CURRENT TRENDS IN HUMANITIES AND LAW RESEARCH

BABCOCK UNIVERSITY

Received: 11-03-2025
Accepted: 05-06-2025

ISSN: 2814-1695

https://doi.org/10.61867/pcub.v3i1a.207

CTHLR 3(1): 151-160 (June, 2025)

DATA PRIVACY CONCERNS: CHALLENGES IN SEEKING REDRESS FOR SOCIAL MEDIA DATA BREACHES*

Emmanuel C. Emmanuel [1]
emmanuelch@babcock.edu.ng

and

Oyindamola O. Olumuyiwa [2]
sikemiolumuyiwa@gmail.com

Babcock University,
School of Law & Security Studies,
Ilishan-Remo Ogun State, Nigeria,

Corresponding Author Email: emmanuelch@babcock.edu.ng

* EMMANUEL, Chinaka Emmanuel, Lecturer, School of Law and Security Studies, Babcock University, Ilisan Remo, Ogun State, Nigeria. Email: Emmanuelch@babcock.edu.ng
** Olumuyiwa Oluwasikemi Oyindamola, Graduate, School of Law and Security Studies, Babcock University, Ilisan Remo, Ogun State, Nigeria. Email: sikemiolumuyiwa@gmail.com

Data Privacy Concerns: Challenges in Seeking Redress for Social Media Data Breaches

Abstract

The existence of social media platforms in modern-day society, though very helpful, has brought about significant data privacy concerns. The operation of many social media platforms is dependent on a practice of collecting and processing the personal and sensitive data of users of the social media platforms. This has introduced an erroneous culture of the infringement of data privacy rights of social media platform users by way of data breaches. The doctrinal research design employed in this study is the doctrinal design, which is a desk-based approach that focuses on the analysis of the existing legal text, instead of its application. The study revealed that there are challenges faced by individuals whose data has been breached by social media platforms and are seeking legal redress. Furthermore, the study accentuates certain challenges that are procedural in nature and how detrimental they can be to a data breach suit. This study concluded that data privacy is a fundamental phenomenon, the absence of which leads to numerous data breaches, with the resultant consequences posing a threat to justice. The study recommended the need for an international or global legal framework aimed at providing a standard practice and approach in data privacy activities.

Keywords: Breach of Data, Data Privacy, Justice, Law and Technology, Social Media Platforms.

1.1. Introduction

Social media serves as a conduit between the data owner (data generator) and viewers (end users). Research reveals that more than 1 billion people use one or more online social networks, including Facebook, Twitter, YouTube, and Google, demonstrating the

unprecedented levels of human connectivity. Personal details, current address, hometown, email addresses, instant messaging usernames, activities, interests, favorite sports, favorite teams, favorite athletes, favorite music, television shows, games, languages, his religious and political beliefs, inspirations, favorite quotes, service user history, education history, relationship status, family members, and software applications are just a few of the vast amounts of data that users provide and share on these social networks. Additionally, the user submits revisions in the form of Tweets or status updates, which may contain a video, an act, a link, or a thought. All of these details reveal a lot about the individual that will be useful to other organizations.[1]

Due to numerous negative events, social networks have been held accountable for violating users' privacy. The value of a user's secrecy has seldom ever been addressed in the media or in academia. Numerous efforts have been made to educate consumers so they do not divulge too much personal information, in addition to various technical solutions that have been suggested. Additionally, social network data is now being linked to users' actual locations, enabling real-time interaction between users' physical surroundings and information about their interests and social connections. Online social networks and real-world mobile computing have combined to generate a rapidly expanding range of applications with distinct needs and as-yet-unknown repercussions.[2]

Therefore, it is has become impossible to overestimate the significance of data and privacy protection in this age of rapid technological innovation. The purpose of this study is to discuss the new issues surrounding data and privacy protection, especially in Nigeria, with the increasing use of social media platforms. It aims to reveal the scope of privacy and data protection issues in Nigeria, suggesting possible ways to resolve these challenges.[3]

2.1. Nature of Data Privacy

Since the beginning of the information era, there has been a great deal of focus on the right to privacy and the corresponding need to secure personal data. Legislative advancements have

[1] Sakshi Rewaria, 'Data Privacy in Social Media Platform: Issues and Challenges' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3793386> accessed 10 October 2025.
[2] ibid.
[3] Patrick Chukwunonso Aloamaka, 'Data Protection and Privacy Challenges in Nigeria: Lessons from other Jurisdictions' (2023) 3 UCC Law Journal 281.

not kept up with the exponential growth of the internet, online information sharing, and data collection, and have not sufficiently protected personal data. But in an effort to address and defend their residents' right to privacy, many areas, including Nigeria, have started implementing laws and policies pertaining to data protection.[4]

Data has been defined in a variety of ways by numerous scholars. The word 'data' is the plural version of a Latin word *datum* which means 'facts or statistics used for reference or analysis.'[5] According to John Hicks, data is 'a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation, or processing by humans or by automatic means.'[6] Section 1(3) of the Nigerian Data Protection Regulation refers to data as symbols, binary, and characters that are processed by a computer, stored in any format or device, and are capable of being transmitted or maintained in the form of electronic signals.

Section 58 of the Cybercrimes Act also defines data as the representation of concepts or information that is prepared in a form suitable for use in a computer.[7] As data has been defined as information, it may be either Personally Identifiable Information (PII) or Non-Personally Identifiable Information (NPII).[8] Personally identifiable information refers to any data that is associated with a specific individual, and can be utilized to ascertain that individual's identity.[9] PII includes but is not limited to: full name, gender, home address, email address, phone number, social security number, driver's license number, international passport number, credit card number.[10] Non-personally identifiable information refers to data that by itself, cannot be used to trace or identify an individual.[11] They include internet protocol (IP) address, cookies, device identification and international mobile equipment identity (IMEI) number.[12]

[4] Media Defence, 'Module 4: Data Privacy and Data Protection' <https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-4-Data-privacy-and-data-protection.pdf> accessed 8 October 2025.
[5] Subhrangsu Santra, 'Data: Types and Sources – Methodology of Research in Sociology' <https://ebooks.inflibnet.ac.in/socp3/chapter/data-types-and-sources/> accessed 4 October 2025.
[6] ibid.
[7] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 58.
[8] Akinkunmi Akinwunmi, *The Nigerian Internet Law* (Ciplus Limited 2019).
[9] IBM, 'What is Personally Identifiable Information (PII)? <https://www.ibm.com/topics/pii> accessed 14 October 2024.
[10] University of Pittsburgh, 'Guide to Identifying Personally Identifiable Information (PII)' <https://services.pitt.edu/TDClient/33/Portal/KB/ArticleDet?ID=1965> accessed 4 October 2025.
[11] Piwik Pro, 'Non-Personally Identifiable Information (Non-PII)' <https://piwik.pro/glossary/non-personally-identifiable-information-non-pii/> accessed 14 July 2025.
[12] Chris Chao, 'What is PII, Non-PII, and Personal Data?' <https://www.centerpointit.com/what-is-pii-non-pii-and-personal-data/> accessed 4 October 2025.

Privacy is a concept which has more than one meaning. In general terms, privacy refers to the right to be left alone.[13] It is also said to be the freedom from disturbance, or unwanted interference.[14] These definitions are however very limiting, and cannot be said to fully explain the concept. There are many classifications of privacy by erudite scholars, but the main focus of this paper is data privacy. Data privacy refers to the principle that grants individuals authority over their personal data, specifically around its collection, analysis, storage, and utilisation.[15] It is the branch of data management that focuses on handling personal data in accordance with data protection laws, regulations, and general best privacy practices.[16] The main purpose of data privacy is to ensure that the sensitive data of individuals is not misused. It gives these individuals the authority to decide who can access their personal information, and how this information is administered. Data privacy ensures that data which is collected for a specific reason is used and handled accordingly.

Social media platforms are the specific websites or applications which allow social media users to create and share content, and to take part in social networking.[17] They are also referred to as interactive digital channels that facilitate the creation and dissemination of thoughts, ideas, and information via virtual networks. These platforms allow users to participate in social networking by creating content, sharing their ideas, commenting on other users' content, and reposting it.[18] Some of the most popular social media platforms includes but is not limited to: Facebook, YouTube, Instagram, WhatsApp and TikTok.[19]

Social media has had, and is still having an impact on society, and humanity at large. For many, social media has improved communication greatly.[20] The creation of social media platforms enables people to maintain constant and instant communication, which permits them to stay in touch across the globe. Additionally, social media provides an outlet for

[13] IAPP, 'What is Privacy' <https://iapp.org/about/what-is-privacy> accessed 14 September 2025.
[14] ibid.
[15] Matthew Kosinski and Amber Forrest, 'What is Data Privacy?' <https://www.ibm.com/topics/data-privacy> accessed 1 October 2025.
[16] Talend, 'What is Data Privacy? Definition and Compliance Guide' <https://www.talend.com/resources/data-privacy/> accessed 14 October 2024.
[17] Maheen Kanwal, 'Social Media Platform' <https://www.webopedia.com/definitions/social-media-platform/> accessed 26 March 2025.
[18] ibid.
[19] Ankit Vora, 'The 20 Most Popular Social Media Platforms in 2025' <https://backlinko.com/social-media-platforms> accessed 26 March 2025.
[20] Gaurav Raju, 'What is the Real Impact of Social Media?' <https://www.simplilearn.com/real-impact-social-media-article> accessed 26 March 2025.

creativity.[21] In today's world, social media is a growing hub for personal growth and creativity. It allows for individuals of all ages to showcase their creative works, learn a new skill, pursue a sport or do whatever it is that piques their interest. Social media also has its negative effects. One of such negative effects is data privacy concerns which is the crux of this paper.[22] While setting up accounts on social media platforms, individuals are required to give out a significant amount of their personal data. Over the years, many of these social media platforms have been found to have vulnerable security systems, which has in turn led to unauthorised persons gaining access to these security systems. Additionally, it has been found that certain social media platforms often use the data they collect from their users for purposes other than which the data was collected for. This has caused users of social media worldwide great concern about their data privacy rights.

A breach is defined as the failure to meet an obligation established by promise, duty, or law, without any cause or justification.[23] It is also said to be an infraction or violation of a law, trust, faith or promise.[24]A data breach on the other hand refers to any security incident where unauthorised personnel gain access to sensitive and confidential information such as personal data and corporate data.[25] A data breach occurs within an organisation when a security incident compromises the confidentiality, availability, or integrity of data (including personal information) handled by the organisation. [26]

Under section 65 of the Nigerian Data Protection Act 2023, personal data breach means 'a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed'. A cybersecurity firm, Surfshack, reported a 64% increase in data breach incidents in Nigeria during the first quarter of 2023,

[21] Linda C Ashar, 'Social Media Impact: How Social Media Sites Affect Society' <https://www.apu.apus.edu/area-of-study/business-and-management/resources/how-social-media-sites-affect-society/> accessed 26 March 2025.
[22] ibid.
[23] FindLaw Legal Dictionary, 'Breach' <https://dictionary.findlaw.com/definition/breach.html> accessed 20 November 2024.
[24] The Free Dictionary, 'Breach' <https://www.thefreedictionary.com/breach> accessed 15 November 2024.
[25] Matthew Kosinski, 'What is a Data Breach?' <https://www.ibm.com/topics/data-breach> accessed 15 November 2024.
[26] Udo Udoma & Belo-Osagie, 'Compliance Obligations under the Nigerian Data Protection Act 2023 2' <https://uubo.org/wp-content/uploads/2023/09/DATA-BREACHES-AND-REGULATORY-COMPLIANCE-OBLIGATIONS-UNDER-THE-NIGERIAN-DATA-PROTECTION-ACT.pdf> accessed 15 November 2024.

totalling 82,000 occurrences, up from 50,000 in the fourth quarter of 2022. The 64% data breach ranked Nigeria as the 32nd most targeted country by hackers globally.[27]

2.1. Nature of Data Privacy

Since the beginning of the information era, there has been a great deal of focus on the right to privacy and the corresponding need to secure personal data. Legislative advancements have not kept up with the exponential growth of the internet, online information sharing, and data collection, and have not sufficiently protected personal data. But in an effort to address and defend their residents' right to privacy, many areas, including Nigeria, have started implementing laws and policies pertaining to data protection.[28]

Since the beginning of the information era, there has been a great deal of focus on the right to privacy and the corresponding need to secure personal data.[29] Since privacy is a multidisciplinary topic, there are many different definitions for it. Many people consider concepts like privacy to include things like anonymity, liberty, autonomy, security, seclusion, and secrecy. While some contend that it is integral to these concepts, others contend that it can be distinguished and is clearly distinct from them.[30] The question of whether privacy should be viewed as a right or only in terms of an individual's one or more interests is likewise intimately tied to the notion of privacy.[31]

3.1. Challenges in Seeking Legal Redress for Breach of Data

Victims of data privacy breaches face numerous challenges when seeking legal redress. The first challenge to be considered is the difficulty in proving harm. When an action for breach of data privacy is brought, the widely known legal maxim ‘he who asserts must prove’ will apply. This maxim is also known as ‘the burden of proof. By virtue of Section 134 of the Evidence Act, the burden of proof in civil cases will be discharged on the balance of

---

[27] Adeyemi Adepetun, ‘Nigeria Suffers 64% Data Breach in Q1, Ranks 32 Globally’ *Guardian.ng* (Nigeria, 24 May 2022) <https://guardian.ng/business-services/nigeria-suffers-64-data-breach-in-q1-ranks-32-globally/> accessed 15 November 2024.

[28] Media Defence, ‘Module 4: Data Privacy and Data Protection’ <https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-4-Data-privacy-and-data-protection.pdf> accessed 8 October 2025.

[29] Informing Science: the International Journal of an Emerging Transdiscipline Volume 19, 2016
Cite as: Pelteret, M. & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organi-
zations. Informing Science: the International Journal of an Emerging Transdiscipline, 19, 277-301. Retrieved fro

[30] Tavani, H. T. (2007b). Philosophical theories of privacy: Implications for an adequate online privacy poli-cy. Metaphilosophy, 38(1), 1–22.

[31] Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In K. E. Himma & H. T. Tavani (Eds.), The handbook of information and computer ethics (pp. 131–164). Hoboken, NJ: John Wiley & Son

probabilities. This simply means that both parties to a civil action will present evidence to the court, and the court will give a judgment based on the strength of the evidence submitted by both parties. This was upheld by the court in *Comfort Sanga v Adamawa State Government & Ors.*[32]

An action for redress of breach of data privacy is a civil action, and as such, the burden of proof will be based on a balance of probabilities. In turn, this means that the party who is claiming breach of data privacy must be able to prove in court that the said breach occurred, and that it caused them harm. While it may be easy to prove that his data privacy was breached, the party alleging breach may find it difficult to prove that this breach caused harm to be done to him. In certain cases where the data accessed illegally was not used maliciously, it will be almost impossible to prove harm, which can lead to the loss of the suit by the injured party. This should not be the case, as a major reason why data privacy exists is to enable individuals to have full authority over who accesses their personal information. The question of whether harm is done to them when their data is accessed illegally negates the protection that data privacy laws are supposed to afford individuals. It also begets certain questions like: are individuals whose data has been accessed illegally supposed to wait for harm to be done to them before they take action? Isn't the law supposed to serve as a preventive measure as well?

Another major challenge that is faced by victims of data privacy while seeking redress is that of jurisdiction. Jurisdiction in this context refers to the authority of a court to hear and determine cases.[33] It is a known fact that many, if not all, social media platforms operate globally. This, therefore, makes cross-border breaches difficult to navigate. A cross-border breach can be said to occur when a social media user who lives in a country other than the country where the social media platform was created and operates primarily has their data breached by the social media platform. In such a case, there is the question of what court has jurisdiction to hear the matter; is it the court in the country of the victim, or the court in the country of the social media platform? Furthermore, it may also prove difficult for the individual whose data privacy has been breached to bring action against the social media platform that breached his data privacy due to the variance in data privacy laws.

[32] NICN/YL/15/2023
[33] Britannica, 'Jurisdiction | Definition, Examples, & Facts' <https://www.britannica.com/topic/jurisdiction> accessed 3 September 2025.

A case study is a Nigerian living in Nigeria who uses the social media platform WhatsApp, and whose data privacy was breached by them. The principal law that governs data privacy is the Nigeria Data Protection Act (NDPA) 2023.[34] In the United States of America, on the other hand, the primary federal law that governs data privacy is the Privacy Act of 1974.[35] The social media platform, WhatsApp, was founded in 2009 in the state of California by Jan Kou and Brian Acton.[36] It is also important to note that California has a comprehensive data privacy law, which is called the California Consumer Privacy Act of 2018.[37] In a scenario such as the one given above, the question of what the applicable law will be is to be considered.

Additionally, whether Nigeria's data protection legal framework is sufficiently developed to support such an action should also be considered. While it is evident that the NDPA 2023 has been improved upon, it is no secret that it remains a far cry from where it ought to be as of 2025. It lacks certain key provisions that will enable Nigerian citizens adequate protection in the case of a data breach. This could also place the injured party in the case study above at a procedural disadvantage in his legal pursuit.

Victims seeking legal redress for a social media data breach also face the challenge of quantifying non-economic damages. When an individual's data is breached, there are certain damages which such person suffers that are not typically economic. Examples of such damages include emotional distress, damage to reputation, fear of identity theft and having sensitive personal information exposed to the general public among others. These damages are different from economic damages like fraudulent charges on a bank account which is easily quantifiable. Therefore, in cases of data breach, victims as well as the courts find it difficult to quantify non-economic damages as they are quite subjective.

4.1. Conclusion and Recommendation

[34] Jumoke Lambo, Chisom Okolie and Opeyemi Adeshina, 'Data Protection Laws and Regulation Nigeria' <https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria> accessed 1 December 2024.
[35] Office of Privacy and Open Government, 'Privacy Laws, Policies and Guidance' <https://www.commerce.gov/opog/privacy/privacy-laws-policies-and-guidance> accessed 1 December 2024.
[36] Pascal Faucon, 'What the History of WhatsApp is Teaching Us?' <https://www.linkedin.com/pulse/what-history-whatsapp-teaching-us-pascal-faucon/> accessed 1 December 2024.
[37] Data Guidance, 'Jurisdictions' <https://www.dataguidance.com/jurisdictions/california> accessed 29 January 2025.

There are a number of challenges that victims of social media data breaches and the courts face when an action for legal redress is brought. This leads to a hindrance of justice; it also causes victims of data breaches to receive inadequate or no compensation for the harm done to them. This study underscored some of these challenges and also proffered solutions to them. This study has highlighted certain challenges faced by victims of data privacy when redress is sought, and it is pertinent to give recommendations that can remedy those challenges.

First, there is a need for the establishment of International standards for jurisdiction and applicable law. It has been established that jurisdiction and applicable law are major challenges faced in social media data breach cases. To solve this, there should be the creation of internationally recognised standards to determine the jurisdiction and applicable law in cases of cross-border data breaches. Second, the elimination of the requirement of proof of harm is important. It is a known general rule that in civil cases, the party bringing the suit must prove that it suffered harm as a result of the other party's action. This should, however, not be the case in data breach cases; it should be enough for the injured party to prove that his data was accessed by the other party without his permission. Therefore, data breach cases should be an exception to the rule of proof of harm.

Third is the need for the establishment of criteria for compensation of non-economic damages. In data breach cases, it is often difficult for the victims and courts to quantify non-economic damages. This, therefore, sometimes leads to victims receiving inadequate compensation for the harm they suffered. As such, there should be a set of criteria for determining compensation for non-economic damages.