Preorcjah Vol. 9, 2024
https://ezenwaohaetorc.org

Developing a consolidated legal framework for Nigerian e-commerce landscape

Onyeka Christiana Aduma
Department of Clinical Legal Education
Faculty of Law, Nnamdi Azikiwe University, Awka
Anambra State, Nigeria

Abstract

The rapid development of information technology over the past decades has had a drastic impact on the business environment. E-commerce has transformed the way businesses operate by providing a more efficient and convenient way to conduct transactions. E-commerce is therefore the use of the internet for marketing, identification, payment, delivery and customer service for goods and services. Through the e-commerce technology, the internet has revolutionized the way businesses transact by providing customers with the ability to bank, invest, purchase, distribute, communicate, explore and research from virtually anywhere and anytime provided there is internet access. In essence, through the internet and information and communication technologies, businesses can reach consumers who otherwise would have never known about or had access to certain products and/or services. This paper is anchored on the innovation diffusion theory and adopts doctrinal research methodology. Primary sources of data include statutes, case law and regulations while secondary sources include textbooks, internet materials, law journals, encyclopedias, and treatises. These sources are used to analyze the current legal frameworks regulating e-commerce in Nigeria and it is discovered that there is no consolidated legal

framework for e-commerce in Nigeria. Instead, e-commerce activities are regulated by several different laws. These laws are generally applicable, rather than being specific to e-commerce. As a result, they lack the level of clarity and predictability needed to effectively regulate e-commerce. This paper recommends among others, the development of a consolidated legal framework that takes into account the diverse nature of the country's e-commerce landscape.

***Keywords**: consolidated, develop, e-commerce, legal framework, Nigeria*

Introduction

The development of internet has resulted to the shift of commercial transactions from traditional face-to-face, physical trading practices, to a more advanced form of trading through electronic means facilitated by the internet. Indeed, by means of the internet and information and communication technologies, businesses are conducted between parties from different parts of the world who may never see themselves in their lifetimes (Nuruddeen, 2011). Thus, e-commerce is rapidly growing globally as consumers can now make online purchases of goods and services from the comfort of their homes and offices (Omar & Anas, 2014). Moreover, the global Covid-19 pandemic forced many companies to shift their business focus to the online environment, as restrictions and rules prevented them from carrying out their usual business activities. While many restrictions have been lifted, many companies continue to reap the benefits of e-commerce. Furthermore, many see e-commerce as an opportunity for developing economies to gain a stronger foothold in the multilateral trading system. This is because e-commerce can play an instrumental role in helping

developing nations like Nigeria reap the benefits of trade (Ugwu & Ogbo, 2021).

Indeed, e-commerce has experienced tremendous growth and has become the backbone of contemporary economic and financial transactions, as well as the preferred choice for many traders and consumers. It not only offers access to national e-stores but also provides access to cross-border markets, eliminating the barriers of international borders. However, this increase has also brought with it a number of legal and socio-economic issues, including a lack of consolidated legal framework to protect consumers, as well as issues concerning the rights and bargaining powers of the consumers in Nigeria. Also, many businesses and consumers remain wary of conducting extensive business over the internet due to the lack of a predictable legal environment governing transactions. This is especially true for international commercial activity, where concerns about enforcement of contracts, liability, intellectual property protection, privacy, security, and other matters have caused businesses and consumers to be cautious. Additionally, most of the statutes addressing legal issues related to e-commerce in Nigeria are still at the draft bill stage. Therefore, despite the growth of e-commerce, there is no consolidated legal framework on e-commerce in Nigeria. The legal issues concerning e-commerce activities are regulated by different laws, which are general and lack the level of clarity and predictability required for e-commerce in Nigeria. Thus, the growing importance of e-commerce in Nigeria has therefore necessitated the need for the development of a consolidated legal framework for Nigerian e-commerce landscape.

The concept of e-commerce

There is no universal definition of e-commerce but some scholars have offered useful descriptions. For example, Chaffey (2003) defines e-commerce as the buying, selling and even advertisement of goods and services electronically via the internet. In this model, the internet provides a direct connection between the trader and the buyer, so the parties do not need to meet face to face. E-Commerce automates manual processes, which has the potential to transform how businesses operate. Moreover, the United Kingdom Cabinet Office defines e-commerce as the exchange of information across electronic networks at any stage in the supply chain. It includes information exchanged within organization, between businesses, between businesses and consumers, and between the public and private sectors. This exchange can be paid or unpaid (Ogundele, 2018). This definition includes the two major business models for e-commerce transactions in Nigeria; business-to-business (B2B) and business-to-consumers (B2C).

The key distinguishing feature between e-commerce and other commercial transactions is the electronic element. This is not just limited to the actual buying and selling, but includes pre-sale and post-sale activities (Filani & Aina, 2020). Therefore, the purchase of goods or services is ordered by those methods, but the payment and delivery may be conducted offline. Müller-Hagedorn (2000) supports this definition, adding that an e-commerce transaction does not have to be fully electronic.

E-commerce enables businesses to sell products without opening a physical shop, which means it can operate without the limitations of a traditional store and thus available to customers 24/7. It enables businesses to establish a global presence, which is particularly valuable for small and newly established companies who want to engage in cross-border trade. E-commerce plays a critical role in today's global community. It enables consumers to

have access to goods and services from anywhere in the world without having to see the sellers in person (Akomolede, 2008). E-commerce has had a significant impact on the foundations of trade. It has brought numerous benefits to individuals and businesses. Many goods and services are now bought and sold online, and some are even entirely virtual. There is no physical or tangible equivalent to these virtual goods and services (Ogundele, 2018).

The legal framework for e-commerce in Nigeria

E-commerce is not specifically regulated under Nigeria's legal system. However, its legal issues are covered by a variety of laws. These include laws on cybercrime, consumer protection, electronic signature and data protection.

Federal Competition and Consumer Protection Act, 2019

The Federal Competition and Consumer Protection Act, 2019 repealed the Consumer Protection Council Act of 1992. FCCPA established the Federal Competition and Consumer Protection Commission and the Competition and Consumer Protection Tribunal. These organizations were established to enforce the provisions of FCCPA. (FCCPA 2019, sections 3& 39). FCCPA aims to promote and maintain competitive markets in the Nigerian economy. It does this by prohibiting restrictive agreements and the abuse of a dominant position. The FCCPA also aims to protect and promote the interests and welfare of consumers by providing consumers with a wider variety of quality products at competitive prices. The rights and protections afforded the consumers under the FCCPA are more defined and comprehensive than those under the repealed Consumer Protection Council Act (Eze & Ogbonna, 2021). The FCCPA provides a long list of rights for the protection of consumers as well as how to enforce these rights (FCCPA,

sections 114 – 134). However, the FCCPA does not address the specific challenges of online consumers. For example, it does not address the right of delivery, data protection, unfair contractual terms and payment method. As a result, the unique rights of e-consumers are yet to be accorded full recognition as a species of consumer rights, under Nigeria's primary consumer protection regime. This is contrary to the United Nations Guidelines for Consumer Protection, which stipulates that the legitimate needs of the Guidelines include the provision of a level of protection for consumers using electronic commerce that is not less than that afforded in other forms of commerce. It also aims to protect consumer privacy and the global free flow of information (Article III Rule 5 paras (j) and (k) of the Guidelines). However, Nigeria's primary consumer protection regime does not currently meet these needs.

The Cybercrimes (prohibition and prevention) Act, 2015

The Nigerian Cybercrimes (Prohibition and Prevention) Act, 2015 provides the legal framework for detecting, preventing and punishing cybercrime in Nigeria. The Act also aims to protect computer systems, electronic communication and privacy (section 1 of the Cybercrimes Act). The increase in cybercrime is directly related to the proliferation of commerce on the internet. This has attracted parties who seek to take advantage of e-commerce for their own gain. The Act covers a range of issues related to e-commerce, including cyber fraud and cyber bullying. However, one of the most significant provisions is the one on electronic signature. According to the Cybercrimes Act, electronic signatures are considered legally binding when purchasing goods or engaging in other transactions (*Ibid,* section 17). If the authenticity of the signature is ever called into question, the burden of proof lies with

the person contesting the signature. They must prove that the signature does not belong to the purported originator (*Ibid*). In addition to protecting consumers, the Act also obligates businesses to report cyber threats (*Ibid* section 21). Thus, any organization operating a computer system or network must immediately notify the National Computer Emergency Response Team (National **CERT**) of any attacks, intrusions and other disruptions that could impact another computer system or network. The National CERT can then take steps to address the issue, such as isolating impacted system until the problem is resolved. (Olubanwo & Oguntuase, 2019). Failure to report a cyber threat within 7 days can result in a penalty of service denial and a mandatory payment of N2 Million Naira into the National Cyber Security Fund (**NCSF**). This fund is used to address national cyber security challenges.

Moreover, financial institutions are required to verify the identity of their customers before conducting electronic transactions, such as transfers, payments, debits and issuances. (*Ibid*, section 37). Failure to identify the identities of customers before executing electronic transactions is a violation that carries a fine of up to N5 Million Naira. If a financial institution makes an unauthorized debit from a customer's account, the money must be refunded within 72 hours (*Ibid*). Service providers are required to share subscriber information and traffic data with relevant authorities and law enforcement agents when requested. This information must be protected and retained as required by law. (*Ibid*, section 38). Indeed, the Cybercrime Act has criminalized certain online fraudulent activities done that were not previously defined as crimes in the Nigeria's regular criminal laws. The Act creates both individual and corporate liabilities and penalties. It also created the Office of the National Security Adviser (NSA) as

the central authority for enforcing the law. While this framework is an important step in protecting consumers online, it does not currently address all the specific challenges faced by e-consumers.

The Evidence Act, 2011

Electronic commerce has raised evidentiary issues in relation to transactions done online. Prior to the Evidence Act 2011, electronic or computer-generated documents was not recognized as evidence under Nigerian law. The admissibility of such evidence depended on whether it fulfilled the general requirements for documentary evidence. (Evidence Act, Cap. E14, Laws of the Federation of Nigeria, 2004) In addition, it was challenging to prove the authenticity of an electronic signature on any computer or online print-out of contractual terms as well as the identity of the person signing.

The Evidence Act of 2011 significantly improved upon the previous legislation by recognizing computer generated evidence and electronic signatures. Sections 84 and 93 of the New Evidence Act address the admissibility of computer- generated documents and the recognition of electronic signatures. Section 84 of the Act contains the criteria for the admissibility of the computer-generated evidence. To be admissible, electronic evidence must meet the requirements outlined in section 84. In fact, the admissibility of a computer-generated document or a document downloaded from the internet is governed by sections 84 of the Evidence Act. The Supreme Court examined sections 84, 34 (1) (b) and 258 of the Evidence Act, 2011 in *Dickson v Kubor*,(2013) to clarify the concept of computer generated documents and held thus:

> There is no evidence on record to show that the appellants in tendering exhibits "D" and "L" satisfied any of the above conditions. In fact, they did not as the documents were tendered and admitted from the bar. No witness testified before tendering the documents so there was no opportunity to lay the necessary foundations for their admissions as e-documents under section 84 of the Evidence Act, 2011. No wonder therefore that the lower court held at page 838 of the record thus: 'A party that seeks to tender in evidence computer generated documents needs to do more than just tendering same from the bar. Evidence in relation to the use of the computer must be called to establish the conditions set out under section 84 (2) of the Evidence Act, 2011.

Similarly, the Court of Appeal in the case of *Akeredolu & Anor v Mimiko & Ors* (2013), held thus:

> Going by the foregoing provision, it is discernible that the appellants who were desirous of demonstrating electronically the content of Exhibit P50A and P50B failed to lay the necessary foundation regarding the condition of the electronic gadget or computer they were going to use. To the extent that those conditions as spelt out in section 84 (*supra)* were unfulfilled, the demonstration ought not to be allowed. The said conditions stipulated in section 84 of the Evidence Act are:

(a) that the document containing the statement was produced by a computer during a period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period, whether for profit or not by anybody, whether corporate or not, or by any individual;
(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;
(c) that throughout the material part of that period the computer was operating properly or, if not, that in any respect in which it was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its content; and
(d) that the information contained in the statement reproduces or in derived from information supplied to the computer in the ordinary course of those activities.

The conditions for admissibility of electronic evidence under section 84 of the Evidence Act are mandatory. The Evidence Act also recognizes that an electronic signature is sufficient to identify a person and fulfill the requirements for a handwritten signature (section 93(2)(3), Evidence Act, 2011). Thus, for the purpose of establishing proof of electronic signatures, the use of a password, identification, user names etc. may suffice.

The Data Protection Act, 2023

The Data Protection Act provides a framework for the regulation of personal data processing (Section 1 of the Data Protection Act). The purpose of the Act is to protect individuals' personal information from unauthorized access, fraud, and identity theft. Improved data security contributes to a safe digital environment, which fosters trust and increases e-commerce transactions. The Data Protection Act establishes the Nigeria Data Protection Commission as an independent body with perpetual succession and a common seal. The Commission is tasked with regulating data protection matters and enforcing compliance with the Act (*Ibid*, section 4). Section 24 of the Act outlines the principles that must be followed when processing personal data. The Act requires that data subjects give their consent to the processing of their personal data. The consent must be given freely and intentionally for the specific purpose or purposes for which the data is processed (*Ibid*, section 25 (1). The Act has specific consent requirements for children and persons lacking legal capacity. In such cases, consent must be obtained explicitly from parents or legal guardians.

The Act places significant emphasis on the rights of data subjects, particularly their rights to be informed about the processing of their data. (*Ibid*, section 27). In addition to the rights of data subjects, the Act also places legal obligations on data controllers and processors. They must ensure the security, integrity and confidentiality of personal data in their possession or under their control (*Ibid*, section 39). To meet the Act requirements, a data controller must implement appropriate technical and organizational measures. This includes protections against accidental or unlawful destruction, loss, misuse, alteration, and unauthorized disclosure or access (*Ibid*).The Data Protection Act also establishes a legal framework for cross-border data transfers.

This ensures that personal data is adequately protected when it leaves Nigerian borders (*Ibid*, section 41). The Nigeria data Protection Act 2023 is indeed a very important piece of legislation. However, there are some concerns about the effectiveness of the Act. For example, the Act does not cover all aspects of data protection, such as the issue of data portability, data retention et cetera. The Act requires data controllers and processors to implement appropriate technical and organizational measures to ensure the security of personal data. However, the Act does not specify what these measures should be or how businesses should assess whether they are appropriate.

Electronic Transactions Bill, 2015

The Electronic Transactions Bill was modeled on the UNCITRAL Model Law on e-commerce 1996. This ensures that member states have uniform and acceptable standard for electronic commerce practices (Nurudden et al, 2016). The Model Law encouraged member states to enact laws that are substantially similar to its. The Electronic Transactions Bill contains provisions on electronic signatures, data protection and electronic contract (Part III, IV, V of the Bill). It validates electronic signatures. (Section 11 of the Bill). Section 26 (2) of the Bill states that the mere fact that an electronic document was used in a contract's formation does not deny its validity or enforceability. In other words, an electronic contract is just as valid and enforceable as a traditional contract. The Bill protects consumers by requiring vendors and service providers to provide sufficient and relevant information; capable of being saved or printed by the consumer, and in a language the consumer understands (section 33 of the Bill). The information must be displayed conspicuously at appropriate stages of the consumer's decision making. This includes before the consumer

confirms transactions or provides any personal information (*Ibid*). A service provider or vendor must ensure that their marketing practices and information are current, accurate and not misleading to consumers (*Ibid*). This provision also protects consumers from unfair terms in standard form contracts. The writer is of the view that with this provision, online traders are now obligated to provide sufficient and correct information about the product they advertise. While this provision may offer some protection for consumers, it does not explicitly empower them to challenge the validity of standard terms in online contracts. This means that some online contracts may still be procedurally or substantively unfair. Section 33 of the Bill requires service providers and vendors to clearly identify themselves and provide information about their business policies and practices. This includes inquiry, complaint and claim procedures, warranties and other support services related to their goods or services. This is meant to prevent electronic transactions fraud and protect consumers. The information that must be provided before a transaction can take place includes a description of the goods or services, the quantity to be purchased, the full price, applicable currency, any shipping charges, taxes and specific reference to any other charges (*Ibid*).The writer is therefore of the view that the purpose of these obligations is to ensure that consumers have full information about the identity of the service provider or vendor, the nature of the goods or services and any associated costs. This enables consumers to make an informed decision about the proposed electronic transaction. These obligations will also help prevent misleading product information on some e-commerce platforms which can give customers more confidence to transact online. This confidence is essential for a successful e-commerce market.

Section 34 of the Bill also requires that the service provider or vendor must allow the consumer to correct or cancel an order before it is accepted or processed. The bill also makes provision for the protection of consumers' data. It requires that service providers or vendors keep the personal data of consumers confidential and make their privacy policies public and easily accessible. Unlike the South African Electronic Communications and Transactions Act 2002, however, the Bill does not address payments procedure or the period of execution of an order. The South African Electronic Communication Transactions Act provides for cooling-off periods, which allows consumer to terminate an agreement within a reasonable time after a transaction (ECT, section 44).This can be useful when "buyer's regret" sets in or when a consumer has had a chance to reflect on the transaction, or get independent advice. It is important to note that the Electronic Transactions Bill does not have any "cooling off" period provisions. This is a significant difference between the Bill and the South African ECT Act.

The Bill (section 43) allows regulatory authorities to make regulations for facilitating its provisions. However, it does not specify authority for implementing or enforcing its provisions or any dispute resolution mechanisms. It's definitely important to consider the potential for confusion about which agency is responsible for enforcing the Bill's provisions. In contrast, the Malaysian Consumer Protection Act provides e-consumers with a fast and inexpensive means of settling disputes. Consumers who are dissatisfied with online dealings can file their claims in the Tribunal for Consumer Claims (TCC). Lodging a complaint before the TCC is free and parties are free to settle their differences on their own. Otherwise, a proper hearing is conducted, but neither of

the parties is allowed to be represented by its full time employed lawyer (Nuruddeen et al, 2016)).

Indeed, the Electronic Transactions Bill contains provisions on the protection of e-consumers, but some important area are missing, such as provisions on the time of delivery, provisions on unfair trade practices, provisions on the institutional framework for regulating electronic transactions, provisions on dispute resolution mechanisms, and provisions on remedies available to consumers. The absence of these provisions could reduce consumer interest in e-commerce since they may not have legal recourse if their rights are violated.

Challenges of e-commerce

E-commerce in Nigeria faces certain challenges that negatively impact its growth and development from technological problems to legal issues. Some of these legal issues are:

Inadequacy of legal framework

The existing legal frameworks are quite inadequate to address the e-commerce legal issues in Nigeria. In fact, (Ahmadu, 2010) described the existing Nigeria's legal framework for e-commerce as "a sketchy picture of the semblance of a legal environment." Without adequate legal framework, it is difficult to regulate and protect consumers, businesses and other stakeholders involved in e-commerce. In addition, it is also difficult to address some of the unique challenges and issues that arise from e-commerce transactions. For example, issues such as cross-border transactions, consumer protection and data protection can be difficult to regulate without adequate legal framework. This can lead to legal uncertainty, which can discourage businesses and consumers from engaging in e-commerce. Nigeria needs an adequate legislation

that will protect e-commerce businesses and consumers to drive growth and boost opportunities in the sector (Nwokpoku, 2014).

Formation of online contracts

The determination of the moment when a contract can be said to have come into existence on the internet is one of the issues in e-commerce. The question is at what point can an offer be made with regards to online transaction or how to differentiate between invitation to treat and offer in an online transaction, at what point can it be said that an intention to enter legal relation is made? In traditional commerce, an offer is an undertaking made by one party to the other with the intention that such an offer becomes binding on the other party when he accepts. Such an offer should be precise and clear; also, it can be made to one person or the entire world. However, where there is no intention to be bound by that offer, such an undertaking would be considered an invitation to treat. For example, the display of goods in a physical shop is usually viewed as an invitation to treat. Thus, when the consumer picks up the item, this is considered to be the offer. The cashier accepts the offer by collecting the money and issues a receipt as proof of the contract. However, in e-commerce, the display and actual sale of the goods are often combined; it then becomes difficult to determine what constitutes an offer and which party makes the offer. Apart from displaying items, there is also the controversial issue of whether web advertisements amount to offers or invitations to treat (Talabi, 2021). For instance, in the case of contracts concluded by e-mail one of the major issues is timing i.e. to ascertain when the contract has been accepted, this would in turn foreclose the possibility for the offeror to retract his offer. One position which follows a rule known as the postal rule is to say that the contract is deemed to have been formed once the email has been

sent. The other rule known as the communication rule makes receipt of email the touchstone. The second rule in particular gets more complicated because e-mails can be misaddressed or delayed by any server on the way, and may not even be delivered or read until sometime after their delivery. It may thus be difficult to know when an e-mail was actually read, to determine when an offer was made or acceptance communicated. Again, would receipt be the time of receipt by the server, the time of delivery from the server to the addressee's email account or the opening of the email by the addressee (Idigbe, 2010). Thus, according to Gringas & Nabarro (1998), the best practice legally is to make any offer by e-mail subject to a date on which the offer will lapse. An objective date and time must be specified. If no intention is shown as to the lifespan of the offer, the courts would imply that the offer lapses after a reasonable time.

Jurisdiction and choice of law issues

The issue of jurisdiction is a very important one in e-commerce because several countries with various legal systems are typically involved in a single transaction. The question has always been which court assumes jurisdiction in resolving a dispute between parties arising from an e-commerce transaction and also the law that is to be applied by that court, in view of the fact that the parties may be residing in different jurisdictions with different legal systems. Is it the law of the place of residence of the defendant? Or the law of the place of performance or principal place of business of the defendants. The issue basically is one of Private International Law, and the relevant Convention is the Brussels Convention on Jurisdiction and Enforcement of Judgment in Civil and Commercial Matters (Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial

Matters 1958). The Convention is applicable to those countries that have ratified it and incorporated its provisions into their municipal laws.

Thus, with respect to internet contracts, the general rule is that jurisdiction is determined by reference to the place or country where the contract is performed and where there are many jurisdictions where the contract is performed, the relevant jurisdiction is the jurisdiction where the dispute arises (Akomolede, 2008). The place of domicile may also determine the court that will have jurisdiction. Thus, where the parties are domiciled in a contracting state under the Brussels Convention, the rules of the Convention are applicable, while the rules of common law are applicable where the parties are not domiciled within a contracting state. Also, a person's domicile must be assessed from the state's legal perspective to determine whether or not he is domiciled in a contracting state. For instance, internet contracts made in the UK, the provisions of section 41(7) of the Civil Jurisdiction and Judgment Act 1982 are applied to determine whether the defendant is domiciled outside the contracting state (*Ibid*).

Conversely, in relation to consumer products, the consumers are allowed to sue and be sued in their home states (Articles 13 and 14 of the Brussels Convention). Also, in case of email contract, the postal rule is inapplicable and the place where the e-mail contract is made is the acceptor's place, and that is the relevant place for purpose of jurisdictions (Denning LJ, in *Entores v Miles Far East Corporation*, 1953).

Indeed, a corollary of the issue of jurisdiction in e-commerce is the choice of law to be applicable in disputes arising from contracts concluded over the internet. The complexities and trans-national nature of the internet make it difficult to apply the rule of

a single jurisdiction (Talabi, 2021). Moreover, it is often impossible to determine which country's law is the most appropriate law to be used. Consequently, the principles of private international law will be applied where these difficulties arise (*Ibid*). However, in practice, companies try to avoid the complexities of applying the principles of private international law by inserting the jurisdiction and choice of law clauses in the standard electronic contracts provided by them.

Data protection and privacy

Trading on the internet is made through transmission of electronic data from e-traders to e-consumers and vice versa. Hence, given the openness and accessibility of the internet, the protection of data and privacy has been a source of concern for internet users (Akomolede, 2008). Protection of such data is a significant issue because any information fed into the internet could be accessed anywhere in the world by other persons using the internet. Without adequate laws in place, this data can be misused or exploited, which can cause harm to consumers and business. One of such harm is the risk of identity theft and fraud since e- commerce transactions involve the sharing of personal information like names, addresses and credit card numbers. Privacy issues have therefore become one of the most significant threats facing e-commerce in Nigeria. This was lucidly captured by Lord Hoffman in the case of *R v Brown (*1996) as follows:

> Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people

that certain things are none of their business is under technological threat.

Thus, different approaches to data privacy and protection are found in different countries such as self-regulation approach, as used in the United States and the government approach, as used in the United Kingdom (Adelola, 2015). Nigeria adopted the government approach via its Data Protection Act, 2023. Perhaps, the Nigerian data protection Act is not adequate with respect to the protection of the data of e- consumers. There is lack of provisions governing the use of cookies and other tracking technologies. Cookies and other tracking technologies are often used by websites to collect information about users, including their browsing habits and personal preferences. Without adequate regulations, consumers may not be aware of how their information is being collected and used. Also, there is also absence of provisions for specific courts with jurisdiction over data protection in the Nigerian Data Protection Act 2023. The writer is of the view that provisions for a specific court with the jurisdiction to adjudicate on data protection and privacy-related subjects in the Nigerian Data Protection Act 2023 are fundamental to achieving the objectives of the Nigeria Data Protection Act 2023 and safeguarding the personal data and privacy of the Nigerian citizens. In addition to this, Section 60 of the Data Protection Act, which provides to the effect that the Minister may give to the Commission directives of a general nature and that the Commission shall comply with the directives contradicts Section 7 of the Act, which clearly provides that the Commission shall be independent in the performance of its functions under this Act. Without adequate data protection and privacy laws, consumers may be reluctant to engage in e-

commerce transactions, fearing that their personal information could be misused. This can limit the growth of e-commerce.

Payment system and cyber crimes

Goods and services bought or supplied through the internet can be paid for through the internet in the same way that the internet can be used to make offers and accept offers. Payment for goods and services bought through the internet can therefore be made by the use of credit cards, smart cards, digital or electronic cheques or cash and debit cards and such payment therefore pose unique problems because of the more vulnerable they are to attack and the inability of the internet to guarantee the safety of such payments (Idigbe, 2010). Also, there is possibility of duplicating payment, since a computer could potentially become a forger of digital banknotes. (Ibid). Thus, the existing legal framework does not specifically address the issue of electronic payment. This means that there is no specific legal framework that governs the use of electronic payment methods. This lack of legal clarity can lead to uncertainty and risk for consumers and businesses ranging from PIN theft, data privacy breaches, financial loss due to technical failures to outright manipulation of software program for criminal purposes. This crime otherwise known as cyber crime has also pose many challenges to electronic commerce and have indeed made internet transactions insecure and vulnerable to manipulation by persons who are not parties to such transactions. The security of the transaction is the core and key issue in the development of e-commerce and e-commerce security provides the security of assets of e-commerce from illegal access, use, modification, or damage (Akinola & Asaolu, 2023). Cyber security therefore remains an area of deep concern in the Nigerian e-commerce landscape.

Evidential issues in e-commerce in Nigeria

The emergence of e-commerce and its growing popularity has provoked fundamental evidential issues especially in relation to the proof of transactions conducted through the internet. Relevancy and admissibility are the twin concepts central to the Nigerian law of evidence (Osipitan, 1995). It then means that for a piece of evidence to be admissible, it primarily must be shown that the piece of evidence is either a relevant fact and is in issue, or in the alternative, the fact must be that which is relevant to a fact in issue (*Abubakar v Chuks* 2008). However, one of the greatest challenges facing the courts in Nigeria is the admissibility of computer-generated evidence, in view of the rule that a party must give the best evidence of facts that are in issue before the courts (This is known as "The Best Evidence Rule" and is contained in Section 77 of the Nigerian Evidence Act). Indeed, with respect to electronic evidence, the major obstacle is the question of which method is to be used in the proof of the content of this specie of evidence; that is, whether the content of the aforementioned evidence is to be proved by either primary or secondary evidence. Prior to the 2011 amendment of the Evidence Act, the validity of contracts, including commercial agreements, were repeatedly challenged in court. The argument was usually that the law as it was then did not recognize the validity of any contract or agreement entered into via the aid of technology, computers and the internet because there was no existing procedure for the recognition of electronically generated evidence. However, this controversy was put to rest by the provisions of Section 84 of the Evidence Act 2011, which provides the criteria for the admissibility of computer-generated evidence.

The need for a consolidated legal framework for Nigerian e-commerce landscape

There is no gainsaying that with e-commerce people can now conduct business without the barriers of time or distance. Consumers can now shop online from the comfort of their homes and offices, at any time of the day or night, anywhere in the world. Consumers do not need to physically visit stores; they can browse and compare prices on countless products within minutes, and order nearly anything they want. (Omar & Anas). While e-commerce offers many benefits, it also presents challenges in terms of legal protection for consumers. Consumers concern in Nigeria face several challenges with e-commerce. These include lack of adequate legal framework, concern about payment security of payment and the validity and enforceability of electronic contracts. In addition, there is a problem with e-traders not providing enough information and engaging in unfair trade practices. Consumers who order online sometimes face several problems such as receiving incorrect or defective goods. In some cases, they do not receive the items they ordered at all. This can happen even after they have paid for the goods through their credit or debit cards. (Nuruddeen et al, 2016). E-consumers in Nigeria also face the challenges of being in an unequal bargaining position with e-traders. Other countries have taken steps to address the problems of unequal bargaining powers and unfair trade practices. For example, Part IIIA of the Consumer Protection Act (amended) Act 2010 in Malaysia deals specifically with unfair contract terms. The Consumer Protection Act (amended) in Malaysia allows consumers to challenge unfair terms in standard form contracts. This gives consumers more power to defend their rights, unlike in Nigeria

In the European countries, consumers are not bound by terms of a contract that have been individually negotiated. This includes terms that are contrary to the requirement of good faith, or that creates a significant imbalance in the parties' rights and obligations (Tiwalade et al, 2014). Thus, regulating e-commerce is essential to protect consumers from exploitation. However, Nigeria's current laws on e-commerce are scattered in different pieces of legislation, making it difficult to address the specific needs of online consumers. It is therefore importance for Nigeria to develop a single, consolidated legal framework to govern the emerging e-commerce regime. This would ensure a more coherent and comprehensive approach to regulating e-commerce.

Conclusion and recommendations

The paper examines the need for a consolidated legal framework to regulate e-commerce in Nigeria and discovers that there is no single, consolidated law on e-commerce in Nigeria. Instead, different aspects of the legal framework including consumer protection, electronic contracts, electronic signatures, cybercrimes, payments and data protection are covered by various laws. However, these laws do not adequately address the unique issues arising from e-commerce in Nigeria. In addition, other relevant laws on e-commerce are still in the draft stage. As a result, Nigeria does not have a consolidated legal framework for the e-commerce landscape. This lack of a unified legal framework has harmed consumers' confidence in e-commerce. In order to facilitate the growth of e-commerce in Nigeria, it's crucial to build consumer confidence. Consumer protection plays a key role in driving this confidence. The writer recommends the development of a

consolidated legal framework in Nigeria. This framework should provide the necessary clarity, predictability and protection to support the growth of e-commerce. Special courts should be established to address the grievances of e-consumers. Access to effective justice is the key to enforcing the rights of e-consumers. In addition to establishing special courts, the law should also establish a single, centralized authority to oversee e-commerce. These bodies would have the necessary expertise to properly regulate this complex and fast-changing industry. Provisions for online dispute resolution mechanisms since e-commerce is borderless, online dispute resolution allow consumers and businesses to resolve dispute quickly and efficiently without the need for in-person meetings or travel. This can help to improve the user experience and build trust in e-commerce. The public must also be educated on the laws and regulations that protect them as e-consumers.

References

Adebola, A.J. & Adebowale, O. (2022). Analytical Review of E-Commerce Business Models. 5(2) *African Journal of Accounting and Financial Research* 5 (2), 48-60.

Ahmadu, M.1. (2022). Information and Consumer technology in Nigeria: Some Lessons on the law and Practice of Electronic Commerce in 12th professorial Inaugural Lecture, Sokoto, Nigeria, 1-14.

O Akinola, O. & Asaolu, O. (2023) . A Trust, Privacy and Security Model for E- Commerce in Nigeria, Nigerian *Journal of Technology* 42 (1), 152-159.

Akomolede, T.I. (2008). Contemporary Issues in Electronic Commerce in Nigeria. PELJ 11(3), 1 – 25.

Chaffey, D. (2003). E-Business and E-Commerce Management (2nd ed.). England: Pearson Education Ltd.

Eze, U. G. & Ogbonna, O. M. (2021). An Evaluation of the Protection of Nigerian Consumers under the Federal Competition and Consumer Protection Commission Act. *IRLJ* 3 (3), 15.

Filani, A.O. & Aina, S.A.(2020). E- Commerce and Enforcement of Consumer Rights in Nigeria: Issues, Prospects and Challenges. *Journal of Law and Judicial System*, 3 (1) 1-15.

Gringas, G. & Nabarro, N. (1998). The Laws of the Internet, Retrieved from 249.https;//lib.urgent.be/catalog/rug01:000434120

Idigbe, C., Legal and Institutional Framework for E-Commerce in Nigeria. Retrieved from https://9jalegal.com.ng/downloads/Articles/Commercial%20transactions/cibn_paper_on_legal_institutional_framework_for_e_commerce-in_nigeria.pdf.

Kalakota, R. & Whinston, A. (1997). *Electronic Commerce: A Manager's Guide.* USA: Addison-Wesley.

Kumar, S., Marc Lim, W., Pandey, N., & Westland, J. C. (2021). 20 years of Electronic Commerce Research. *Electronic Commerce Research* (21) 1–40.

Muller-Hagedorn, L. (200). E-Commerce. United Kingdom: Alpha Science International Ltd.

Nuruddeen, M. (2011). An Appraisal of the Legal Requirements of Electronic Commerce Transactions in Nigeria, *Bayero University Journal of Public Law* 3 (1), 164–183.

Nuruddeen, M., Yusof, Y. & Abdulla, N. A.B. Legal Framework for E-commerce Transactions and Consumer Protection: A Comparative Study, Retrieved from

Ogundele, G. P. (2018). Developing Legal Framework for Electronic Commerce in Nigeria: Some Lessons from the UK and Singapore, Retrieved from https://papers.ssrn.com/so13/Delivery.cfm/SSRN_ID3719431_code2992951.pdf?abstractid=318.

Olubanwo, F. & Oguntuase, O. Milestone In Electronic Commerce: How The Cybercrime Act 2015. Retrieved from Impacts Businesses, https://www.mondaq.com/nigeria/security/788730/milestone-in-electronic-commerce-how-the-cybercrime-act-2015-impacts-businesses.

Omar, C. & Anas, T. (2014). E-Commerce in Malaysia: Development, Implementation and Challenges. *Irmbrjournal* 3 (1), 291–298.

Organisation for Economic Corporation and Development (1997). Report on Electronic Commerce: Oppportunities and Challenges for Government, 20.

Osipitan, T., (1995). Admissibility of Computer Printout under Nigerian Law of Evidence. *Lawyers' Bi-Annual* 2 (2), 236 - 239.

Tiwalade, A. Dawson,R., Batmaz, F. Privacy and Data Protection in E-commerce in Developing Nations: Evaluation of Different Data Protection Approaches, Reftrieved from https://core.ac.uk/download/pdf/288375411.pdf accessed 17/10/23.

Ugwu, C .C. & Ogbo, A. (2021). The Implications of Legal and Policy Frameworks for E-Commerce in Nigeria. *BN Bullion*, 45 (2), 73 – 80.

Case Laws

Abubakar v. Chuks (2008) 152 LRCN 1, 17).
Dickson v Kubor(2013) All FWLR (Pt. 676) 392 at 429
Entores v Miles Far East Corporation (1953)
R v Brown (1996) 1 All ER 545, 556

Legislation

Cybercrime (Prohibition, Prevention, Etc.) Act, 2015
Data Protection Act, 2023
Electronic Transactions Bill, 2015
Evidence Act 2011
Federal Competition and Consumer Protection Act, 2019

Onyeka Christiana Aduma is a lecturer in the Department of Clinical Legal Education, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.

