CHALLENGES AND PROSPECTS TO THE ADMISSIBILITY OF ELECTRONICALLY GENERATED EVIDENCE

JACOB OSARIEMEN ABUSOMWAN*

Abstract

We reside in an era dominated by electronic technologies, wherein every government institution, business, and industry, regardless of size, as well as personal relationships among families and friends, engage in interaction and communication via electronic mediums. Electronically generated evidence and computer forensics represent relatively recent additions to the array of evidentiary methods in our judicial processes. However, there are certain legal requirements that the collected electronic evidence must satisfy for it to be admissible. They include relevance, reliability and authenticity. Most times, computers are considered the repositories of essential digital evidence such that communications sent via E-mail or files on a computer can either make or mar a case. Although, the legal profession appreciation the value of electronic evidence, however, it has also sparked considerable and often controversial arguments most especially among legal professionals with regard to its authenticity. This paper seeks to critically explore the difficulties and potential outcomes linked with the acceptance of electronically generated evidence within the framework of the Nigerian legal system. In adopting the doctrinal method of research it was revealed the provision is not stringent enough to prevent abuses hence proffered recommendations, however, the newly amended Evidence (Amendment) Act, 2023 seems to have resolved the problems associated with it.

Keywords: Challenges, Prospects, Admissibility,Electronically, Generated and Evidence

* LLB, (Hons) (Uniben), BL, LL.M (AAU), Ph.D (IUO), Senior Lecturer, Department of Private and Property Law, College of law, Igbinedion University, Okada, abunsomwanventures1@gmail.com

1.0 Introduction

The law of evidence is the spine of our law. This assertion is in every ramification true as the law finds expression only in the evidence alluded to it. On this ground, therefore, every jurisdiction tends to have a uniform code on the rules of evidence. Thus, there is a radical evolution in the 21st century *vis-a-vis* Information Technology which makes the world now a digital world, where virtually all forms of man's activities are guided and aided by computers or any electronic machine. Nearly every facet of business relies on electronic communications, and transactions are concluded, documented, and reported through intricate computer technology platforms.Nearly every facet of business relies on electronic communications, and transactions are concluded, documented, and reported through intricate computer technology platforms. The adoption of computers and various types of electronic storage and communication systems has significantly surged in commercial and financial transactions within Nigeria[1].

Electronic evidence, it means evidence generated by some mechanical or electronic process. The utilisation of computers and other varieties of electronic storage and communication systems is swiftly supplanting the conventional approach to record-keeping and communication through written documents.

Electronic and computer-generated evidence serves as a comprehensive term encompassing specific categories of evidence that are processed, stored, or derived from computers, computer-based devices, or electronic communication systems. A primary attribute of these types of documents is their paperless nature, except in cases where they are printed. While existing within tangible objects, they remain visually perceptible yet intangible.These encompass a range of items such as diverse forms of bankers' books, emails, telephone records, text messages, digital photographs, mobile phones, letters, or any other documents processed through a computer or electronic device, and stored within computer-based storage systems[2].

---

[1] M.A Ajomale, A case for Legislative Control in Banking and Other Financial Malpractices in Nigeria; the emergence of computerized banking transaction , Malthouse Press, 1990, 45

[2] Hon. Justice Chinwe E lyizoba, Cybercrime: Challenges before *Judicial Officers.* Commentary presented at the All Nigerian Judges Conference 16-20 November 2009.

The passing of the Evidence Act of 2011marks a watershed in the evolution of our legal system. One major area where the current Act has introduced radical changes pertains to evidence generated electronically and produced by computers.

Electronic evidence is a fairly recent inclusion in the means for providing evidence within legal proceedings, this development also introduces another which is 'computer forensics. Computer forensics is still in its initial phases of development, leaving some questions unanswered, consequently giving rise to emerging issues that cast doubt on the credibility of computer forensics applications in Nigeria's legal systems. For practical considerations, the pertinent legal matters related to computer forensics encompass issues of evidence admissibility, adherence to standards and certifications, analysis procedures, and preservation practices. The conclusion is that electronically generated evidence must be both scientifically sound and legally relevant and admissible. This article, therefore, seeks to critically appraise the challenges and prospects posed by the admissibility of electronically generated evidence under the Nigerian legal system.

2.0 What Constitutes Electronically Generated Evidence?

The Evidence Act [3] expanded the definition of documents to include computer and electronically generated evidence. Section 258 of the Act however defined document to include:

a) Books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means intended to be used or which may be used for the purpose of recording that matter;
b) Any disk, tape, sound track or other device in which sounds or other data (not being visual images are) embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it;
c) Any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it; and
d) Any device by means of which information is recorded, stored or retrievable including computer output.

[3] S. 83 and S. 86(1) Evidence Act 2011.

Primary documentary evidence is the original document itself produced for the inspection of the court[4]. Secondary evidence is the direct opposite of primary evidence. It has long been a subject of debate whether computer print-outs should be accepted as primary or secondary evidence. Osipitan[5]believed that electronically produced evidence needs to be treated as primary evidence when presented in our courts and that such evidence is not to be admissible as secondary evidence. When several documents, however,are all generated through a consistent procedure, as seen in the instance of printing, photography, lithography[6], computer or other electronic or mechanical process, each of these documents will be considered as the primary evidence for the contents of all documents generated through this uniform process[7]. According to section 87 of the Act secondary evidence includes the following:

(a) Certified copies.
(b) Copies made from the original by mechanical means, e.g. photocopies
(c) Copies made from or compared with the original, e.g. handwritten or typewritten copies made from the original[8].
(d) Counterparts of a document as against the parties who did not exhibit it.
(e) Oral accounts of the contents of a document given by some person who has himself seen it.

To eschew the argument associated with the classification of evidence and the question of what constitutesan original copy in relation to electronic/computer-generated evidence, section 258 of the new Act defined what constitutes a copy of a document. By the section, a copy of a document includes:

---

[5]T. 0sipitan , Admissibility of Computer Print-Out under Nigerian Law, *Lawyer Bi-Annual vol. 2, No. 2,* (1995) 236-248.

[6]*Esso West Africa Inc. v. Oladiti*[1968] NMLR 453, where it was held that the process of printing, lithography and photography are not meant to be exhaustive of the whole process, but as examples of the uniform process intended. Where an agreement is typed in a draft form, each copy of the letter is primary evidence of the other copies including the top.

[7]Section 86(3(d) Evidence Act 2011.

[8] *Also see Esso West Africa v. Alli*[1968] NMLR P.414.

a) In the case of a document falling within paragraph (b) but not (c) of that definition of 'document' in this subsection, a transcript of the sounds or other data embodied in it;
b) In the case of a document falling within paragraph (b) but not (c) of that definition, a reproduction or still reproduction of the images embodied in it whether enlarged or not;
c) In the case of a document falling within both those paragraphs, such a transcript together with such a still reproduction; and
d) In the case of a document not falling within the said paragraph (c) of which a visual image is embodied in a document falling within that paragraph, a reproduction of the image, whether enlarged or not, and any reference to a copy of the material part of a document shall be construed accordingly.

The elucidation expressed in this section is quite appropriate as it saves the judiciary the worry of inquiring into whether a transcript or replayed audio or printed pictures, with or without negative qualifies as admissible secondary evidence. A careful look at sections 86 and 258 would clearly show that primary evidence refers to an original writing or recording itself, or any other equivalent intended to achieve the same purpose, executed or issued by the same individual[9]. In the same vein, the original of a photograph should encompass the negative or any print derived from it. Moreover, in cases where data is stored in a computer or comparable device, any printout or other output that can be read by sight and is demonstrated to accurately represent the data would be considered an original[10].

An electronic signature fulfils the legal prerequisite for a document to be signed, provided that the signature indicates that a process was adhered to wherein the individual executing a symbol or utilising another security procedure to confirm the authenticity of the signature to an electronic record, indeed followed such a prescribed procedure. Section 93(3) of the Evidence Act states that an electronic signature may be proved in any manner, including by showing that procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person. Agaba believed that the provision for electronic

[9]J. A .Agaba, *Practical Approach to Criminal Litigation in Nigeria: Pre-Trial and Trial Proceeding*, (1st ed., Abuja, Law Lords Publication, 2011) P.748.
[10]*Ibid*.

evidence is a welcome innovation as virtually every electronic transaction requires one form of identification or another[11].

However, the court must refrain from forming any assumptions regarding the recipient of such a message without the support of corroborative evidence[12]. The numerous condition precedents which the computer-generated documents must fulfil include, section 84(3) where the operation of storing and processing information for the duration of a period, necessary for the conduct of various activities consistently performed throughout that period as indicated in subsection (2) (a) of this section, was systematically executed by computers, whether-

(a) By a combination of computers operating over that period;
(b) By different computers operating in succession over that period;
(c) By different combinations of computers operating in succession over that period; or
(d) In any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer.[13]

3.0 Problems of Admissibility of Electronically Generated Evidence

Computer-generated records are qualitative and different from traditional paper records, thus, they are more vulnerable by their very origin, nature, mode of transmission, storage and usage, electronically generated evidence poses certain challenges when used in evidence. These challenges include issues bordering on authenticity, integrity and confidentiality of the pieces of evidence.

Hence, electronically generated materials do not readily lend themselves to the effective authenticity tests that are typically feasible with traditional documents. Consequently, the law insists that the party aiming to utilise it must present evidence that verifies the evidence's authenticity in terms of its source (origin) and content (what it represents). This practice is popularly

[11] J. A.Agaba (n- 9) 748.
[12] section 153(2) of the Evidence Act 2011.
[13] *Ibid*, Section 84 it is important to note that all the computers used for that purpose during that period shall be treated for such purpose and thus constitutes a single computer.

referred to as authentication. Authenticity primarily concerns the verification of whether the material or information indeed originated from the claimed source and accurately represents its intended content. In usual circumstances, when data is inputted into computer memory, an e-mail is sent or an order is placed for goods or services through the internet, the sender is unable to authenticate the information he has sent by way of a signature. It is the same if he speaks with another person on the telephone, leaves a message on that other person's voicemail or sends a text message (SMS). Even if he uses a password or an acronym, they may not be peculiar to him the way a signature written by him would be. The password or acronym can also be endorsed or used by anybody else who knows them far more easily than a signature can be imitated. A voice on the phone can also be imitated. In a workplace, anyone can input information into computer memory, claiming that it was entered by someone else. As a result, when a customer's account records are called up in a bank's computer system, there is hardly any way of knowing which person made such an entry. This makes it difficult to ascertain whether or not that person was an appropriate officer to make the entry. Even if one of several appropriate officers makes a wrong entry, it may not be traceable to him since he has not signed it, because there is no way he can sign it.

If such a deceptive entry or message is submitted to the court, it would be challenging to identify its falsity. The court can thus be easily misled. The existence of signatures on comparable non-electronic documents or materials enhances their authenticity and increases the difficulty of counterfeiting or imitation. Signatures of course can be forged on non-electronic documents, however, a court can assess an allegedly forged signature by comparing it with other signatures from the same individual and arrive at an informed judgment on the matter.

Section 84[14]raises many questions for determination.
The first question is: what is a *certificate*in the framework of *section 84(4) of the Act?* The Act did not define the word *certificate.* It is therefore unclear what a *certificate*is. Nonetheless, it is glaring from the provision that the authentication required here has to be in writing and not oral[15]. It is our view

[14]**Evidence Act 2011**
[15] **This view is supported by the fact that the section expressly mentioned certificate; and that the certificate has to be signed by a person occupying a responsible position in relation to the operation of the relevant device or**

that instead of ordinary written certificates, the use of affidavits should be adopted in the authentication. This is the practice in the majority of the jurisdictions consulted[16]and out of four jurisdictions consulted, it is only in America that the stance broadens the required authentication scope to encompass evidence beyond just an affidavit[17].

Secondly, is it only experts who are authorised to sign the certifying document? The Act stipulates that the certifying document should be *signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities.*

Obviously, it does not insist that only experts can sign the certificate. This view is in line with the position in other jurisdictions. In the English case of *R* v. *Dean*[18], it was argued on appeal that since there was no evidence of an expert that the naval computer databases in question were at the relevant time operating properly, the evidence on the searches on those bases generated from them was inadmissible as outlined in section 69 of the *Police and Criminal Evidence Act, 1984.* The Court of Appeal rejected this submission, holding that since there had been no known reported problems with the databases, an officer who had carried out the search was qualified to give evidence of the real ability or accuracy of the databases.

While we commend the liberal approach of the court, the point must, however, be made that each case must be considered in the light of its

---

management of the relevant activities. Has it envisaged oral authentication, it would not have required signing.

[16] For instance, in *DPPv. Mckeon* [1993] 1 E.L.L. E. R. 225, the English Court while interpreting *paragraph 8 schedule 3 of the United Kingdom Police and Criminal Evidence Act (in parimateria*section 84(4) of our Evidence Act) admitted a computer printout authenticated by a certificate, filled in the form of a standard statement on oath, which stated that to the best of the knowledge of the maker, the requirements of *section 69(1) of the Police and Criminal Evidence A ct. S. 3 of the South African Computer Evidence Act* which makes *authenticated computer print-out* admissible defines *authenticated*' to mean that the print-out must be accompanied by an authenticating affidavit or other supplementary affidavit necessary to establish the reliability of the information contained in the printout. Under *section 7 of the Canadian Uniform Electronic Evidence Act,* evidence may be given by way of affidavit to prove the authenticity of electronic records.

[17] See American Federal Rules of Evidence, 2014, Rule 109.

[18][1998] 2C.A.R. 171

peculiar circumstances. Situations may arise where only the evidence of an expert may suffice.

Thirdly, it is the requirement of section 84(4) that the authenticating certificate be *signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities.* What happens where the evidence sought to be authenticated is to be tendered against the interest of the person or company in charge of the computer? Since it is the person or employee of the company that will be required to sign the certificate, he may refuse to sign it or evendisown the electronic evidence.In such circumstances, the possible solution to this challenge would be for the party aiming to present the electronic evidence to issue a notice to produce, in line with section 89(a) of the Act, to the individual or entity declining to sign the authenticating certificate. Upon the failure of the person or company so served to sign and produce the authenticating certificate, the other party will then be at liberty to give evidence explaining the circumstances leading to his inability to accompany the electronic evidence with the authenticating certificate. It is hoped that when that is done, the court will admit the electronic evidence even though not authenticated as required by the section.

Lastly, The quality of the certificate issued pursuant to section 84(4) is further whittled down by the concluding phrase that *for the purpose of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.* This will give room for all kinds of quacks and mediocre to issue certificates to the best of their knowledge and belief. This will be quite unfortunate.

Defining the attributes of authentic records is generally associated with the 'wholeness and soundness' of the document. This is consistent with whether the document can be seen as a whole and unaltered. Conversely, integrity pertains to the record's state of being whole anduntouched. While this definition of '**integrity**'might relate to the capability to confirm that the content of a document remains unchanged from its initial composition, completion, and acceptance by the author (if the author is known, or remains anonymous for good reason).

Other pertinent aspects to contemplate encompass the utilisation of a time stamp, its accuracy assessment, and, if uncertainty arises, the adherence to the designated standards associated with the specific type of time stamp

employed; whether it is a document that has undergone partial writing; whether the integrity assessment should exclusively relate to the initial version or if it is also warranted to track the subsequent circulation of the document.

Continuing, the integrity of the circulation metadata might be necessary; if the metadata can be considered trustworthy and meaningful. The notion of integrity will be intricately linked to the organisation's ability to safeguard the preservation of a document. Central to ensuring the integrity of a document is the utilisation of a digital signature, serving as proof that the document remains unaltered, and the integrity of any digital signatures may also be questioned. It may also be necessary to consider the relevance of any data logs that might exist. Data logs are a complex topic, but a data log or data logs have the potential to support or undermine the truth of a claim as to the actions that were being carried out on a particular computer or system at a material time.[19]

Confidence and confidentiality are not often associated with electronic evidence. This perception arises from the fact that computers are generally seen as innovative devices with intricate and somewhat enigmatic internal operations. Their use could be abused, and they could fail to operate properly. Electronic evidence, therefore, is seen as being susceptible to all kinds of modifications, distortions, processing errors and contamination. Opposing parties frequently argue that electronic evidence lacks authenticity due to concerns that it may have been tampered with or altered subsequent to its creation.

Furthermore, considering the challenges, section 84 of the Act will give rise to an increase in the use of expert evidence. Parties to dispute will at the earliest opportunity, use experts to challenge statements in documents produced by computers and tendered by the other party. The court will consequently become the arena for settling cyber litigation. The provision is not stringent enough to prevent abuses. For instance, it is suggested that where the court is to rely on a mere certificate to lay a foundation concerning the acceptability of electronic evidence, the certificate should be issued by an expert. This will be in tandem with the usual trend of such certificates under

---

[19] Stephen Mason, *Electronic Evidence*, (2nd ed., India, LexisNexis Butterworths, 2010) 103

the Act. See for example the provision on the opinion of expert witnesses in sections 68 to 71 of the Act.

The quality of the certificate issued pursuant to section 84(4) is further whittled down by the concluding phrase that: *for the purpose of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.* This will give room for all kinds of quacks and mediocre to issue certificates to the best of their knowledge and belief. They will be quite unfortunate.

It is the view thatthe full implication of section 84 of the Act was not fully comprehended by the Law Reform Commission before the bill was sent to the National Assembly to be enacted into law. The Commission appeared to be in a hurry to catch up with the trend in other computer-advanced countries. The Commission must take a second look at this section.

It needs to be pointed out that the difficulties posed by electronically generated materials do not impede their admissibility in Nigerian law. They can only influence the significance attributed to those pieces of evidence after they have been admitted. Admissibility is entirely determined by relevance, and a piece of evidence that is relevant will be accepted. Queries regarding its authenticity, forgery, tampering, or accuracy in its assertions only influence the level of credibility the court might assign to it. Should the court determine that a document or other material lacks authenticity or integrity in a significant manner, it is inclined to dismiss the content or assertion as unverified. This holds regardless of whether the evidence was generated electronically or not.

In *Jacob* v *A. G. Akwa Ibom State,*[20] *it was observed*that admissibility hinges solely on the concept of relevancy, a piece of evidence which is relevant, would be admissible. A document could lack integrity or authenticity and the courts would be well to reject the contents. These problems are not insurmountable. Electronically generated materials have become indispensable in life and business and it is extremely commendable that the courts should admit and count on them in relevant cases. It would be lame to argue that they are excluded because they may sometimes be tempered with, and could mislead the courts when tendered as evidence by unscrupulous parties.

[20] (2002) FWLR (pt. 86) 576, CA

It should be noted that every cost-benefit analysis would show that the advantages of admitting and acting on electronically generated evidence far outweigh any disadvantages envisaged. No doubt the opinion of experts in some areas of the law is necessary is admissible evidence in order to the attainment of justice in a case.

It is also a fact, however, that these challenges of electronically generated evidence are far less easy to detect. It is easier for the court to refuse to act on electronically generated evidence than would be the case with conventional documents and materials. It is far more difficult to detect that an electronic message or document has been tampered with than it is to detect tampering with a hard copy document or other material.

4.0 The Way Forward

The challenges mentioned above can be traced down to affect the relevancy and admissibility of electronic evidence. In determining the relevance of such electronic evidence, it is necessary to, first of all, establish that the electronic document is what it purports to be and carries an accurate representation of the data or information which is relevant to the proceedings. This raises the salient question of the **authenticity of the evidence.**This implies that the document must be verified by an external source for it to be considered admissible. Now, the document cannot speak for itself.

Consequently, the party intending to use it must provide evidence that substantiates the document's authenticity in terms of its source (origin) and its substance (what it represents). The issue of **authentication**is a matter of leading evidence to satisfy the requirements of the Act in this regard.[21]

Hence, a digital document can be authenticated through either direct or circumstantial evidence. Circumstantial evidence encompasses various factors such as the document's appearance, content, subject matter, and any distinctive characteristics that establish a connection.Proving the authenticity of instant messages is also perfectly possible through the use of compelling

---

[21] Hon. Justice P.A. Akhihiero. Edo State Customary Court of Appeal; his paper "Admissibility of Electronic Evidence in Criminal Trials. How practicable?" A Paper Presented at the 2013 Annual General Meeting of the Magistrates Association of Nigeria, Edo State Branch held on Tuesday, 23rd of July, 2013.

circumstantial evidence.[22] In the case of *In the interest of F.P., a minor*[23]in which the Pennsylvania intermediate appellate court considered whether instant messages were properly authenticated pursuant to Pennsylvania Rule of Evidence 901(b)(4), providing that a document may be authenticated by distinctive characteristics or circumstantial evidence. In this case, Ford Elliot J. stated that:

> ...we believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework. ...we see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundation showing of their relevance and authenticity.

The tests of authenticity of electronic evidence will also depend on the source and type of electronic data. Electronic data exist in a variety of formats. For example, there are applications such as word processing and databases. There are other applications that enable a user to obtain access to the internet and email. Also, there are other data emanating from mobile telephones, storage devices and drives. There are large-scale devices like mainframe computers which cannot be moved into any court hall. For such a device you must rely on output such as the printouts. Here you may require the evidence of the expert in charge of that mainframe device.

The assurance of a document's integrity is often connected to the use of digital signatures, which serve as evidence that the document has remained unaltered. However, even the integrity of digital signatures can come under scrutiny.

Besides the above-mentioned solutions, computer or digital forensics is another solution to the challenges of electronically generatedevidence. These challenges include issues bordering on authenticity, confidentiality and integrity of the pieces of evidence.

---

[22] **Stephen Mason, (n- 20)96.**

[23] **In the case of *the interest ofF.P., a minor2005* PA Super 220, 878, A.2d 91, 2005 Pa. Super. LEXIS 1499**

The incorporation of electronic evidence and computer forensics into legal proceedings is a relatively recent development in the realm of evidentiary practices. In contrast to numerous other forensic disciplines that were seamlessly integrated into the trial process without extensive legal deliberation, the introduction of electronic evidence has ignited substantial and frequently contentious discussions within the legal community.As per Stephen Mason's observations,[24]diverse legal systems responded variably to this novel challenge. Certain jurisdictions recognized the necessity for enacting fresh legislation tailored to digital evidence, while others attempted to identify the "closest match" to established evidentiary principles and applied these regulations through analogy.

Forensics involves employing scientific expertise to gather, analyse, and present evidence in a court of law. (The word *forensics* means "to bring to the court.") Forensics primarily focuses on retrieving and analysing latent evidence, which can encompass various types, ranging from fingerprints on surfaces to DNA evidence found in bloodstains or files stored on a hard drive.

Due to the novelty of computer forensics as a discipline, there exists limited standardization and consistency across both legal jurisdictions and the industry. Consequently, it has not yet gained formal recognition as an established discipline, specifically a "scientific" discipline. *We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.*[25]

From a technical perspective, the primary objective of computer forensics is to ascertain, gather, protect, and analyse data in a manner that safeguards the integrity of the collected evidence, enabling its effective utilization in legal proceedings.

What are some common elements involved in a computer forensics investigation? To begin with, computer forensic investigations involve several key aspects that play a crucial role in uncovering evidence. Computer-related crimes can span a wide spectrum of criminal activities,

---

[24]**Stephen Mason, (no- 20) 21**

[25] **Produced 2008 by US-CERT, a government organization. Updated 2008.**

encompassing everything from instances of child pornography and theft of personal data to the deliberate destruction of intellectual property. Secondly, the investigator needs to select suitable tools for the task. Files could have been deleted, corrupted, or encrypted, necessitating the investigator's proficiency in utilising various methods and software to ensure the preservation of data during the recovery process.

There are two primary groups of data that are gathered in computer forensics. *Persistent data* refers to information stored on a local hard drive or other storage medium, which remains intact even when the computer is powered off. *Volatile data* encompasses information stored in memory or during transit, which is ephemeral and will be lost when the computer is powered off or loses electricity. Volatile data is present in registries, cache, and random access memory (RAM). Given its transient nature, an investigator must be proficient in capturing this type of data using reliable methods.

System administrators and security personnel must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

Those responsible for network security must possess a comprehensive understanding of the legal consequences associated with forensic operations.Security experts must contemplate their policy choices and technical measures within the framework of established legal regulations. For example, obtaining authorisation is necessary before monitoring and collecting data related to a computer breach. Additionally, employing security monitoring tools has legal implications.

5.0 Recommendations

There is a big challenge to e-Commerce as transactions are now carried out with a high level of fearful caution. This has developed scepticism in unfavourable business, coming on the heels of the recent transition to a cashless economy. Since Nigeria has adopted the cash-less regime, regulatory agencies and lawmakers should equally as a matter of urgency, collaborate inenacting a Cybercrime law is essential to safeguard consumers within the cashless scheme. Furthermore, financial institutions

in the country should for security reasons, develop ' fraud detective departments[26].

Until a centralised electronic databank containing specific information about each resident or visitor to Nigeria is established, exposure of criminal intentions before they are executed and the effective investigation of crimes committed would continue to pose a heavy challenge to security agencies.
Most importantly, parents hold the responsibility to closely monitor and potentially supervise their children's internet usage to mitigate instances of cybercrime[27]. The Nigerian National Bureau of Statistics reports that approximately 20 million individuals in Nigeria are unemployed, and this number is further compounded by the addition of around 2 million new entrants into the territory of the unemployed annually. There is a proverb that goes "An idle mind is the devil's workshop", as a result, many of our young people may utilise their time and skills as a foundation for engaging in criminal activities in order to enhance their living conditions and meet their needs. Hence, the establishment of job opportunities for the vast number of unemployed youths will significantly contribute to reducing the threat; 'cybercrime'[28].

6.0 Conclusion

Computers, automated data systems and other electronic devices have presented an enormous opportunity for committing criminal activities, especially against persons, organizations or properties. Such crimes include fraud, money laundering, cyber-stalking, trafficking, spamming etc. thereby creating new challenges for the Judges and Lawyers. Most times, computers are considered the repositories of essential digital evidence such that any message sent via a computer can either make or mar a case.

The importance of technology and digital devices in our everyday lives cannot be overemphasized since the world itself has become a global village.

---

[26]Albinus Chiedu,*'Tackling the Cybercrime menace in Nigeria'* p.12.

[27]Every day at a cybercafé, someone is sending some mail to a Prime Minister, President or top government official, requesting payment for some business transaction or contract that never was and never would be. If you love your country do not hesitate to call the cops when next you observe such an attempt to commit crime. Thus, the responsibility of reducing the rate of cybercrimes in Nigeria is that of every stakeholder.

[28]B H Anah ,*'Cybercrime in Nigeria:Causes, Effects and the Way-out,* 628-629.

The Nigerian legislature should be commended for their tremendous effort of including the admissibility of computer-generated documents into the procedural legislation; to wit, the Nigerian Evidence Act 2011. The provision[29] in this Act has posed a challenge as to how far and possibly will such electronic documents be admitted. It is noted however that the newly amended Evidence (Amendment) Act, 2023 has in no doubt resolve the challenges associated with the electronically generated evidence but the law will continue to be amended because of diverse and dynamic technological innovations which may further catch up with the newly amended evidence law.

[29]S.84 (2) (a-d): Evidence Act 2011.