issues of jurisdiction and applicable law. Digital content published in one jurisdiction may be accessed globally, creating overlapping claims and conflicting legal standards.

The challenge of cross-border jurisdiction has been addressed in various jurisdictions through principles such as the "effects doctrine," which allows courts to assert jurisdiction over a case where harm is suffered. However, enforcement remains problematic, particularly where defendants are located in foreign jurisdictions or operate through anonymous digital identities. The global nature of data flows further complicates regulation. Data collected in one country may be processed in another and stored across multiple jurisdictions, making it difficult to determine which legal frameworks apply.[69]For Nigeria, the absence of clear rules on extraterritorial jurisdiction and limited participation in international enforcement mechanisms significantly hinders the effective regulation of cyber torts. Digital platforms such as Meta Platforms, X, and Google play a central role in the dissemination of online content. Their influence raises critical questions regarding platform liability for harmful content. In many jurisdictions, platforms benefit from “safe harbour” protections, which limit liability for user-generated content. However, increasing concerns over misinformation, cyber harassment, and privacy violations have prompted calls for stricter regulation.

---

[68] S Larkin and S. Abuzneid, ‘Data Broker Loopholes and Privacy’ (2024) *Journal of Information Security*.

[69] Crootof (fn.43).

7. Conclusion and Recommendations

This study has demonstrated that while Nigeria possesses a foundational legal framework for the protection of privacy, anchored in constitutional provisions and supplemented by statutes such as the Nigerian Data Protection Act 2023 and the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, its legal system remains inadequately equipped to address the complex realities of cyber torts in the digital age. The persistence of doctrinal gaps, the over-reliance on criminal law mechanisms, the limited development of civil remedies, and the absence of a coherent jurisprudence on digital privacy collectively undermine the effective protection of individuals against technologically mediated harm. Comparative analysis with jurisdictions such as the United Kingdom, the United States, and South Africa reveals a clear trajectory toward judicial innovation, legislative responsiveness, and the recognition of privacy as a dynamic and enforceable right within both public and private law. These jurisdictions demonstrate that the evolution of cyber torts is neither accidental nor purely legislative; rather, it is the product of a deliberate interplay between courts, lawmakers, and regulatory institutions. In contrast, the Nigerian experience reflects a cautious, fragmented approach that, while preserving doctrinal stability, has impeded the development of a robust legal response to emerging digital harms.

In light of these findings, this paper recommends a multi-layered reform strategy. First, there is an urgent need for the formal recognition and development of cyber torts within Nigerian law, either through legislative codification or judicial innovation. Courts should be encouraged to adopt a purposive approach to extending existing tort principles, such as defamation and breach of confidence, to digital contexts, while drawing on persuasive comparative authorities. Second, the Nigerian Data Protection Act 2023 should be strengthened to incorporate explicit provisions on civil liability, including statutory damages and mechanisms for judicial enforcement, particularly in relation to data breaches and automated decision-making systems. Furthermore, a comprehensive civil remedies framework must be established to enable victims to obtain compensatory damages, injunctive relief, and takedown orders against digital platforms. Institutional capacity should also be enhanced through increased funding, technical training, and the establishment of specialised cyber law units within the judiciary and regulatory bodies.

Finally, Nigeria must actively engage in international cooperation mechanisms to address the transnational nature of cyber torts, including participation in global data protection initiatives and cross-border enforcement frameworks. Ultimately, the regulation of cyber torts and digital privacy in Nigeria must evolve beyond its current fragmented structure toward a coherent and integrated legal system. Such a transformation is essential not only for protecting individual rights but also for fostering trust, accountability, and justice in an increasingly digitised society.