

Data Protection and Breach of Privacy: An Analysis of the Legal Regime for Prevention and Punitive Measures in Nigeria

Ubong Udoh

Postgraduate Researcher, Faculty of Law, Delta State University
Email Address: ubudoh6@gmail.com

Ejiro Kore-Okiti

Lecturer, Faculty of Law, Delta State University, Abraka, Nigeria

doi: <https://doi.org/10.37745/gjplr.2013/vol14n45984>

Published September 06, 2026

Citation: Udoh U., and Kore-Okiti E. (2026) Data Protection and Breach of Privacy: An Analysis of the Legal Regime for Prevention and Punitive Measures in Nigeria, *Global Journal of Politics and Law Research*, 14(4),59-84

Abstract: *The protection of the right to privacy of individuals in Nigeria is a constitutionally and statutorily enshrined right, which attract remedies in cases of unlawful breach. Accordingly, personal information or data such as names, addresses, health status, gender, Bank verification Numbers among others, are pieces of personal data that must not be unduly exposed, shared or sold by data controllers or processors in custody of such data. Using the doctrinal research methodology, this research critically analyzed Nigeria's legal and institutional framework on the protection of data and the punitive measures for incidences of data breaches. Accordingly, this study found that the right to protection of privacy is statutorily protected by laws such as the Constitution of the Federal Republic of Nigeria, 1999 (as amended), the Nigeria Data Protection Act and other ancillary legislations. Arising from analysis, this research found that Nigeria's current legal framework adequately provides for the protection of data but however lags greatly in the aspect of monitoring, enforcement and implementation. As part of its recommendations, it was suggested that more resources and manpower are needed by the Nigeria Data Protection Commission and allied agencies to pursue enforcement of the law through the registration of more data controllers, and data protection officers as well as in carrying out wider sensitization for individuals and corporate bodies on the rights of data subjects and the statutory obligations of those in charge of personal data of others. The research contributed to knowledge by showcasing the challenges in the aspect of monitoring, enforcement and implementation of the Nigeria Data Protection Act, 2023.*

Keywords: data protection, breach of privacy, legal regime, prevention, punitive, Nigeria

INTRODUCTION

Privacy forms one of the essential barrier preventing absolute state control and dominance.¹The recent substantive legislation on data protection, such as the new Data Protection Act 2023, specifies basic standards governing the gathering, use, and disclosure of individuals' personal data in order to safeguard their human rights including rights to privacy and freedom of speech. The goal of these legislation is to ensure that personal data is used appropriately rather than to outright forbid its processing, which may be virtually unachievable in today's globalized society, especially considering the ubiquitous nature of the internet.²

As long as it is done in a way that respects people's rights, personal data can be gathered and used.³ In this situation, personal data may be freely used for a variety of reasons as long as the individual subject of the data has considerable control over its collection and use. Therefore, data privacy laws fundamentally shield people from being victims of data misuse which has significant impact on the actualization of their human rights.⁴

In the context of this study, a data breach occurs when private, protected, or sensitive information is copied, communicated, viewed, taken, altered, or used by someone who has no right to do so.⁵ The most common means of data breach over the internet includes hacking, malware, phishing and human error.⁶ Even while legislative attempts are admirable, numerous individuals are still vulnerable to hazards including exploitation and misuse of their personal information as a result of challenges such as low level of awareness of these frameworks or poor enforcement capacities of the relevant institutions.⁷

The issue of safeguarding data spans the globe and raises concerns among diverse stakeholders. It remains persistently under siege from governments and corporate bodies that gather and wield personal information of internet users with little regard for individual rights.⁸ The widespread expansion of personal data has its merits, yet it opens individuals to specific vulnerabilities, such

¹N.Danjuma, 'Examining the Legal Framework for Data Protection in Nigeria viz a viz the Exercise of Human Rights on the Internet' *Benue State University Journal*(2023) 12(1), 138-154
<<https://www.bsum.edu.ng/journals/law/vol12n1/files/11.pdf>> accessed 18 June 2026.

² Ibid

³K. Michael et al, 'Privacy, Data rights and Cybersecurity: Technology for good in the Achievement of Sustainable Development Goals in 2019' (IEEE International Symposium on Technology and Society (ISTAS) held on 15 November 2019, 1-13). IEEE.

⁴L.A. Abdulrauf and A. Daibu, ' New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension Between Traditional and Modern Conceptions' *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*(2016) (7).

⁵Ibid.

⁶Ibid.

⁷Ibid.

⁸(n. 1).

as heightened transparency and susceptibility to various transgressions by both state, corporate actors or even perpetrators of criminal activities.⁹ Instances include the misuse of people's data for purposes beyond their original intent, as well as the exposure to risks stemming from insufficient security measures for lawfully collected information.¹⁰

This unchecked handling of personal data might further amplify the asymmetry in information and influence between citizens and these entities, be they governmental or corporate. The increased need for personal data in the globalized and digital era has given rise to all of these problems.¹¹ Consequently, this study seeks to look into the existing legal framework on data protection to determine whether these incidences are allowed, and if they are not, what duties does the law provide for data processors and the existing punitive measures that exist to curb these incidences. This study shall also look into the existing regulatory bodies and their roles in the regulation of data managers in Nigeria and the extent of their powers. In recent times also, the Nigerian judicial system has been developed to recognize the breach of data privacy as a civil wrong against individuals and in deserving circumstances, a number of claims arising from these breaches have been successful. This study shall therefore, also look at individual remedies for breach of data privacy in Nigeria.

Conceptual Clarification

Data

Data generally refers to characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.¹²

Under the Nigeria Data Protection Act, any information relating to a person who can be identified or is identifiable, either directly or indirectly, by reference to an identifier like a name, an identification number, location information, an online identifier, or one or more factors particular to that person's physical, physiological, genetic, psychological, cultural, social, or economic identity is considered personal data.¹³

What constitutes personal data is a broad concept but it covers information that relates to individuals such as one's name, address or health records. However, sometimes it is not clear if

⁹ Ibid.

¹⁰ (n.4).

¹¹ Ibid.

¹² Section 1.3 of the National Information Technology Development Agency Data Protection Regulation, 2019. (The acronym 'NITDA' shall hereinafter be used to refer to the Nigeria Data Protection Regulation).

¹³ Section 65 of the Nigeria Data Protection Act, 2023 (hereinafter referred to as the DPA, 2023).; NS. Danjuma, 'Examining the Legal Framework for Data Protection in Nigeria viz a viz the Exercise of Human Rights on the Internet' *Benue State University Law Journal*, (2023) 12(1), 138-154 <<https://www.bsum.edu.ng/journals/law/vol12n1/files/11.pdf>> accessed 18 June 2026.

the data is in fact personal data and in such a situation, a case by case assessment must be made as to whether the data could be deemed personal data or not.¹⁴

Database

Database means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type databases.¹⁵

A database is also defined as information that's set up for easy access, management and updating. Computer databases typically store aggregations of data records or files that contain information such as sales transactions, customer data, financials and product information.¹⁶Databases are used for storing, maintaining and accessing any sort of data. They collect information on people, places or things.¹⁷

Data Subject

A data subject is a term in privacy law that refers to individuals that can be identified using specific data such as location details, national ID numbers, ethnicity, race, purchase history, credit card information, IP addresses, and more.¹⁸ Data subjects refer to collecting and processing personally identifiable information — where entries in large data sets can be tied back to specific individuals.¹⁹

The Nigeria Data Protection Act defines data subject as ‘an individual to whom personal data relates.’²⁰A Data Subject is the identifiable person who is identified directly or indirectly with reference to an identification number or other factors specific to his/her physical, physiological, mental, economic, cultural or social identity.²¹

Breach of Privacy/ Data Breach

Privacy generally refers to the state of being apart from other people or concealed from their view; solitude; seclusion.²² It is the state of being free from unwanted or undue intrusion or disturbance

¹⁴ Data Protection Commission, ‘What is Personal Data?’ <<https://www.dataprotection.ie/en/faqs/general/what-personal-data>> accessed 18 June 2026.

¹⁵Section 1.3 NITDA, 2019.

¹⁶S. Alexander, B. Lutkevich & A. Hughes, ‘What is a database (DB)? Definition from Techtarget’ <<https://www.techtarget.com/searchdatamanagement/definition/database>> accessed 18 June 2026.

¹⁷Ibid.

¹⁸‘Data Subject: Definition, Meaning and Applicability’ <<https://www.enzuzo.com/privacy/data-subject-meaning>> accessed 18 June 2026.

¹⁹Ibid.

²⁰Section 65 NDPA, 2023.

²¹ Section 1.3 NITDA Regulation, 2019; (n.1).

²² ‘Privacy: Definition & Meaning’ (Dictionary.com) <<https://www.dictionary.com/browse/privacy>> accessed 18 June 2026.

in one's private life or affairs; freedom to be let alone: invasion of privacy.²³ Privacy is a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination.²⁴

Generally speaking, privacy includes the right; to be free from interference and intrusion; to associate freely with whom you want, and to be able to control who can see or use information about you. Also, there are different ways to look at privacy, such as: physical privacy,²⁵ surveillance²⁶ or information privacy.²⁷

From the analysis of what 'privacy' means, a privacy breach could be defined as the improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information.²⁸ Privacy breaches may occur because of innocent mistakes or intentional actions by public service employees; third-party service providers acting on behalf of federal institutions; outside parties who have malicious intent other internal or external parties.²⁹

Consequently, data breach could be seen as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where; a person other than an authorized user accesses or potentially accesses data or an authorized user accesses data for an other than authorized purpose.³⁰

Data Processor/ Data Controller

Data controllers are persons or organisations that collect personal data and decide how and what these data will be used for example; Facebook, Banks, Telcos, Twitter, etcetera.³¹ Data processors on the other hand, use, analyse, compute and transfer these data on the instructions of the

²³ Ibid.

²⁴ 'What is Privacy? (OAIC) <<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-privacy#:~:text=Privacy%20is%20a%20fundamental%20human,free%20from%20interference%20and%20intrusion>> accessed 18 June 2026.

²⁵ for instance, being frisked at airport security or giving a bodily sample for medical reasons).

²⁶ where one's identity cannot be proved or information is not recorded.

²⁷ (n.24); Information privacy is about promoting the protection of information that says who we are, what we do and what we believe.

²⁸ 'Identifying a Privacy Breach: Definitions and Scenarios' <<https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/privacy-policies-guidance/breach-management/phase-1/definitions-scenarios.html>> accessed 18 June 2026.

²⁹ Ibid.

³⁰ CSRC, 'Privacy Breach – Glossary' <https://csrc.nist.gov/glossary/term/privacy_breach#:~:text=Definitions%3A,an%20other%20than%20authorized%20purpose> accessed 18 June 2026.

³¹ F.Ololuo, 'NDPR? Data Privacy for Nigerian Businesses' <<https://uubo.org/wp-content/uploads/2022/08/ndpr-data-privacy-for-nigerian-businesses.pdf>> accessed 18 June 2026.

controllers. Controllers and processors could be the same or different entities. Many fintech companies and other start-ups are both data controllers and processors, for example, Paystack.³²

Section 65 of the Nigerian Data Protection Act defines a data controller as "an individual, private entity, public commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data". The Act also defines a data processor as, an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor.³³

Data Protection/Data Privacy

The phrases "data privacy" and "data protection" are occasionally used interchangeably.³⁴ There are some distinctions despite the fact there are certain shared characteristics.³⁵ The right of a person to be free from unauthorized observation might be referred to as data privacy. On the other hand, data protection is the practice of safeguarding sensitive information from data loss and corruption. Its goal is to protect data and ensure its availability and compliance with regulatory requirements.³⁶

Analysis of Peculiar Incidences of the Use of Data and Breach of Privacy

With the advent of digital technology, use of social media and even the reliance on e-commerce for trading, the likelihood of undue exposure of data and breach of privacy of data subjects has grown sporadically, with these breaches manifesting in different forms and means. This section of the study shall be considering some of the incidences wherein data breaches occur in Nigeria.

Digital Lending Firms and the Violation of Privacy of Defaulting Debtors

Prior to the introduction of digital money loaning agencies, people in need of credit facilities had to borrow money either from close friends, acquaintances, cooperative societies or financial institutions such as commercial and microfinance banks. In most of these cases, especially as it pertains to banks and money lenders, collaterals are requested before these loans are granted subject however to the verification of the title of the collateral used. These processes were mostly laborious and time consuming and could not be reliable for urgent use. Then came the emergence of fintech companies including those that specialized in granting loans without collateral and delay.

However, what seemed as an advantage to borrowers turned to a sour and embarrassing experience as many debtors who could not meet up with their repayment obligations were exposed to different forms of harassments, verbal abuse and ultimately, the exposure of their data (their names, pictures

³² Ibid.

³³ Section 65 NDPA, 2023.

³⁴(n.1).

³⁵Ibid.

³⁶What is Data Protection? (IBM) <<https://www.ibm.com/think/topics/data-protection>>accessed 18 June 2026.

and amount owed)³⁷ to their contacts and the general public.³⁸ These incidences were rife in Nigeria until the Federal Competition and Consumer Protection Commission (FCCPC) stepped in to stem the tide, albeit it is yet to completely eradicate this practice.³⁹

Incidences of Breach of Privacy through the Use of Social Media Platforms

Another form of data privacy breach that has become common in Nigeria in recent time, is the use of social media platforms to expose or leak personal data of other persons including private messages, photos, videos and even voice recordings. This issue has become rampant with even vendors resorting to using social media platforms to expose those who allegedly owe them, while other social media users share these photos and messages on their respective pages and groups thereby causing irreparable damage to the affected individual or company particularly where these allegations are untrue.

With the introduction of the Cybercrimes Act, affected individuals may seek the help of law enforcement agencies or institute civil proceedings in seeking redress against those suspected of breaching their privacy. Beyond the abuse of personal data by individuals, several companies are also guilty of breaching the data privacy and unauthorized cross-border transfer of data of data subjects in Nigeria.

Breach of Privacy via the release of mug shots and media parade of alleged criminals by security agencies

As the modern trend reveals, releasing and ‘advertising’ the mug shot of suspects on media and social media platforms as well as parading of suspect on camera is now a norm by the Nigerian Police Force (NPF), Economic and Financial Crimes Commission (EFCC) and other law enforcement agencies as way of flexing their efficiency to their appointers and the public.⁴⁰ Parading of suspects is done by law enforcement agencies such as the police which is the most visible part of the criminal justice system⁴¹ in respect of several forms of offences, from serious offences of felony to misdemeanor, and simple offences. As recent as April 2024, several

³⁷ Hannah Johnson, ‘Loan app sparks outrage by posting 87 debtors’ photos online’ (PUNCH: 5th January 2025) <<https://punchng.com/loan-app-sparks-outrage-by-posting-87-debtors-photos-online/>> accessed 18 June 2026.

³⁸Ebenezer Amadi, ‘Digital Lending Apps and the Violation of Privacy Rights of Borrowers: A Growing Concern in Nigeria’ <<https://thenigerialawyer.com/digital-lending-apps-and-the-violation-of-privacy-rights-of-borrowers-a-growing-concern-in-nigeria/>> accessed 18 June 2026.

³⁹‘DIGITAL LENDING: FCCPC TACKLES ABUSES, ISSUES LANDMARK REGULATIONS - Federal Competition & Consumer Protection Commission’ FCCPC <<https://fccpc.gov.ng/digital-lending-fccpc-tackles-abuses-issues-landmark-regulations/>> accessed 18 June 2026.

⁴⁰Amos, ‘Legality of Media Publication of Mugshot and Public Parading of Suspects in Nigeria ‘ The Guardian (May, 7 2024) <<https://guardian.ng/features/legality-of-media-publication-of-mugshot-and-public-parading-of-suspects-in-nigeria/>> accessed 18 June 2026.

⁴¹ K. Okiti and T. Avwomakpa, ‘The Nigerian Criminal Justice System: History, Law and the Operators’ EBSU Law Journal (2020) 11(1),73-86.

individuals were prejudicially paraded as criminals for the offence of failing to use the pedestrian bridge with media coverage.⁴²

Whether a suspect of crime has a reasonable and legitimate expectation of privacy is a question of fact which is determined by the court through concrete evaluation of the circumstances.⁴³ There is now a uniform general practice by state investigatory bodies not to identify those under criminal investigation prior to charge, the rationale for which was the risk of unfair damage to reputation, together with other damage, and which applied regardless of the nature of the suspected offence or the public characteristics of the suspect.⁴⁴ Consequently, as the law stands, in the absence of any counteracting factor, every suspect of crime is entitled to a reasonable and legitimate expectation of privacy prior to being charged.⁴⁵

Amongst other factors, public identification and media parade, transcends the infringement of the suspect's right to privacy and bruises a great deal against his right to dignity.⁴⁶ For instance, some suspects are subjected to inhumane and bad conditions, foisted to confess to crimes without prior consultation with counsel and often times cruelly shackled and rendered shirtless while sitting on bare grounds with standby media coverage by the Nigerian Police.⁴⁷ In another sense, publicity may create and thrust the suspects life in danger, leading to vulnerable and deadly attacks on the suspect whose guilt is yet to be substantiated. In all of these instances usually, publicity is certainly not in the interest of the state or the accused. Hence, the need for publicity of this sort to be brought to an end.⁴⁸

A major excuse furnished by security agencies in Nigeria for undertaking media parade of suspects or releasing their mugshots, is what they consider to be its deterrent value against the commission of crime, curbing criminal tendencies and aiding as a notice to the public to provide vital information at their disposal that may assist in the prosecution of a criminal suspect by the police.⁴⁹ However, it must be observed that media parade of suspects of crime has had little or no effect in curbing criminal activities which are as a result of the high unemployment and poverty rates in the Nigerian society.⁵⁰

⁴²Ibid.

⁴³WI. Nnorom, 'Rights Against Media Parade and Public Identification of Criminal Suspects: The Privacy Rage' *SSRN Journal*(2023)

<https://www.researchgate.net/publication/373852850_Rights_Against_Media_Parade_and_Public_Identification_of_Criminal_Suspects_The_Privacy_Rage> accessed 16 June 2026.

⁴⁴ Ibid; See the case of *ZXC v. Bloomberg LP* (2022) WLR (D) 96.

⁴⁵ Ibid; *ERY v. Associated Newspapers Limited* (2017) EMLR 9.

⁴⁶ Ibid; Article 5 of the African Charter for Human and People's Rights, 1981, provides that every individual shall have the right to the respect of the dignity inherent in a human being and to the recognition of his legal status.

⁴⁷Nnorom (n.43).

⁴⁸Ibid.

⁴⁹Ibid.

⁵⁰ Ibid.

Over the years a number of laws and Judicial pronouncements have been made affirming the unconstitutionality of media parade or release of mugshots of suspects to the public. For instance, section 36(5) Constitution of the Federal Republic of Nigeria 1999 (amended) states that, ‘every person who is charged with a criminal offence shall be presumed to be innocent until he is proved guilty’.

In addition, Section 9(a) of the amended administration of criminal justice law of Lagos state,⁵¹ provides that the police shall refrain from parading any suspect before the media. Furthermore, the anti-torture Act under section 2(xi) stipulates that torture includes parading a person to the public against his/her will. In the case of *Ndukwem Chiziri Nice v. AGF & Anor*⁵², the Court condemned the media parade of suspects and held that it is a fundamental breach of the constitutional rights of suspects.

The Use of Artificial Intelligence (AI) and its Effect on Data Breach/Copyright Infringement

The introduction of artificial intelligence (AI) has come with its advantages and disadvantages. Some of its disadvantages, unfortunately is the fact that in the process of its development, it relies on existing words, texts, images and even videos, most of which are copyrighted and private data of different individuals. In the American case of *De La Torre v. LinkedIn Corp.*⁵³, an action was filed by a LinkedIn premium user who discovered that her Inmail messages and private information was disclosed to third parties to train generative artificial intelligence models around September, 2024.⁵⁴

While issues of AI such as ChatGPT and OpenAI relying on existing images to train their machine usually raises issues of copyright infringement for copyrighted works, these companies responsible for developing such AI models, generally rely on the principle of ‘fair use’ as a defense.⁵⁵ It is however a different ballgame, where private information of users of certain platforms are adapted or transferred for training of AI models. Such use of private information without the consent of the data subject totally amounts to a breach of privacy and the concerned data subject is entitled to seek redress.

Legal and Institutional Framework on Data Protection in Nigeria

Although there are several laws and regulations which generally make provisions on data protection in Nigeria, for the purpose of this research, attention shall be paid to a select few laws with significant provisions on the subject matter such as the 1999 Constitution, the Nigeria Data

⁵¹Administration of Criminal Justice Law Lagos State, 2021.

⁵²*Ndukwem Chiziri Nice v. AGF & Anor*⁵² (2007) CHR218 at 232.

⁵³ *De La Torre v. LinkedIn Corp*, U S District Court, Northern District of California, No. 25-00709

⁵⁴Chioma Unini, ‘LinkedIn Sued Over Private Data – Users say messages used for AI without Permission’ (The Nigerian Lawyer – January, 22 2025) <https://thenigerialawyer.com/linkedin-sued-over-private-data-users-say-messages-used-for-ai-without-permission/#google_vignette> accessed 16 June 2026.

⁵⁵ Tori Noble, ‘Copyright and AI: the Cases and the Consequences’ (EFF : February 19, 2025) <<https://www.eff.org/deeplinks/2025/02/copyright-and-ai-cases-and-consequences>> accessed 16 June 2026.

Protection Act (NDPA) as well as the NDPA-General Application and Implementation Directives. The institutions currently responsible for the regulation of data and protection of customers (data subjects), which are mainly the Nigeria Data Protection Commission (NDPC) and the Federal Consumer Competition Protection Commission (FCCPC) will also be evaluated in this research.

Constitution of the Federal Republic of Nigeria

The Constitution of the Federal Republic of Nigeria 1999 (as amended) under section 37 provides for the right to private and family life of its citizens. The section stipulates, that ‘the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected’.

In this modern age of technology and rampant use of social media platforms, the current trend most times where there are disputes between individuals or between individuals and corporations, is that several private information, such as messages, photos, videos or documents are leaked or shared online without the permission of its owner, with the aim, most times, being to embarrass, discriminate and shame the affected party. Beyond the fact that these acts are criminalized under the relevant criminal laws in Nigeria, they also infringe on the Constitutional right to freedom from discrimination as protected under section 42 of the Constitution.

Over the years, a number of actions have been successfully been instituted with regard to the protection of the constitutional right of privacy in Nigeria. In the case of *Bi-Courtney Aviation Services Ltd v. Kelani*,⁵⁶ the Court of Appeal held that the unauthorized use of a person’s photograph for advertisement was a breach of the person’s right to privacy. For better understanding, the facts of the case are highlighted below.

FACTS:

The Respondent's case at the trial Court, was that the Appellant, an aviation management services Company, and who were the concessioners of the Murtala Muhammad Airport (Terminal 2) Lagos, had taken and caused to be published, the Respondent's photographs for the purpose of its business advertisement for its commercial benefit, the act was said to have been done while the Respondent travelled through the MMIA (terminal 2) sometime in 2015, without the knowledge of the Respondent, nor his consent sought and obtained.

The Appellant denied the Respondent's claim in the statement of defence dated 5/04/16 and prayed the trial Court that same be discountenanced. The trial judge, in a considered judgment delivered on 29th June, 2018, granted the reliefs sought by the Respondent. The trial Court delivered its judgment in favour of the Respondent, while the general damages was assessed and granted in the sum of N25,000,000.00 in favour of the Respondent. Aggrieved by the decision of the trial Court, the Appellant appealed to the Court of Appeal.

⁵⁶*Bi-Courtney Aviation Services Ltd v. Kelani* (2021) LPELR-56365(CA).

In determining the legal question, - ‘Whether the unauthorized use of a picture, photograph, drawing or film of a person is a breach of right to privacy?’, the Court of Appeal⁵⁷ held thus;

A picture of a person mirrors his own image which is personal to him. It is a clone of an individual. For a business concern to take a picture of somebody, for pecuniary interest, without his consent or authorization, constitutes a serious erosion of right of privacy of that citizen. The appellant's procurement and public display of the respondent's photograph for commercial needs, without his endorsement, is an unwarranted infraction of the respondent's inviolable right to private life as, deeply, ingrained in Section 37 of the Constitution, as amended.

In order to ensure that the constitutional rights of individuals in the country are protected, the Constitution provides that any person who alleges that any provision of Chapter IV has been, is being or likely to be contravened in any State in relation to such an individual, he/she may apply to a High Court in that State for redress.⁵⁸

In this light, where an individual is being threatened that his personal/confidential information would be leaked online, he or she can swiftly apply to protect his right to privacy through the institution of a suit for the protection of his fundamental rights. The Fundamental Rights Enforcement Procedure Rules, 2009 was introduced by the Chief Justice of Nigeria in pursuance to the provision of section 46(3) of the Constitution to enable individuals easily access the court for the protection of their fundamental rights

Furthermore, the Nigeria Data Protection Act, which is the substantive National Legislation on data protection in the country specifically provides that any person who feels his rights has been infringed may bring a civil action against the defaulting party. Section 51 of the Act provides that; ‘data subject who suffers injury, loss, or harm as a result of violation of this Act by a data controller or data processor, may recover damages from such data controller or data processor in civil proceedings’.

Nigeria Data Protection Act

The Nigeria Data Protection Act (NDPA) was introduced in 2023, after several attempts in the past to produce a substantive legislation to regulate data protection in Nigeria. As part of its objectives, the Act seeks to safeguard the fundamental rights and freedoms, and interests of data subjects in line with the provisions of the Constitution of the Federal Republic of Nigeria, 1999. It also seems to protect data subjects’ rights, and provide means of recourse and remedies, in the event of breach of the data subject’s rights.⁵⁹

⁵⁷ Per Abdullahi Mahmud Bayero, JCA at (Pp 21 - 24 Paras E - A).

⁵⁸ Section 46(1) CFRN 1999.

⁵⁹Section 1 of the Nigeria Data Protection Act, 2023 (hereinafter referred by the acronym ‘NDPA’).

Accordingly, the NDPA applies in any of the following instances. They include; where the data controller or processor is domiciled, resident or operating in Nigeria; processing of personal data occurs within Nigeria or the data controller or data processor is not domiciled, resident or operating in Nigeria, but is processing personal data of a data subject in Nigeria.⁶⁰ The NDPA shall however not be applicable where the processing of personal data carried out by one or more persons is solely for personal or household purposes as long as such purposes do not infringe on the fundamental rights to privacy of a data subject in Nigeria.⁶¹

Furthermore, the NDPA⁶² provides that in certain other instances, the requirements under part V shall not be applicable to a data processor or data controller if the processing of personal data is carried out in the following circumstances;⁶³

- (a) Carried out by a competent authority for the purposes of the prevention, investigation, detection, prosecution or adjudication of a criminal offence or the execution of a criminal of a criminal penalty, in accordance with any applicable law;
- (b) Carried out by a competent authority for the purposes of prevention or control of a national public health emergency;
- (c) Carried out by a competent authority, as is necessary for national security;
- (d) In respect of publication in the public interest, for journalism, educational, artistic and literary purposes to the extent that such obligations and rights are incompatible with such purposes; or
- (e) Necessary for the establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

In order to extensively regulate issues relating to data processing within the country and also enforce its provisions, the NDPA provided for the establishment of the Nigeria Data Protection Commission, which is a body corporate, having its head office at the federal Capital Territory, Abuja, and other offices in any other parts of Nigeria.⁶⁴ The powers and functions of the Commission are spelt out under sections 5 and 6 of the Act, and it is to be headed by a Chairman, and shall also have a governing council.⁶⁵ The law also provides that the commission shall be independent in the performance of its functions.⁶⁶

Just as is applicable in other regional and international instruments earlier reviewed, the principles of data processing seem to be uniformed with what is provided under section 24 of the Act. The

⁶⁰ Section 2 NDPA 2023.

⁶¹ Section 3(1) Ibid.

⁶² Section 3(2) Ibid.

⁶³ These data controllers and processors are however bound to observe the provisions of sections 24, 25, 32 and 40 under part V of the NDPA, 2023.

⁶⁴ Section 4 NDPA 2023.

⁶⁵ Section 8 and 9 Ibid.

⁶⁶ Section 7 Ibid.

NDPA under section 34 provides that a data subject has the right to obtain from a data controller, without constraint or unreasonable delay;⁶⁷ a confirmation whether a data controller or processor is storing or processing his/her personal data; a copy of his/her personal data in an electronic format; the correction or deletion of his/her personal data if it is inaccurate, out of date, incomplete or misleading; erasure of a data subject's personal data without undue delay and restriction of personal data processing pending resolution of a request, objection by the Data subject or exercise, establishment or defense of a legal claim. The right of a data subject also extends to the right to lodge a complaint with the commission.⁶⁸ Section 35 of the Act also provides that a data subject shall have the right to withdraw his consent at any time with regard to the processing of his personal data. A Data subject shall also have the right to object to the processing of his or her personal data⁶⁹ and shall also not be subject to a decision based solely on automated processing of personal data.⁷⁰

An important provision of the Act, is its provision on the lawful basis of processing personal data. Accordingly, the Act provides that data processing shall be lawful where the data subject has given consent and not withdrawn same consent for the specific purpose the data was sought for.⁷¹ It further provides that it shall be lawful to process personal data if the processing is necessary for the following;⁷²

- i. For the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract,
- ii. For compliance with a legal obligation to which the data controller or data processor is subject,
- iii. To protect the vital interest of the data subject or another person,
- iv. For the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor, or
- v. For the purposes of the legitimate interests pursued by the Data controller or data processor, or by third party to whom the data is disclosed.

The Act however provides that it shall not be lawful to process personal data where it overrides the fundamental rights, freedoms and interests of the data subject; is incompatible with other lawful with other lawful basis identified above or the data subject would not have a reasonable expectation that his or her personal data would be processed in the manner envisaged.⁷³ A data processor or

⁶⁷ Section 34(1) Ibid.

⁶⁸ Section 1(a) (vi) NDPA 2023. Section 34(2) provides that a data controller shall erase personal data without undue delay where it is no longer needed in relation to the purpose for which it was first obtained or they have no other lawful basis to retain same again.

⁶⁹ Section 36 NDPA 2023.

⁷⁰ Section 37 Ibid.

⁷¹ Section 25(1)(a) Ibid.

⁷² Section 25(1) (b) Ibid.

⁷³Section 25(2) Ibid.

data controller bears the burden of proving that a data subject provided consent before they proceeded to process his/her data. The data processor or data controller shall also ensure that certain information are provided to a data subject about its identity before collecting personal data of the data subject.⁷⁴ Such information include; its residence/ place of business, means of communication, lawful basis for seeking such data, retention period of the data, recipients of the collected data among others.⁷⁵

Furthermore, a data processor or data controller is mandated to carry out an extensive data privacy impact assessment where the processing of personal data may likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purpose.⁷⁶ The data controller may also consult the commission prior to the processing, if notwithstanding the measures envisaged, the data protection impact assessment indicates that the processing of the data would result in a high risk to the rights and freedom of a data subject.⁷⁷

Also, the Act mandates that data controllers and data processors must implement appropriate technical and organizational measures to ensure security, integrity and confidentiality of personal data in their possession or control, including protections against accidental or unlawful destruction, loss, misuse, alteration, unauthorized disclosure, or access.⁷⁸ In any instance where the personal data of a data subject is breached, a data processor in control or possession of such data must provide full details of the breach to a data processor or controller that engaged it, notify the commission within 72 hours of becoming aware of the breach.⁷⁹ Where the personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller or processor must immediately inform the data subject, and advice on what measures could be taken on the part of the data subject to resolve the breach. Where however, it is difficult to directly reach the data subject(s), or it would be too expensive, the data controller or processor may proceed to make a public communication in one or more widely used media sources such that the data subject is likely to be informed.⁸⁰

More importantly, the Act provides that a data controller or data processor shall not process sensitive personal data of a data subject except where; consent has been obtained and not withdrawn; processing is necessary to perform the controller's obligations or exercise rights of the data subject under employment or security laws; necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent etcetera.⁸¹

⁷⁴Section 26 NDPA 2023.

⁷⁵ Section 27 Ibid.

⁷⁶Section 28(1) Ibid.

⁷⁷ Section 28(2) Ibid.

⁷⁸ Section 39 Ibid.

⁷⁹ Section 40(1) (2) Ibid.

⁸⁰ Section 40(3) Ibid.

⁸¹ Section 30 NDPA 2023.

Where a data subject is a child, or a person lacking legal capacity to consent, the Act requires a data controller to obtain the consent of the parent or legal guardian, as applicable.⁸² The Act does not expressly define who a child is, but stipulates that a child has the meaning ascribed in the child's right Act.⁸³ Part X and XI of the Act deals with provisions on enforcement and legal proceedings of matters addressed under the Act. These parts will be elaborately considered in subsequent aspects of this study.

Nigeria Data Protection Act General Application and Implementation Directive, 2025

On the 20th of March, 2025, the Nigeria Data Protection Commission (NDPC) introduced the 'Nigeria Data Protection Act General Application and Implementation Directive'(GAID) with the aim of providing clarity and practical guidance on the implementation of the Act.⁸⁴ Accordingly, the introduction of this directive, effectively repealed the Nigeria Data Protection Regulation 2019.⁸⁵ It is however provided that in the event of a conflict between the Act and the GAID, the Act shall prevail.⁸⁶

Article 6 of the GAID, provides that an individual who processes data solely for personal or household purposes shall respect the privacy of a data subject and shall be held accountable for the conduct which puts the privacy of a data subject at risk.⁸⁷ Some of these conducts include sharing or transferring personal data to any person or platform; lack of duty of care in handling any device which stores personal data etcetera.⁸⁸ Article 7 of the directive enumerates the compliance measures that must be followed by data controllers and processors. On addition, data controllers or data processors of major importance, as designated by the Commission, are mandated to register with the commission in accordance with the guidance notice issued by the commission.⁸⁹ The directive further requires these major data controllers and processors to file compliance audit returns with the commission on a yearly basis. The template of the compliance audit returns is listed under schedule two of the GAID.⁹⁰

Without prejudice to the provisions of the Nigeria Data Protection Act, the directive provides that consent is required in the following instances;⁹¹

- a) For any direct marketing activity;

⁸²Section 31 Ibid.

⁸³ Section 65 Ibid.

⁸⁴ This directive was introduced pursuant to section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) and Sections 1(a), 6(c), 61 and 62 of the Nigeria Data Protection Act 2023.

⁸⁵G. Elias, 'Highlights of The Nigeria Data Protection Act General Application and Implementation Directive, 2025' <<https://share.google/wf9E6Yt6ipzqPIU1T>> accessed 16 June 2026.

⁸⁶ See section 63 of the NDPA and the Article 3(2) of the GAID.

⁸⁷ Article 6(1) GAID.

⁸⁸ Article 6(2) GAID.

⁸⁹Article 9 Ibid; This guidance notice is reproduced under schedule 7 of the GAID.

⁹⁰ Article 10 Ibid.

⁹¹ Article 18 Ibid.

- b) For the processing of sensitive personal data;
- c) For further processing that is incompatible with the original purpose of processing;
- d) For the processing of the personal data of a child;
- e) Before personal data may be transferred to a country in respect of which the commission has not made an adequacy decision; and
- f) Before the data controller makes a decision based solely on automated processing which produces legal effects concerning or significantly affecting the data subject.⁹²

Furthermore, article 19 stipulates that operation of cookies and other tracking tools shall comply with the principles of data protection under section 24 of the NDPA, and except as otherwise provided under the GAID, the use of cookies on a website or other digital platforms requires consent which shall be freely given, informed and specific.⁹³

The GAID reaffirms the provision of section 28 of the NDPA, that a data privacy impact assessment shall be necessary when data processing may likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes.⁹⁴ In addition, a data controller or data processor is mandated to put in place, appropriate technical and organizational measures to prevent the use of its platform, facility, network from being used to breach the privacy of a data subject.⁹⁵

The directives also introduce new rights for data subjects. These rights include the rights to data portability,⁹⁶ exercise of right to be forgotten (having one's data erased),⁹⁷ and the right to lodge a complaint with the commission.⁹⁸ In addition, the directive provides that a data subject has the right to seek redress for the violation of his or her data privacy rights in line with section 46 of the 1999 Constitution at the closest federal or state high court in line with settled precedents of the Supreme Court of Nigeria and extant Fundamental Rights Enforcement Procedure Rules.⁹⁹

Analysis of the Institutional Framework on Data Protection in Nigeria

Nigeria Data Protection Commission

The Nigeria Data Protection Commission was established pursuant to the provisions of the Nigeria Data Protection Act,¹⁰⁰ as a body corporate, with perpetual succession, a common seal with powers

⁹² A compliance audit returns (CAR) shall state whether or not the data controller or data processor relies on consent to carry out data processing in any of the activities itemized in sub-article 1 of Article 18.

⁹³ Article 19(1)(2) and (3) of the Ibid.

⁹⁴ Article 28 Ibid.

⁹⁵ Article 32 GAID.

⁹⁶ Article 37 Ibid.

⁹⁷ Article 38 Ibid.

⁹⁸ Article 39 Ibid.

⁹⁹ Article 47 Ibid.

¹⁰⁰ Section 4(1) of the NDPA (2023).

to sue and also be sued.¹⁰¹ The commission is also granted power to acquire, hold and dispose of its property,¹⁰² with its head office at Abuja and other branch offices across the nation.¹⁰³ The commission is headed by a national commissioner who is appointed by the President upon the recommendation of the minister.¹⁰⁴ The commissioner holds his/her office for a term of five (5) years and may be re-appointed for another five years.¹⁰⁵ In addition, the Act provides that there shall be a governing council for the commission which shall comprise of a chairman and other members as stipulated thereunder.¹⁰⁶

The functions of the commission are outlined under section 5 of the NDPA, and they include; the regulation of deployment of technological and organizational measures to enhance personal data protection; register data controllers and data processors of major importance and promote awareness of their obligations under the Act; receive complaints relating to violations of the Act or subsidiary legislations made under the Act etcetera.

Furthermore, the powers of the commission under the Act covers the conduction of investigations on violation of the Act, imposition of penalties for violation, issuance of regulations, rules, directives and guidance under the Act etcetera.¹⁰⁷

In furtherance to the powers of the Commission as stated under section 6 of the Act, section 46 and 47 of the Act provides for the steps to be taken by the commission on receiving complaints, carrying out investigations and ensuring compliance by data controllers and data processors. In a situation where a data controller or data processor has violated any provision of the Act, the commission may either, make any appropriate enforcement order, alternatively impose a sanction on them or inform the concerned data controller or processor or a data subject of its decision.¹⁰⁸ Furthermore, an enforcement order or sanction by the commission could include demanding that the data controller or processor pay compensation to the affected data subject; remedy the violation or even pay a penalty or remedial fee.¹⁰⁹ A penalty or remedial fee could range between an amount higher than #2,000,000 or #10,000,00 or 2% of the defaulting data controller or processor's gross revenue in the preceding financial year.¹¹⁰

In addition, section 58 of the Act provides that the commission has the power to arrest, search and seize evidence, where it has evidence of a crime being committed upon applying for an issuance

¹⁰¹ Section 4(2) Ibid.

¹⁰² Section 4(2)(c) Ibid.

¹⁰³Section 4(3)(4) Ibid.

¹⁰⁴ Section 14(1) Ibid.

¹⁰⁵Section 14(4) Ibid.

¹⁰⁶ Sections 8-13 Ibid.

¹⁰⁷ Section 6 Ibid.

¹⁰⁸ Section 48(1) NDPA.

¹⁰⁹ Section 48(2) Ibid.

¹¹⁰ Section 48(3)(4)(5) Ibid.

of warrant, ex-parte from a Judge in Chamber.¹¹¹ As part of its efforts to ensure compliance and punish erring data controllers, it was reported that the commission imposed a fine of ₦555,800.000 on Fidelity Bank in 2024¹¹² on issues bordering on data breach and also investigated companies such as Tiktok and Truecaller for allegations of cross-border data transfer and data breach.¹¹³

Pursuant to its power to issue regulations and directives, the commission in 2025, released the General Application and Implementation Directive (GAID) for the Nigeria Data Protection Act. Consequently, this directive (GAID) formally brought about the inapplicability of the Nigeria Data Protection Regulation 2019 as a legal instrument by the Commission as a legal instrument for regulating data privacy and protection in Nigeria.¹¹⁴ With regards to its power to regulate data processing and transfer as well as the protection of data privacy in the country, the commission has been responsible for this role since its inception and has recorded quite a number of success in monitoring of data processors and controllers as well as the punishment of defaulting bodies in Nigeria.

Federal Competition and Consumer Protection Commission

The Federal Competition and Consumer Protection Act, 2018 is the main statute governing consumer protection and competition regulation in Nigeria. The Act established the Federal Competition and Consumer Protection Commission (FCCPC)¹¹⁵ and the Competition Consumer Protection Tribunal (CCPT) for the development and promotion of fair, efficient and competitive markets in the Nigerian economy to facilitate access by all citizens to safe products and secure the protection of rights for all consumers in Nigeria and for related matters.¹¹⁶

The Commission (FCCPC) enforces compliance with consumer protection laws and other regulations which impact consumer rights including the breach of their data privacy.¹¹⁷

¹¹¹ Section 58 Ibid.

¹¹²Unini Chioma, 'NDPC Fines Fidelity Bank ₦555.8m, Payable Within 14 Days, For Breaching Customer Data Protection' TheNigeriaLawyer (August 21, 2024) <<https://thenigerialawyer.com/ndpc-fines-fidelity-bank-n555-8m-payable-within-14-days-for-breaching-customer-data-protection/>> accessed 16 June 2026.

¹¹³Unini Chioma, 'NDPC Probes TikTok, Truecaller Over Alleged Data Privacy Violations In Nigeria' TheNigeriaLawyer (March 21, 2025) <https://thenigerialawyer.com/ndpc-probes-tiktok-truecaller-over-alleged-data-privacy-violations-in-nigeria/#google_vignette> accessed 16 June 2026.

¹¹⁴ Article 3(3) GAID 2025.

¹¹⁵Section 3 of the FCCPA 2018.

¹¹⁶FCCPA, 'Federal Competition & Consumer Protection Commission' <<https://fccpc.gov.ng/resources-library/fccpa/>> accessed 16 June 2026.

¹¹⁷ Section 148 FCCPC 2018.; A. Alex-Adedipe & E. Best, 'Consumer Protection Regulation in Nigeria: The Role of the Federal Competition and Consumer Protection Commission' (2024) <<https://www.mondaq.com/nigeria/consumer-law/1504638/consumer-protection-regulation-in-nigeria-the-role-of-the-federal-competition-and-consumer-protection-commission>> accessed 16 June 2026.

Another agency that has been at the front row of data protection compliance is the Federal Competition and Consumer Protection Commission. For instance, in order to tackle issues of online loan companies leaking private data of its debtors to the public, the commission introduced the Digital, Electronic, Online, or Non-Traditional Consumer Lending Regulations (DEON Consumer Lending Regulation) 2025, to address longstanding consumer complaints and a variety of issues.¹¹⁸

This landmark regulation, made pursuant to sections 17, 18 and 163 of the Federal Competition and Consumer Protection Act,¹¹⁹ establishes a robust legal framework to register, monitor and sanction all forms of digital and non-traditional lending in Nigeria. Importantly, the regulation prohibits pre-authorized or automatic lending, compel clear and accessible loan terms, ban unethical marketing, and mandate local ownership of at least one service provider for airtime or data lending services.

Under its provisions, all digital lenders must register with the FCCPC within 90 days of commencement. Approval is dependent on meeting consumer protection, data compliance, and transparency standards. Non-compliant operators face sanctions, which may include fines of up to #100 million or 1% of turnover, as well as potential disqualification of directors for up to five years. Since the introduction of this regulation, reports of loan companies harassing or publicly embarrassing its debtors has been reduced to a minimal level.

Furthermore, the FCCPC in collaboration with the NDPC successfully investigated META (parent company of Instagram and Facebook) before proceeding to impose a fine of \$32.8 million in February, 2025. After Meta took the commission to the Federal High Court to challenge their powers to impose such fines, parties were eventually able to reach an amicable resolution and proceeded to adopt terms of settlement, bringing the case to an end.¹²⁰ In another report, the tribunal affirmed the \$220 million fine the FCCPC imposed on social media platform, Whatsapp for data violations and what it described as sharp practices.¹²¹

¹¹⁸FCCPC, 'DIGITAL LENDING: FCCPC TACKLES ABUSES, ISSUES LANDMARK REGULATIONS - Federal Competition & Consumer Protection Commission' <<https://fccpc.gov.ng/digital-lending-fccpc-tackles-abuses-issues-landmark-regulations/>> accessed 16 June 2026.

¹¹⁹2018.

¹²⁰Unini Chioma, "Meta, FG Reach Truce" — Court Adopts Settlement As Facebook, Instagram Owner Ends \$32.8m Data Violation Dispute With Nigeria' TheNigeriaLawyer (November 3, 2025) <<https://thenigerialawyer.com/meta-fg-reach-truce-court-adopts-settlement-as-facebook-instagram-owner-ends-32-8m-data-violation-dispute-with-nigeria/>> accessed 16 June 2026.

¹²¹Unini Chioma, 'Tribunal Upholds FCCPC's \$220m Fine Against Facebook, WhatsApp Over Sharp Practices Against Nigerians' TheNigeriaLawyer (April 25, 2025) <<https://thenigerialawyer.com/tribunal-upholds-fccpcs-220m-fine-against-facebook-whatsapp-over-sharp-practices-against-nigerians/>> accessed 16 June 2026. Whatsapp has since applied to stay the enforcement of the tribunal's decision <<https://thenigerialawyer.com/meta-owned-app-seeks-urgent-stay-of-order-says-tribunal-ruling-misrepresents-its-practices/>> accessed 16 June 2026.

Evaluation of Individual Rights to Protection of their Data and the Remedies Available in Cases of Breach

The main essence of the data protection framework in Nigeria, and all over the world revolves around the need to protect the privacy of data subjects and the regulation of the use of certain types of data. In Nigeria, the legal basis upon which data rights of persons must be legally protected arises from the provisions of the Constitution of the Federal Republic of Nigeria, 1999. Section 37 of the 1999 Constitution of the Federal Republic of Nigeria¹²² protects the fundamental right of a person to private and family life. The implication of this provision is that any person can enforce his/her fundamental right to the protection of his privacy in court.

The NDPA under sections 34-38 also enumerates the different rights of data subjects in Nigeria. Accordingly, section 34 provides that a data subject has the right to obtain from a data controller, without constraint or unreasonable delay;¹²³ a confirmation whether a data controller or processor is storing or processing his/her personal data; a copy of his/her personal data in an electronic format; the correction or deletion of his/her personal data if it is inaccurate, out of date, incomplete or misleading; erasure of a data subject's personal data without undue delay and restriction of personal data processing pending resolution of a request, objection by the Data subject or exercise, establishment or defense of a legal claim.

The right of a data subject also extends to the right to lodge a complaint with the commission.¹²⁴ Section 35 of the Act also provides that a data subject shall have the right to withdraw his consent at any time with regard to the processing of his personal data. A Data subject shall also have the right to object to the processing of his or her personal data¹²⁵ and shall also not be subject to a decision based solely on automated processing of personal data.¹²⁶ In addition to the above, the Act mandates the commission to make regulations which would entitle the data subject to receive personal data from a data controller in a commonly used form and structure and be able to easily transfer such personal data to another data controller of his or her choice without delay.¹²⁷

Beyond a data subject's right to lay complaints to the commission, which would in turn investigate the claims and make a decision, the data subject also has the right to seek civil redress personally. Section 51 of the Act provides as that; 'a data subject, who suffers injury, loss, or harm as a result of a violation of this Act by a data controller or data processor, may recover damages from such data controller or data processor in civil proceedings'.

¹²² Constitution of the Federal Republic of Nigeria, 1999 (as amended).

¹²³ Section 34(1) NDPA 2023.

¹²⁴ Section 1(a) (vi) NDPA 2023. Section 34(2) provides that a data controller shall erase personal data without undue delay where it is no longer needed in relation to the purpose for which it was first obtained or they have no other lawful basis to retain same again.

¹²⁵ Section 36 NDPA 2023.

¹²⁶ Section 37 Ibid.

¹²⁷ Section 38 NDPA 2023.

In line with the provisions of section 51 above, article 47 of the Nigeria Data Protection Act General Application and Implementation Directive (NDPA-GAID), provides that a data subject may seek redress for the violation of his or her right to privacy at the closest Federal or State High Court in line with settled precedents of the Supreme Court of Nigeria and extant Fundamental Rights Enforcement Procedure Rules.

In line with these statutory directives, many persons have in recent times enforced their rights to privacy in court against certain data controllers and processors in Nigeria. In the case of *Bi-Courtney Aviation Services Ltd v. Kelani*,¹²⁸ the Court of Appeal held that the unauthorized use of a person's photograph for advertisement was a breach of the person's right to privacy and accordingly granted damages.

In an unreported suit between Chukwunweike Araka Akosa vs Eat 'N' Go Limited, the court awarded the sum of ₦3,000,000.00 (Three Million Naira) against Domino's Pizza (a subsidiary of Eat 'n' Go Limited) for breach of privacy of the applicant. The case began on December 14, 2023 when Akosa noticed that Domino's Pizza had been sending promotional messages to his phone. Despite not providing his data to the restaurant or consenting to its use for marketing, the messages continued. By May 25, 2024, the unsolicited messages had reached 16 instances.¹²⁹

Investigations revealed that Jumia Food, an e-commerce platform, initially collected Akosa's personal data when he placed a food order. However his data was later shared with Domino's Pizza, which then used it for marketing purposes without his consent. Jumia, after being contacted, failed to resolve the issue, leading Akosa to seek legal redress through Equibridge Attorneys.¹³⁰

During the court proceedings, Jumia Food was identified as a data controller under section 65 of the Nigeria Data Protection Act, 2023, which means it is responsible for ensuring lawful processing of user data. However, the court ruled that Jumia fulfilled its duty by notifying Domino's Pizza to cease the misuse of customer data. Since there was a written agreement between Jumia and Domino's Pizza regarding such instances, Domino's Pizza was held solely liable for the data breach.¹³¹

Accordingly, the court found Domino's Pizza liable for breach of the applicant's data privacy and awarded the sum of ₦3,000,000.00 (Three Million Naira) as compensation for the violation of his fundamental right to privacy.

¹²⁸ *Bi-Courtney Aviation Services Ltd v. Kelani* (2021) LPELR-56365(CA)

¹²⁹ Unini Chioma, 'Court Awards N3 Million Against Domino's Pizza For Unlawful Use Of Customer Data In Marketing' *TheNigeriaLawyer* (March 5, 2025) <<https://thenigerialawyer.com/court-awards-n3-million-against-dominos-pizza-for-unlawful-use-of-customer-data-in-marketing/>> accessed 16 June 2026.

¹³⁰ *Ibid.*

¹³¹ *Ibid.*

In the case of *Emerging Markets Telecommunications Services v Eneye*¹³², the Court of Appeal held that the acts of the appellant in giving unknown persons and organizations access to the Respondent's Etisalat GSM phone number to send unsolicited messages into it, amounts to violation of the Respondent's right to privacy guaranteed by section 37 of the Constitution, which includes the right to the privacy of a person's personal telephone line.¹³³

Examination of Compliance with Legal Regime on Data Protection in Nigeria

Living in an information age with a considerable proportion of global citizens now having easy access to internet enabled devices such as phones, tablets, laptops etcetera, comes with its pros and cons.¹³⁴ For instance, when a person visits online websites, they are often required to meet certain conditions precedent before they can access the services available on the website.¹³⁵ For example, to create an email account on Hotmail, Yahoo, or Gmail, first time registration requires input from the would-be user of specific personal information including their personal address, phone number, date of birth, occupation and next of kin to form the basis of their security information.¹³⁶ It is widespread practice that most websites which offer online services require personal data to create online accounts through which purchases, and other concurrent engagements can be undertaken online by the consumer.¹³⁷ The average individual has access to many online platforms which require the use of personal data, such as social media accounts (e.g., Instagram and Facebook); email accounts; banking or finance applications; online vendor platforms such as Amazon and Jumia; betting agencies such as Betway, Naira Bet etcetera.¹³⁸

The widespread imposition on consumers to provide personal data prior to using online services on different platforms creates a very real risk of misuse of personal data which can lead to various infractions such as identity theft, illegal sharing of personal information with third parties and the rise in spam phone calls and emails when the personal data of users are illegally sold to companies which engage in electronic marketing.¹³⁹

In Nigeria, there have been a rising amount of cases of data breaches by data controllers and processors, with some of these breaches being undocumented. According to the report published on the Nigeria Data Protection Commission's international journal, the NDPC has investigated over 20 cases of data breaches across various sectors; received over 4,500 complaints of data breach from individuals; received over 8,142 audit filings from registered data controllers and

¹³² *Emerging Markets Telecommunications Services v Eneye*(2018) LPELR-46193 (CA)

¹³³ In an unreported case, the court order MTN to pay #15,000,000 to a subscriber for illegal airtime deductions via unsolicited services and breach of privacy<<https://thenigerialawyer.com/privacybreach-court-of-appeal-orders-mtn-to-pay-n15m-to-subscriber-for-illegal-airtime-deductions-via-unsolicited-services/>> accessed 16 June 2026.

¹³⁴ F. Fawehinmi, 'An Overview of the Legal Framework of Data Protection in Nigeria' (ALP NG & CO) <<https://share.google/78sMjpHEV8liqCtMX>> accessed 16 June 2026.

¹³⁵ Ibid.

¹³⁶ Ibid.

¹³⁷ Ibid.

¹³⁸ Ibid.

¹³⁹ Ibid.

processors; registered 33,053 controllers and processors and over 7,213 data protection officers as at 2025.¹⁴⁰

Despite the progress made in advancing data protection initiatives, the Nigeria Data Protection Commission (NDPC) affirms that several challenges remain in the effective enforcement of data privacy laws in Nigeria. This study concurs with the findings of the Nigeria Data Protection Commission, that there is more to be done in the aspect of ensuring compliance to data protection regulations in the country by not just data controllers and processors of major importance but also the minor ones as breach of privacy in whatever form, could be devastating to the affected party. The examination of the registered data controllers and processors in Nigeria in contradiction with the real number of unregistered number of data controllers and processors in reality reveals that many persons and corporations are not yet fully compliant with Nigeria's data protection framework. This challenge of non-compliance in reality could be linked to lack of awareness of the existing framework and its requirements, amongst several other contributory factors.

Identification of the Challenges in Ensuring Data Protection in Nigeria

With the emergence of the Nigeria Data Protection Act as well as the introduction of the Nigeria Data Protection Act General Application and Implementation Directive, there is clear indication that efforts have been made in beefing up Nigeria's legal framework on data protection. Despite these innovations as well as the efforts of the Nigeria Data Protection Commission, a number of challenges exist with regard to the enforcement and compliance with the legal framework in Nigeria. Some of the challenges affecting complete data protection in Nigeria are identified below.

i. Weak enforcement of existing laws and regulations:

Although the existing laws have extensively provided for the protection of data in Nigeria, the unfortunate reality is that both public and private organisations in Nigeria frequently disregard the requirement of consent before collection of data, causing countless people and even business entities to suffer difficulties.¹⁴¹ For instance, the Act requires that informed consent must be sought before any personal data is collected. This is especially true when the goal of the data collection is clearly stated and further consent is required for sharing personal information with other parties.¹⁴² However, in Nigeria, there are several occasions where businesses and organisations with which data subjects are likely to have never consciously interacted are generating and capturing data and information about them without their awareness and nothing is being done about it, even though the law has stated that everyone that may be in possession of personal data of others should register with the Nigeria Data Protection Commission as a data controller or processor to ensure better monitoring.

¹⁴⁰Vincent Olatunji, 'Implementing a Data Protection Law: The Case Study of Nigeria' *NDPC- International Journal of Data Privacy and Protection* (2025), 1-25 <<https://share.google/4YtTJgnaaTl8g4tLQ>> accessed 16 June 2026.

¹⁴¹H. Bagudu, 'Legal and Institutional Challenges to the Enforcement of the Nigeria Data Protection Act' *UDUS Law Journal* (2026) 1(1).

¹⁴²Ibid.

ii. Lack of Awareness and Education

One of the major obstacles to data protection in Nigeria is the lack of widespread awareness and education about data privacy rights and obligations. Many organizations, as well as individuals, are still unaware of their rights and responsibilities under the Nigeria Data Protection Act (NDP Act), making it difficult to foster a culture of compliance.¹⁴³

iii. Shortage of Competent Professionals in the Country

The emergence of new roles under novel legislation, such as the Data Protection Act and the NDPR, pose one of the major challenges facing data privacy and compliance in Nigeria.¹⁴⁴ Such roles include data protection officers (DPOs) which requires expert knowledge and certain skill sets. Nigerians and citizens of other third-world countries are not familiar with such role, in contrast to citizens of western countries.¹⁴⁵

iv. Increasing risk from advances in information technology

It goes without saying that technology has been, and continues to succeed at, the role of putting the world at our fingertips, to the point that almost all information can be obtained at the convenience of our zones.¹⁴⁶ The fact that abusers have taken advantage of these systems' weakness to further their actions shows that this is not without problems. Of course, the concerns posed by the advancement of information technology to further improve the circulation and retention of data are cause for concern as they extend to the absence of suitable laws to fully address existing issues relating to the data subject. One of the fundamental flaws in the current data legislation is that there are only measures for protecting digital data and none for offline data, in addition to the fact that there aren't many situations where the issue has been resolved.¹⁴⁷

Furthermore, the rapid pace of technological advancements presents a significant challenge for data protection regulation. Emerging technologies, such as artificial intelligence, big data analytics, and the Internet of Things (IoT), create new vulnerabilities in personal data processing, which require the continuous adaptation of policies and enforcement mechanisms.¹⁴⁸

v. Limited Resources

The NDPC, like many regulatory bodies, faces resource constraints that affect its ability to fully implement and enforce the NDP Act. Limited human, financial, and technical resources hinder the

¹⁴³Vincent Olatunji, 'Implementing a Data Protection Law: The Case Study of Nigeria' *NDPC- International Journal of Data Privacy and Protection* (2025), 1-25 <<https://share.google/4YtTJgnaaTl8g4tLQ>> accessed 16 June 2026.

¹⁴⁴(n.141).

¹⁴⁵Ibid.

¹⁴⁶PC Aloamaka, 'Effective Data Protection in Nigeria: Challenges' *Commonwealth Law Review Journal* (2022) 8,656-662 <<https://share.google/jrUvPpLbogHlbD2aI>> accessed 20 June 2026.

¹⁴⁷O. Babalola, 'Data Protection and Privacy Challenges in Nigeria (Legal Issues) - Privacy - Nigeria' (Mondaq 2020) <<https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues->> accessed 20 June 2026.

¹⁴⁸(n.10).

Commission's capacity to conduct widespread inspections, investigations, and capacity building initiatives.¹⁴⁹

CONCLUSION

Data protection generally refers to the efforts put in, to safeguard or shield personal data or information against misuse, corruption, breach, or loss.¹⁵⁰ In this modern age where more reliance has been placed on technology, and the personal data of individuals are also being stored digitally, there is always a risk that these data could be exposed or breached either inadvertently or through cyber-attacks. As shown in the cause of this research, the consequences of such non-consented breach or exposure of data are dire, including financial losses or reputational damages.

Consequently, several countries and international organizations, in their recognition of the risks posed by uncontrolled use of data or data breaches, came up with different legal and institutional frameworks to ensure that data is protected as much as possible. In Nigeria, several legislations such as the Nigeria Data Protection Act, the Nigeria Data Protection Act General Application and Implementation Directive (GAID) as well as other sector-related regulations exist for the protection of Data in Nigeria.

From the analysis of the legal regime for data protection in Nigeria, this study finds that the existing regime adequately regulates data protection in the country on paper, the reality is that these laws have not been fully implemented in Nigeria, thereby limiting the realization of its full potential and the identification of any lapses.

This research however revealed that in recent times the regulatory agency, the Nigeria Data Protection Commission, has done its bit in ensuring that major data controllers and processors are registered and monitored. An indication of this, is the mention of several cases wherein the agency has imposed punitive fines for defaulting controllers/processors, as well as the civil remedies under the law which has led to monetary benefits for victims of data breaches, as was shown in the course of this research. This study therefore concludes that more needs to be done in the aspect of sensitization of the public and stakeholders on their responsibilities under the law, and for broader implementation of the law.

Recommendations

While it could be said that Nigeria boasts of an impressive cache of laws on data protection, the same thing cannot be said about its implementation culture. In the course of this study, a number of challenges have been identified, as hindering the full development and effectiveness of Nigeria's legal framework on data protection. Accordingly, the following recommendations are suggested.

¹⁴⁹Ibid.

¹⁵⁰ Section 65 Nigeria Data Protection Act 2023.

- i. More efforts has to be invested by the Nigeria Data Protection Commission as well as other affiliated agencies, to ensure the full enforcement and implementation of the laws. For instance, while the commission is saddled with the responsibility of registering data controllers/processors, the reality is that thousands of these controllers/processors are operating without license and as such their activities are not being monitored.
- ii. There is an imminent need for the responsible agencies to carry out widespread sensitization of the public on the provisions of Nigeria's legal framework in order to expose data subjects to their rights and also intimate data processors/controllers on their responsibilities. Even though it is settled that ignorance of the law is not an excuse, sometimes the cost of such ignorance is too damaging beyond what can be resolved by the imposition of fines or penalties. A lot of Nigerians are not aware that their data protection rights have been unlawfully breached or that they are entitled to civil and administrative remedies for these breaches.
- iii. It is important that more financial resources are provided to the data protection agencies to enable them perform their responsibilities better. The presence of financial backing would translate to a wider monitoring/implementation coverage by the commission, through the employment and training of more personnel, especially data protection officers.
- iv. There is also need for increased level of punitive punishments for defaulters to serve as deterrence to others. The efforts of the Nigeria Data Protection Commission in imposing fines on major data controllers such as financial institutions and Meta (as was shown in course of this research), is a step in the right direction. It is therefore recommended that more needs to be done in this aspect in order to reduce incidences of data breaches and indiscriminate data sharing by data controllers/processors to the barest minimum.