# AN EXAMINATION OF DATA PROTECTION AND THE RIGHT TO PRIVACY IN THE NIGERIAN TELECOMMUNICATIONS INDUSTRY

*Written by* ***Omoniyi Bukola Akinola* & Jane K Morsindi*****

** Professor of Law, Faculty of Law, Redeemer's University, Ede, Nigeria*

*** 5th Year LLB Student, Redeemer's University, Ede, Nigeria*

## ABSTRACT

In the world today, when looking for someone, the first thing that a person does is pick up their phone and search for the person's name, and a lot of the time, the internet is bound to turn up something about that person. This is because everyone in this day and age belongs to at least one social networking site due to technological advancement and numerous social networking sites. As a result of belonging to one of such social media sites, you are required to fill out a form that usually asks for personal details, which are also displayed for anyone to view when they conduct a simple internet search. With the preceding, it is easy to see that people's data can easily be accessed not just by the sites being given personal information but also by anyone anywhere in the world. As a result, data protection and privacy are pressing issues in the digital age and one that cannot be overemphasized. A major research question in the above analysis is to what extent should a person's data be in the public domain considering his constitutionally guaranteed right to privacy under the law especially in Nigeria? The paper adopts the doctrinal methodology by examining the various legal regimes, judicial decisions where applicable, and opinions of authors, among others. This paper, in answering this question, discussed the concept of personal data, the right to privacy under the constitution, the need for enforcement of data protection laws, and the data protection laws in existence. The paper ends with recommendations to protect the data of citizens in Nigeria.

***Keywords***: Data Protection, Right to privacy, Telecommunication Industry

## INTRODUCTION

Data has surpassed oil as the world's most valuable asset. Data is a factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation.[i] Data has been defined as distinct units of information that may be measured, gathered, reported, saved, and analyzed. Data is information that has been transformed into a form efficient for transfer or processing in computers. Data is regarded as the "oil" of the digital era. Google, Apple, Facebook, and Amazon (GAFA) are among the world's most valuable corporations, as are Baidu, Alibaba, and Tencent (BAT). Their members are often expected to disclose their data to allow access. The internet and cell phones have substantially increased the value, availability, and abundance of data. The easy access to data has brought up the need to look at the fundamental human right to privacy as entrenched in the constitution and see if this right is being infringed upon as a result of the practices of the digital era. The first part of this paper gives an overview of the basic concepts under examination and the second part analysed the international instrument for the regulation of privacy rights and data protection. The third and fourth parts of the paper examined the existing legal and institutional framework for data protection and appraised the level of enforcement of data protection rights vis-à-vis existing level of citizens awareness of their rights and possible remedies available for violations especially in Nigeria.

## AN OVERVIEW OF THE CONCEPT OF THE RIGHT TO PRIVACY

As a legal principle, the right to privacy appeared earlier in a law review paper written by two young Boston attorneys, Samuel Warren and Louis Brandeis, in December 1890.[ii] The first time the right to privacy was articulated, Warren and Brandeis wrote that it was a common law right that guaranteed protections for each person's "inviolate personality".[iii] Warren and Blandeis asserted that, "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others... fixing the limits of the publicity which shall be given to them."[iv]

Warren and Brandeis reasoned that when information about a person's private life is made public, it tends to affect and even harm the very basis of a person's personality—"his appraisal

of himself" and that is why the legal system must acknowledge the right to privacy. The psychological insight that an individual's personality, particularly their self-image, can be affected and sometimes distorted or injured when information about that person's private life is made available to other people was thus embodied in Warren's and Brandeis' original concept of the right to privacy, which was at the time reasonably unexplored. To put it simply, Warren and Brandeis believed that everyone has the right to maintain their psychological integrity by exerting control over the material that reflects and influences their personalities.[v]

The privilege of individual independence is crucial to the" right to be left alone". The right to privacy is a constitutional constraint on the state's powers. This right is provided for in section 37 of the Constitution of the Federal Republic of Nigeria [CFRN], which states: "The privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected."[vi] Kennedy and Alderman posit that the word privacy is not found in some nation’s constitution but it does not erode the fact that right to privacy exists in several constitutions of nations.[vii]

It is worth noting, however, that the private zone has suddenly taken up the invasion of a person's privacy that was historically attributed to the government. In our globalizing world, the ever-increasing risks to national security have encouraged the development of high-tech security [CCTV and biometric identification procedures] that limit residents' right to privacy. "It would be a good thing if privacy could be protected," says Jeremy M. Miller, "but the war and way of technology and the needs of security have de facto made the right to privacy a dead letter."

As a result, "Big brother" (the state as referred to in George Orwell's 1984) appears to be invading its inhabitants' lives. The most significant hurdles to the right to privacy are technology and social media. Facebook and Instagram are two examples of social media platforms where personal information and photographs are shared. Technology has been used to manipulate certain information relating to a person through various means, including electronic monitoring of people by intercepting other people's emails and merging databases containing personal data, as practised by many advertising and marketing firms.

The right to privacy encompasses several concerns, including confidential correspondence, email and internet use, medical history, personal data, eavesdropping, sexual orientation, and personal lifestyles. According to Solove4, privacy consists of six components:

1. personal autonomy;
2. restricted access to the self;
3. secrecy;
4. personal information management;
5. the right to individuality; and
6. connection

Based on these factors, it becomes evident that privacy is only significant when it strives to preserve an individual's rights that they wish to keep private, i.e. events that are not intended to be in the public domain.

As a result, it is reasonable to argue that behaviours that individuals wish to keep hidden from the public eye or from the society in which they live are not protected by the right to privacy. Simply expressed, the right to privacy is defined as any activity that is meant to be kept secret from others.

The right to privacy entails preventing the public from delving into an individual's affairs. Another critical part of the right to privacy is the right to safeguard one's image and personality, as well as to have complete control over one's zones of exclusivity, space, and sensitive information. The sphere of self is where privacy exists; the right to own something. It is the moral liberty of an individual to do whatever they see fit in order to maintain their individuality while keeping others beyond the sphere of themselves.[viii]

In the case of *Incorporated Trustees of Laws and Rights Awareness Initiative v. Zoom Video Communications Inc (FHC/AB/CS/53/2020)*,[ix] in order to safeguard the rights of zoom users to data security and privacy, Trustees of Laws and Rights Awareness Initiative filed a data privacy lawsuit against Zoom Video Communications Inc.

The lawsuit was brought by Olumide Babalola LP on behalf of the NGO. The Applicant, who sued for and on behalf of its members, claimed that Zoom's privacy policy stated that it was a data processor rather than a data controller and that it was in violation of the Nigeria Data

Protection Regulation 2019 as a result. As a result, the Applicant claimed that Zoom could face sanctions from the National Information Technology Development Agency (NITDA). The case is still ongoing.[x]

## AN OVERVIEW OF THE CONCEPT OF DATA PROTECTION

According to Section 1.3 of the Nigeria Data Protection Regulation (NDPR) of 2019, data is defined as '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.[xi]' The section also defines personal data as 'any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.'[xii]

It also defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. [xiii] Almost every human activity leaves a digital footprint. When we are connected to the internet, our heartbeat, pulse, a running event, and navigating through traffic all produce data. The more internet-connected automobiles, watches, and phones, the more data may be generated.

Internet subscribers and social media users are frequently expected to disclose personal and sensitive information to gain access to and utilize these platforms. Almost all online transactions require the disclosure of some personal information. Although social media users are frequently notified of data privacy rules, this does not limit the use or sharing of such personal data in some instances. This raises the prospect of sensitive personal information being shared with or sold to high-level security agents or blue-chip firms to facilitate

monitoring and data collection.[xiv] There is a critical need to ensure that the data of individuals are protected.

Data protection is the act of protecting critical data against corruption, compromise, or loss, as well as giving the ability to restore the data to a functioning condition if anything happens to leave the data inaccessible or useless. Data protection ensures that data is not damaged, is only available for allowed reasons, and complies with all applicable legal and regulatory standards; when needed, protected data should be accessible and used for the intended purpose. It entails safeguarding personal data, which includes facts and views about an individual. It is our view that data protection includes data identity.

In furtherance of the above, data protection is broadly divided into three categories: conventional data protection (such as backup and restoration copies), data security (such as encryption, access control, and threat monitoring), and data privacy (such as legislation, best practice and policies). [xv] Data protection techniques and business practices are utilized to achieve the overall aim of continuous availability and immutability of essential corporate data through the procedures and techniques used to preserve and secure data.[xvi]

The main principles of data protection are to protect and make data available in all circumstances. Data security techniques are advancing in two directions: data availability and data management. Data availability guarantees that users can access the information required to perform business, even if the data is corrupted or destroyed.[xvii] The European Convention on Human Rights, which guarantees the right to privacy and family life, is an example of data protection law. It also states that no public authority may interfere with the exercise of this right unless it is required by law and is necessary for a democratic society for the purpose of national security, public safety, or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.[xviii]

This has ramifications for information about people's data in terms of how it is maintained, processed, and communicated, especially as abuse might violate the aforementioned right. In a recent case of Google against the Australian competition watchdog, Google has agreed to pay a fine of 60 million dollars for deceiving customers about the acquisition of sensitive location data. In April of 2021, a federal court ruled that Google violated consumer laws by tricking

confident local consumers into believing the firm was not gathering personal data about their whereabouts via mobile devices running Android. The dispute was about whether it was clear enough that Google would still collect and access location data when a user's location history was set to "off." Still, their browser and app activity were set to "on," and one of its applications was utilized. The organization was also found to be violating two additional consumer regulations, one involving behaviour likely to mislead the public and the other involving making misleading assertions regarding the performance qualities of service. At the time, the Australian Competition and Consumer Commission described the decision as a strong message to digital platforms to be transparent with customers about what is happening with their data.[xix]

## AN OVERVIEW OF THE NIGERIAN TELECOMMUNICATIONS INDUSTRY

The telecommunications industry is made up of corporations that enable worldwide communication, whether through the phone or the internet, airways or cables, wires or wirelessly. These corporations built the infrastructure that allows data to be transferred anywhere globally in the form of words, speech, audio, or video. Telephone (both landline and wireless) operators, satellite companies, cable companies, and Internet service providers are the leading corporations in the industry.[xx]

Prior to 2001, Nigeria's telecommunications market was not yet deregulated and the country had about 400,000 lines, which were insufficient to accommodate the rising demand for telecommunications services by Nigerians.[xxi] Access to information technology was also restricted due to Nigerian Telecommunications Limited's unsuccessful operations (NITEL). In 2001, the sector was liberalized, ushering in the first Global System for Mobile Communication (GSM) operator and the first Digital Mobile License (DML) issue.[xxii] Since then, the sector has seen an unprecedented boom in investment and growth (with over $18 billion invested since 2001). Introducing new operators has also increased competition in the industry, which benefits from the large subscriber base.[xxiii]

## INTERNATIONAL INSTRUMENTS FOR THE PROTECTION OF THE RIGHT TO PRIVACY

The formal normative basis for data protection laws is derived primarily from catalogues of fundamental human rights set out in several multilateral instruments, notably:

***Article 12 of The Universal Declaration of Human Rights (UDHR) provides:***

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[xxiv]

***Article 17 of The International Covenant on Civil and Political Rights (ICCPR) provides:***

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.
2. Everyone has the right to protection of the law against such interference or attacks.[xxv]

***Article 16 of The Convention on the Rights of the Child (CRC) provides:***

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

2. The child has the right to the protection of the law against such interference or attacks.[xxvi]

***Article 14 of the International Convention on the Protection of All Migrant Workers and Members of Their Families provides:***

No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, , correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.[xxvii]

At the regional level, the right to privacy is protected by:

***Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) which provides:***

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[xxviii]

***Article 11 of the American Convention on Human Rights (ACHR) provides:***

1. Everyone has the right to have his honor respected and his dignity recognized.

2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

3. Everyone has the right to the protection of the law against such interference or attacks. [xxix]

All of these agreements specifically recognize privacy as a basic human right except for the African Charter on Human and People's Rights. The exclusion of privacy in the African Charter is not seen in all human rights catalogues from outside the Western, liberal-democratic realm.[xxx]

## INTERNATIONAL FRAMEWORK FOR DATA PROTECTION

On a global scale, there is no legal tool for individual data protection. Instead, there exist territorial data protection regulations that apply only to specific nations or areas. These laws establish a legal framework for collecting, using, and storing natural people's personal data.[xxxi]

Therefore, in looking at the international laws that govern data protection, we would be looking at data protection laws established by various countries and regions that govern data protection within that country or region.

In the United States, for example, data privacy regulations have been extensively described as "sectoral," referring to fragmented, cross-governmental, and industry-specific regulation. Unlike in Europe, the United States' legal system does not recognize a fundamental right to privacy. Although the United States Constitution does not directly protect privacy, constitutional privacy rights are inherent in the First, Third, Fourth, Fifth, and Fourteenth Amendments.

Data protection regulation places restrictions on sectors that traditionally handle sensitive private data. Data protection laws are frequently narrowly crafted, targeting specific parts of personal information or discrete uses of discrete data." State and local data privacy laws in the United States complicate matters even more. The Federal Health Insurance Portability and Accountability Act, for example, has no pre-emptive impact, allowing state governments to enact further legislation affecting medical and health information.[xxxii]

An example of data protection law in the United States is The California Consumer Privacy Act (CCPA), which is a state-wide legislative act in the United States that intends to govern how businesses all over the globe are permitted to handle the personal information of California citizens.

The CCPA exclusively applies to for-profit businesses. If a company does business in California and gathers personal information from at least one California citizen, the following conditions must be met:

The company has (i) more than $25 million in annual gross sales, (ii) handles personal information for at least 50,000 California customers, households, or devices, or (iii) gets more than 50% of its annual income from selling personal information.[xxxiii]

Unlike in the United States, privacy is a fundamental right in the European Union (EU). Rather than sectoral and industry-specific privacy regulations combined with industry self-regulation, the EU enacted comprehensive laws to safeguard personal data across the board.

The General Data Protection Regulation (GDPR) is an EU-wide data privacy regulation that seeks to better individuals' fundamental rights to personal information and privacy in the digital age.

Even though the GDPR has been implemented and is in effect in Europe, it has far-reaching consequences. Its scope extends outside the EU, and enterprises providing products or services to EU nationals for the purpose of monitoring their online conduct must comply with it regardless of location.

GDPR grants data subjects various rights, including the right to access data, the right to erasure (also known as the right to be forgotten), the right to data correction, the right not to be subject to automated decision-making, and so on. These rights provide data subjects more control over their personal data and how organizations utilize it.

GDPR imposes severe fines for noncompliance. The rule specifies a two-tiered punishment scheme. As a result, for less serious infractions, the administrative fee is equivalent to 2% of worldwide annual revenue or 10 million Euros, whichever is greater, and for more serious violations, the administrative fine is equal to 4% of global annual sales or 20 million Euros, whichever is more.

In Brazil, they have the Lei Geral de Protecao de Dados (LGPD) as the general data protection law. It is Brazil's most comprehensive data privacy law in history, and it was established in reaction to the GDPR. The LGPD puts many requirements on corporations while also offering internet users rights.

LGPD applies to businesses and individuals who process personal data in the following circumstances: (i) the processing activity is carried out anywhere in the world for the purpose of offering or supplying goods or services or processing data of individuals located in Brazil, or (ii) the personal data was collected in Brazil.

Brazilian law also imposes severe administrative fines for noncompliance. As a result, businesses may face an administrative fine of up to 2% of their annual revenue, up to a maximum of 50 million Brazilian reals. [xxxiv]

## LEGAL FRAMEWORK FOR DATA PROTECTION IN NIGERIA

Several laws have been established in Nigeria, just like in the United States, Brazil and the European Union, to govern the protection of the data of Nigerian citizens. Some of these regulations or laws are as follows:

***The National Information Technology Development Agency (NITDA) Regulation***

While there are various legislations in Nigeria that contain ancillary provisions aimed at protecting data privacy, the most extensive legislative instrument for this purpose is a subsidiary legislation enacted under the NITDA Act. The NITDA Act gives the National Information and Technology Agency (NITDA) the authority to develop recommendations for electronic governance and monitoring electronic data exchange. NITDA subsequently designed and released the Nigeria Data Protection Regulation 2019 based on this clause. The NITDA Regulation is notable for having data privacy and protection-specific set of laws, as opposed to being an auxiliary component in legislation whose major goal is not data protection.

***The 1999 Constitution of the Federal Republic of Nigeria***

The Constitution of the Federal Republic of Nigeria 1999, as amended ("the Constitution"), through section 37 thereof, protects the rights of citizens to their privacy and the privacy of their homes, correspondence, telephone conversations, and telegraphic communication, is the source of Nigeria's data privacy and data protection regime, as applies to most jurisdictions. Thus, the extension of a citizen's fundamental right to privacy is data privacy and protection.

***The Child Rights Act***

In order to domesticate the United Nations Convention on the Rights of the Child, a human rights agreement created to protect children's civil, economic, political, social, cultural, and other rights, Nigeria established the Child Rights Act (CRA) in 2003. The CRA is a piece of legislation designed to safeguard and defend the rights of Nigerian children who are those that are below the age of 18. The provisions of Chapter IV of the Constitution, which deal with citizens' fundamental rights, are incorporated into Section 3 of Part II of the CRA. Additionally, a kid is entitled to his privacy, family life, home, mail, and telephone calls, according to Section 8 of the CRA, which addresses a child's rights to private and family life.

***Freedom of Information Act 2011 (FOIA)***

The FOIA was created to provide public access to official documents and data held by government organizations. It does, however, clearly specify an exemption with regard to personal data, information, and privacy-related issues. In this regard, section 14 of the FOIA prohibits government entities from exposing people's personal information unless they have their consent or it is already in the public domain.

***Cybercrimes (Prohibition, Prevention Etc) Act 2015 (CPPA)***

Establishing a framework for the prescription, prevention, identification, prosecution, and punishment of cybercrimes in Nigeria is the main goal of the CPPA. Mobile networks, computer service providers, and communications service providers are required to keep and preserve subscriber information for a minimum of two years. Importantly, it mandates that these service providers give high priority to an individual's constitutionally protected right to privacy and take measures to protect the confidentiality of any data they process.

***Central Bank of Nigeria Consumer Protection Framework 2016 (CPF)***

The Central Bank of Nigeria (CBN) established the CPF to, among other goals, increase public trust in the financial system as part of its mission to foster a stable financial system. The Central Bank of Nigeria act of 2007 (CBN act) was modified, and the Banks and Other Financial Institutions Act (BOFIA) of 2007 made the CPF a secondary piece of law. According to the CPF's section 3.1(e), customer information must be protected from unauthorized access and disclosure. Before customers' data may be shared with other parties or used for promotional purposes, financial services organizations are required to get written authorization from them in order to authorize disclosure.

***The Credit Reporting Act (CRPA) 2017***

The CRPA was passed in order to standardize risk management in credit transactions and improve access to credit information. It offers the foundation for credit bureaus, licensing, and reporting. Section 9 of the CRPA states that, with the limitations outlined in sections 9(2) to 9(6), Data Subjects, or those whose data is stored by credit bureaux, are entitled to the privacy, confidentiality, and security of their credit information.[xxxv]

***The National Identity Management Commission Act (NIMC Act) 2007***

The NIMC Act creates the national identification database, and the National Identity Management Commission (NIMC) is taxed with the responsibility of maintaining it, registering persons, and issuing general multipurpose identity cards.

***The Nigerian Communication Commissions Act 2003***

Among other things, this statute calls for the Nigerian Communications Commission (NCC) to be reformed as an independent regulatory body. The creation of this body is for the regulation of the telecommunications industry; the formation of the National Frequency Management Council; and the establishment of the Universal Service Fund.[xxxvi] This Act played a major role in the reforms experienced in the telecommunication sector in Nigeria. It is established as an agency of government under the Federal Ministry of Communications and Digital Economy.

## THE SCOPE OF RIGHT TO PRIVACY AND DATA PROTECTION IN THE NIGERIAN TELECOMMUNICATIONS INDUSTRY

Over time, the idea of privacy has evolved from a civil and political-rights problem fuelled by polemic ideology to a consumer-rights one anchored by data-protection principles and trading-standards law. Privacy has evolved from a matter of societal power dynamics to one of the tightly defined legal rights. If opinion surveys truly represent community opinions, there is presently more worry about privacy violations than at any previous period in recent history. People all around the industrialized world are concerned about the loss of privacy and the possibility of computer spying. In today's world, privacy protection is commonly seen as a set of technological regulations controlling data handling.[xxxvii]

One of the major global collectors of private data is the telecommunications sector. Telecommunication firms are continuously pursued by hackers because they get personally identifiable information (PII) and financial data from millions of consumers.

43% of telecom operators experienced DNS-based malware assaults in 2018, and a startling 81% took three days or more to implement a vital security fix when a data breach was discovered, according to cybersecurity firm EfficientIP. The same analysis revealed that among all businesses, the telecoms industry had the highest rate of sensitive data theft, with 30% of the participating telecommunication companies reporting stolen client data.

The telecoms sector was most frequently targeted by a distributed denial of service (DDoS) assaults in the first quarter of 2021, a considerable increase from the previous year, according to more recent data from security firm Cloudflare.

A Kaspersky investigation also revealed that insiders are frequently used by cybercriminals to target telecom providers. Hackers use compromising information gleaned from open sources to blackmail personnel or transform angry employees into malevolent insiders. At the time the study was published, insiders were involved in about 28% of all cyber attacks with telecom targets.

However, there are other threats that telecom businesses should be concerned about as well. A recent wave of data protection regulations and international standards also protects private information (PII) and financial data.

The protection of personal data is now required by law in every country, from the EU's General Data Protection Regulation (GDPR) to Brazil's Lei Geral de Proteço de Dados (LGPD) to Japan's Act on the Protection of Personal Information (APPI). These rules carry severe financial fines and reputational risks for breaking them.[xxxviii]

In Nigeria, the telecommunication sector is regulated by The Nigerian Communications Commission (NCC). The NCC is the autonomous governing body for Nigeria's telecommunications sector. The NCC was tasked with creating performance criteria for telephone services in Nigeria, encouraging competition, and regulating the provision of telecommunications services and facilities.

The Federal Government adopted a number of projects that called for the collecting of people's personal information through several of its institutions, including the Federal Road Safety Corps (FRSC), National Identity Management Commission (NIMC), Central Bank of Nigeria, and INEC. These programs include the registration of SIM cards, National Identity Cards, New

Vehicle Licenses, BVN, Voter's Cards, Tax Identification Numbers (TIN), and a plethora of additional programs. The number of customers to various telecommunication services has also increased dramatically as a result of developments in the telecoms sector.

In order to improve security and accountability, it is crucial that the proper enabling legislation be passed alongside these projects, technologies, and services. At the same time, efforts should be made to streamline and harmonize the storage of personal data.[xxxix]

The NCC, under the Regulation of Telephone Subscribers (RTS) Regulation, 2011, created guidelines for the provision of internet service regulations to govern the use of (personal) data by telecommunications operators and/or Internet Service Providers (ISPs), as well as to safeguard the security and confidentiality of data kept and handled by telecommunications firms and independent agents. All custodians of telecommunications data are required by the Regulations to maintain subscriber data and to make reasonable efforts to guarantee its confidentiality and protection against unauthorized disclosure. It further states that customer information "must not be shared to any third party unless otherwise authorized or required by any applicable laws or regulations." However, the Regulations only apply to operators in Nigeria's communication business.

Section 9 of the Regulation of Telephone Subscribers (RTS) Regulation, 2011 states that subscribers' information contained in the Central Database shall be kept strictly confidential, and no person or entity shall be permitted to access any subscriber's information that is on the Central Database, which contains all Subscribers' biometric and other registration information, except as prescribed by the regulation. The regulation does not identify such exclusions or the requirements for access to the central database. Section 21 of the Regulation imposes penalties on offenders.[xl]

The NCC also adopted the Consumer Code of Practice Regulations 2007. The regulation states that all licensees are required to take reasonable precautions to protect customer information from "improper or unintentional disclosure" and to ensure that such information is securely kept. It further states that customer information "shall not be shared to any third party unless otherwise approved or by other applicable laws or regulations." Unlike the Constitution, the NCC Regulations extend to all customer information related to consumers of any nationality who use a licensee's network and are not limited to Nigerian nationals.[xli]

## SUMMARY, CONCLUSION AND RECOMMENDATIONS

It is a notorious fact that the more technologically advanced an environment is, the easier it is to break into; you can just walk in the front door. In as much as the continuous advancement of technology brings with it many benefits to society, there are equally just as many disadvantages to society. One of such major disadvantages is the fact that it is very easy for hackers to hack into a person or company and just take whatever information they require, which can be used for unscrupulous means.

The world today is one plagued with many forms of insecurity, and they especially exist online. People have had their identities stolen and then used to engage in fraudulent activities without their knowledge all as a result of unscrupulous individuals having access to their data. Some people have also had money stolen from their bank accounts as a result of hackers who were able to gain access to their banking information.

The need for data protection laws in order to protect the fundamental right of privacy entrenched in the constitution is one that cannot be overemphasized. The current era has often been described as a digital era, and as a result, this means the constant use of technology and social media. The constant use of social media and technology comes with people posting very personal information on various social media sites for anyone to gain access to and use. This puts the personal information of people at risk, and there is, therefore, a need for governments all over the world to establish laws that would help to protect the personal data of individuals.

This paper has been able to discuss the concept of data itself, the fundamental right of privacy and the importance of ensuring that personal data is protected. It also discussed the various laws that have been established to help in the protection of personal data.

### *Findings*

No law exists to cover data protection on a global scale. There only exist laws on the national and continental levels to help protect the data of people. Nigeria also lacks adequate laws to protect the data of people from the telecommunications sector. The current law is wholly outdated, and there is a need for updated laws as the role of the telecommunication sector in

Nigeria has advanced since the year 2011, when the Regulation of Telephone Subscribers (RTS) Regulation was made. The telecommunication sector has more access to the personal information of users than any other sector in Nigeria, and there is a need to have appropriate laws that regulate their access to said personal information.

Also, despite its merits, the NDPR does not address online privacy protection, internet access, video surveillance, search engines, or social networking. All of these are contemporary obstacles to the Act's effective enforcement. The absence of a thorough Database and Data Protection Authorities/Commissioners, as with best practices, may offer a significant obstacle to the Act's enforcement. The procedure of gathering information about a person may cause delays in some legitimate critical tasks. For example, it may impede the successful criminal investigation conducted by authorized agencies. Individuals may use data protection rules to commit illegal acts since they have a considerable amount of control over who has access to their personal data and information.

***Recommendations***

In view of the above findings, it is recommended that:

I A Data Protection Act should be enacted into law. The Act should be one that incorporates data protection standards that are aligned with the EU's General Data Protection Regulation (GDPR) and other more advanced data protection laws that exist in other parts of the world.

II The NIMC Act should be amended to integrate strong data protection principles and broaden NIMC's powers to serve as a data protection body, ensuring that public and private organizations in Nigeria follow data protection standards while processing personal data.

III The NCC should update its regulations to protect the data of the customers of telecommunication corporations, not just from the corporations themselves but from anyone seeking to hack into their systems and steal the data of their customers. The NCC should also be given the power to enforce its regulations and adequately punish any corporation that contravenes said regulations.

## ENDNOTES

[i] Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/data Accessed 23 December 2022
[ii] Warren and Brandeis, The Right to Privacy, *Harvard Law Review* Vol. 4, 15 (1890) 5, p. 1
[iii] *Ibid*.
[iv] *Ibid*.
[v]Dorothy J. Glancy, 'The Invention of the Right to Privacy' [1979] 21(1) *Arizona Law Review*
[vi] CFRN s.37
[vii] Caroline Kennedy and Ellen Alderman, The Right to Privacy. (Vintage Publishers, Baltimore, 1997) p. 1
[viii]Yinka Olomojobi, 'Right to Privacy in Nigeria' (*SSRN papers*, 31 October 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062603#:~:text=National%20Protection%20The%20right%20to,is%20hereby%20guaranteed%20and%20protected.%E2%80%9D> accessed 12 August 2022
[ix] Unreported *FHC/AB/CS/53/2020*
[x]Halima Abiola, 'Data Privacy ' (*Loyal Nigerian Lawyer*, 30 June 2020) <http://loyalnigerianlawyer.com/data-privacy-federal-high-court-of-nigeria-orders-zoom-to-be-served-by-e-mail/> accessed 12 September 2022
[xi] Nigeria Data Protection Regulation 2019
[xii] N4
[xiii] N4
[xiv]Uche Val Obi, 'An Extensive Article on Data Privacy and Data Protection Law in Nigeria' (International Network of Privacy Law Professionals, 9th September) <https://inplp.com/latest-news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria/#:~:text=The%20right%20to%20data%20privacy,from%20corruption%2C%20compromise%20or%20loss.> accessed 25 August 2022
[xv] Snia, 'What is Data Protection?' (*SNIA*, 2022) <https://www.snia.org/education/what-is-data-protection> accessed 15 August 2022
[xvi] *Ibid*.
[xvii]Paul Crocetti, 'What is data protection and why is it important?' (*TechTarget*, February 2021) <https://www.techtarget.com/searchdatabackup/definition/data-protection#:~:text=Data%20protection%20is%20the%20process,to%20grow%20at%20unprecedented%20rates.> accessed 15 August 2022
[xviii] Franklin F. Akinsuyi, 'Data Protection Legislation for Nigeria: The Time is Now!',2007.

[xix]Chioma Unini, 'Google To Pay $60m Fine For Misleading Australians About Collecting Location Data' (The Nigeria Lawyers, 12th August) <https://thenigerialawyer.com/google-to-pay-60m-fine-for-misleading-australians-about-collecting-location-data/> accessed 13 September 2022
[xx]Brian Beers, 'What Is the Telecommunications Sector?' (*Investopedia*, 7 October 2021) <https://www.investopedia.com/ask/answers/070815/what-telecommunications-sector.asp> accessed 27 August 2022
[xxi] Uwuagwu Obi, The Revolutionary Years: Nigeria's Telecommunication Industry 2001 – 2011, p. 6. In Ndukwe Ernest. "An Overview of Evolution of the Telecommunication Industry in Nigeria and Challenges Ahead 1999 – 2003", October 2003
[xxii] *Ibid*.
[xxiii]Deloitte, 'Nigeria's telecommunications industry: Looking back, Looking forward' (Inside Tax, 2015) <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/tax/inside-tax/ng-nigeria-telecommunications-industry-looking-back-looking-forward.pdf> accessed 25 August 2022
[xxiv]Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12
[xxv] International Covenant on Civil and Political Rights 1996.
[xxvi] Convention on the Rights of the Child 1989
[xxvii] International Convention on the Protection of All Migrant Workers and Members of Their Families 1990
[xxviii] European Convention on Human Rights and Fundamental Freedoms 1953
[xxix] American Convention on Human Rights 1969
[xxx]LeeA Bygrave, 'Privacy and Data Protection in an International Perspective ' [2010] 1(1) Stockholm Institute for Scandinavian Law

[xxxi]Secure privacy, 'What are the International Privacy Laws and how to comply with them?' (*Secure Privacy*, 27 September 2021) <https://secureprivacy.ai/blog/what-are-the-international-privacy-laws#:~:text=The%20most%20prominent%20examples%20of,Act%20of%20Canada%20(PIPEDA).> accessed 7 September 2022

[xxxii]McKay Cunningham, 'Complying with International Data Protection Law' [2018] 84(2) University of Cincinnati Law Review

[xxxiii]Secure privacy, 'What are the International Privacy Laws and how to comply with them?' (*Secure Privacy*, 27 September 2021) <https://secureprivacy.ai/blog/what-are-the-international-privacy-laws#:~:text=The%20most%20prominent%20examples%20of,Act%20of%20Canada%20(PIPEDA).> accessed 7 September 2022

[xxxiv]Secure privacy, 'What are the International Privacy Laws and how to comply with them?' (*Secure Privacy*, 27 September 2021) <https://secureprivacy.ai/blog/what-are-the-international-privacy-laws#:~:text=The%20most%20prominent%20examples%20of,Act%20of%20Canada%20(PIPEDA).> accessed 7 September 2022

[xxxv]UcheVal Obi, 'An Extensive Article On Data Privacy and Data Protection Law in Nigeria' (*International Network of Privacy Law Professionals*, 9th September 2020) <https://inplp.com/latest-news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria/#:~:text=The%20right%20to%20data%20privacy,from%20corruption%2C%20compromise%20or%20loss.> accessed 7 September 2022

[xxxvi]Emeka Ekweozor, 'An Analysis of the Data Privacy and Protection Laws in Nigeria'(June 30, 2020) < https://ssrn.com/abstract=3639129> accessed 10th September 2022.

[xxxvii]Philip E. Agre and Marc Rotenberg, Technology and Privacy: The New Landscape (2nd edn, MIT Press 2001)

[xxxviii]Andrada Coos, 'How Can Telecom Companies Reduce Data Security Risks' (Endpoint Protector, 23 November) <https://www.endpointprotector.com/blog/reducing-data-security-risks-in-the-telecom-industry/> accessed 8 September 2022

[xxxix]Umar Danbatta, 'Regulators Perspective on Personal Data and Privacy of Users' (*Nigerian Communications Commission*, 22 October 2015) <chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ncc.gov.ng/accessible/documents/721-regulators perspective-on-personal-data-and-privacy-of-users/file> accessed 12 September 2022

[xl]AA Elgujja, 'A synopsis on data protection under the Nigerian laws : has the universality of right to privacy trickled down to Nigeria?' [2020] 1(1) University of Salford < http://usir.salford.ac.uk/id/eprint/60203/> accessed 7 September 2022

[xli]Emeka Ekweozor, 'An Analysis of the Data Privacy and Protection Laws in Nigeria'(June 30, 2020) < https://ssrn.com/abstract=3639129> accessed 10th September 2022.