International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 15-06-2025, Accepted: 16-07-2025, Published: 31-07-2025
Volume 11, Issue 7, 2025, Page No. 114-122

A comparative analysis of the admissibility rules of computer generated evidence in Nigeria, the United States of America, South Africa, and England and Wales

Henry Okolie Onyebuolise[1], Dr. Oyovwikerhi Imoni-Ogbe[2], O K Edu[3]
[1] Doctoral Candidate, Faculty of Law, Delta State University, Abraka, Delta State, Nigeria
[2] Lecturer, Department of Jurisprudence and International Law, College of Law, Western Delta University, Oghara, Delta State, Nigeira
[3] Lecturer, Faculty of Law, Delta State University, Abraka, Delta State, Nigeria

Abstract
Given that computer-generated evidence is unique and has many complex origins, it became necessary to create regulations governing its acceptance in Nigeria and other jurisdictions. Since digital evidence is easily manipulated, it is expedient to convince the court that the collected digital evidence is genuine in order to increase its chances of admissibility and the weight to be attached to it. Authenticity pertains to whether or not the evidence is accurate in its message and truly emanated from the person or source it claims to emanate from. Nigerian and the United States of America (USA) laws treat authenticity of digital evidence as a pre-condition to admissibility. In South Africa, England and Wales, their laws treat authenticity as a post-admissibility matter. Is the admissibility of digital evidence a pre-admissibility or post-admissibility matter? What is the implication of these respective rules of admissibility of digital evidence for justice delivery? It is premised on the above questions that this article compared the admissibility status of computer-generated evidence in Nigeria, the United States of America, South Africa, England, and Wales and their effects on the administration of justice. In accomplishing this goal, the doctrinal research method was adopted. In the course of this research, it was found among others that section 84 of the Evidence Act (Nigeria), 2011 is interpreted cosmetically and unfairly by Nigerian courts. Based on the finding, it was recommended among others that Nigerian courts should give vent to the real essence of section 84 of the Evidence Act and treat authenticity of digital evidence as pre-admissibility matter, as obtains in the USA.

Keywords: Authenticity, integrity, admissibility, forensic science, computer forensics, digital evidence

Introduction
Rules of evidence are in place in every country to help courts carry out their difficult responsibility of administering justice in an effective and efficient manner. The evidence presented by parties must be relevant to the issues under trial. The evidence must also not offend any rule of admissibility. Once any piece of evidence is relevant, and does not offend any admissibility rule, it is admitted in evidence by court and relied on in adjudicating or determining the case being tried. Evidence could be oral, documentary or real. With the emergence of computer and the internet age, the meaning of document has been extended in several jurisdictions to include digital documents. Video tape, Digital Video Recorder (DVR), Compact Disks (CDs), Digital Versatile Disks (DVDs), Subscriber Identity Module (SIM), Compact Flash (CF), Digital Audio Player (MP3) are now interpreted by courts as documents. The sources of digital evidence are complex, while their nature is malleable. This implies that special procedure should govern how to collect and handle digital evidence so as to be seen as credible and admissible by courts in legal proceedings. Several countries including Nigeria, the United Kingdom (UK), South Africa, the United States of America (USA) and Canada have developed various and varied rules to govern the admissibility of digital evidence, all geared towards ensuring that the ends of justice are met in legal proceedings.

Generally, from applicable rules within the selected jurisdictions, there are two schools of thought on authenticity and admissibility of electronic evidence, *viz*: conservative school and liberal school. The conservative school sees authenticity as condition precedent to admissibility. The conservative school gives forensic science its dues in deciding admissibility. This is because forensic science helps to establish authenticity. The liberal school sees authenticity as a post-admissibility matter. This school denies the role of forensic science in determining admissibility. This school will admit electronic evidence, once pleadings show that provisions of the evidence law on admissibility have been met, without interrogating the system device and procedure. This school resolves authenticity on the altar of expediency and convenience, preferring to treat authenticity as a matter of weight, rather than a matter of admissibility. What reasons drive these schools of thought? Which approach serves the best interest of justice? Which approach is better, especially for Nigeria, whose law on digital evidence is still at its infancy? These are the questions that this articles seeks to answer.

Conceptual Clarification
Under this heading of the article, some key concepts would be explained for the better understanding of the article.

1. Concept of Digital Evidence
In all developed legal systems, documents constitute very important form of evidence. Consequently, electronic documents are a particularly important form of evidence. Lawyers and judges must bridge the mental gap between the digital world, which seems so foreign to those who are unfamiliar with it, and the physical world, with its familiar paper documents. Digital data presented to the human eye

on a screen or printed is an illusion that requires further explanation. In a digital record system, the components that make up the data are stored independently of one another. Different items of data are stored on different parts of the application system and they are made manifest in human readable format when brought together on a screen as if it is an entire and complete record. The program combines disparate data points and arranges them in a way that makes the file seem like a whole unit. The files are not as real as they appear on the screen, and similarly, there is no assurance that the different parts of the file will be kept in a fashion that will allow for future reconstruction.

Particular characteristics of digital documents impact the way evidence is gathered and managed prior to trial, as well as the authenticity or source verification, should authenticity be a concern. Compared to papers on physical media, digital evidence should be subject to a more rigorous and careful process. Physical document integrity is frequently protected in a quite casual manner. The same cannot be said of documents in digital format. Because the standards by which a digital document must be evaluated are different from those of a physical document by definition, it is impossible to compare the two types of documents like for like. There are certain characteristics of digital documents that pose unique difficulties compared to paper carriers in the real world [1].

2. The Concept of Forensic Science and Computer Forensics

Forensic science is a multi-disciplinary area of study. The application of their specific scientific field to criminal, civil, legal, and judicial concerns is the focus of this collection of scientific disciplines [2]. The field of computer forensics integrates aspects of computer science and law to gather and examine data from wireless communications, computer networks, storage devices, and systems in a manner that can be used as evidence in court. Computer forensics has emerged as a crucial investigative and criminal investigation technique in the current digital era, as nearly everything is saved, transmitted, and processed on electronic devices [3]. The main difference between the two disciplines is that forensic science emphasises physical evidence, while computer or digital forensics emphasises digital evidence [4].

Authentication of Digital Evidence

Courts generally ask if the recovered evidence is the same as the originally seized data, when considering whether digital evidence is admissible. In other to prove that digital evidence is authentic, it is generally necessary to satisfy the court that it was obtained from a specific computer and/or location; that a complete and accurate copy of the digital evidence was obtained and it has remained unchanged since its collection. In certain situations, it could also be required to provide proof that certain details, including dates connected to a certain file that is significant to the case, are true. It is obvious that the authenticity of digital evidence is crucial to the process. Chain of custody and honest documentation is crucial for proving that digital evidence is authentic. An appropriate chain of custody proves that digital evidence was obtained from a particular system and/or place and that it has been under constant supervision ever since it was gathered. The court can thereby connect the digital evidence to the offense through appropriate chain of custody paperwork. Documentation of integrity aids in proving that digital evidence has not been tampered with since it was gathered [5].

Hash values are used to determine the integrity of copied digital evidence. When digital evidence's hash value deviates from the original, it might be feasible to separate the modified section while confirming the integrity of the remaining component. For instance, a hard drive's damaged sectors typically result in a different hash value each time it is computed [6]. Finding the locations of subpar parts will help a digital investigator determine whether or not they are linked to case-relevant files. Additionally, to make sure that particular files are not affected by the faulty sectors, the hash value of each file that is crucial to the case can be checked with those on the original hard drive [7].

In *United States v Bunty* [8], the US Customs and Border Protection officers discovered child pornographic photos on Patrick Bunty's two laptops and other storage devices upon his arrival in Philadelphia from London. The agents tried to look at Bunty's laptops' contents and opened files on his storage media on a government-owned computer. Bunty put a wrong password on one of his laptops when they asked him to grant them access, locking the device and preventing the agents from examining the data at the moment. Due in part to the government's failure to produce forensic copies of the media before their examination, Bunty contended in court that the evidence should not be allowed. The court determined that the government handled the evidence in good faith and that their changes to it were insufficient to rule it out, thus it found that the evidence was admissible. The defendant in *United States v Tank* [9], a case involving the orchid wonderland investigation, contended that the veracity and applicability of online chat logs were not sufficiently demonstrated. The defense made the argument that it was simple to alter the chat logs. Several witnesses were employed by the prosecution to prove the authenticity of the logs. According to the court, printouts of computer-generated logs of 'chat room' discussions can be proven by proof of their preparation, the correctness of the discourse they depict, and their relationship to the defendants.

Authenticity Rules and Admissibility in Selected Jurisdictions

Under this heading, the article would examine the authenticity rules of admissibility in the following selected jurisdictions: Nigeria, the USA, South Africa, and England and Wales.

1. Nigeria

Section 84 of the Evidence Act addresses digital evidence authentication. The section's main goal is to guarantee that only authentic computer-generated documents are allowed to be used in court. In this context, authentication simply means that the party providing electronic evidence must provide enough proof to establish that the document in question is what it claims to be [10]. Section 84(2) and (4) of the Evidence Act, as amended by the Evidence (Amendment) Act 2023, are central to our discussion here. The provisions outline the prerequisites that must be met for computer-generated evidence to be admissible. Authenticity has two thresholds. Establishing a connection between the accused and the evidence presented is the first step. The ability of investigators to effectively handle the 'identity problem' is necessary for this. This could be a forensic problem for several reasons, but it is evidently more so in a

network setting, whether it be closed like a corporate network (intranet), or open, like the internet. The second step is to connect the material to the appropriate computer or system (the 'computer source' threshold).

In the light of these thresholds, section 84 of the Evidence Act 2011 as amended by the Evidence (Amendment) Act 2023, laid down certain conditions, which must be shown to exist for electronic evidence to be admissible in any proceedings. These conditions were provided to assure authenticity and integrity of electronic evidence. Before electronic evidence is admissible in evidence in any proceedings by virtue of section 84(1), certain conditions specified in subsection (2) must be shown to exist. The conditions are:

a. The statement or electronic record must have been generated by the computer during the time frame that the computer was routinely used to store or process data for any activity. During the same time frame, such activity must be consistently conducted;
b. The data entered into the computer during routine tasks must be of the type that is included in the electronic record or the type from which the data in the electronic record was derived;
c. The computer was in proper working condition throughout the relevant part of the period. Where it was not, it must be shown that the fault was not the type that would affect the production or electronic record, document or the integrity of its content;
d. (d) The data in the statement or electronic record must be replicated or derived from data that was entered into the computer during routine operations.

The jurisprudence of the above conditions is founded on the fact that it is easy to create, alter or manipulate electronic evidence. These requirements have prevented a scenario in which parties to a lawsuit would use these weak points of electronically generated evidence to fabricate evidence that supports their position before appearing in court. Besides, due to the uniqueness of this type of evidence and its fray features portrayed above, section 84(4) prescribes the supply of a certificate of compliance:

a. Pinpointing the document bearing the data and narrating the way it was produced.
b. Identifying such particulars of the computer used to generate the document, for the purpose of proving that the document was generated by a device.
c. The certificate should be endorsed by someone holding a responsible position in relation to the operation of the relevant computer or the handling of the relevant activities as the case may be.

Section 84(b) of the Evidence Act of 2011 eliminated the distinction between original and secondary evidence of electronic documents for the purposes of the aforementioned. One of the difficulties facing Nigerian advocates on the tendering of electronically generated evidence is proving not only that the computer that created the document worked properly, but also that the data it contained had not been altered or changed. It is not necessary to take electronic documents as proof. Therefore, there must be an evidentiary basis for concluding that a document is what it purports to be before it can be admitted in evidence. In summary, this is what section 84 of the Evidence Act aims to achieve. This is by no means a simple undertaking, particularly since the presiding judge and the attorneys presenting the evidence may not be familiar with the nuances of electronic evidence.

The opposition attacks the electronic evidence presented by the prosecution, either by attacking the evidence itself and/or by attacking the process and personnel associated with collection and analysis of the evidence. According to section 84 of the Evidence Act, there are two ways to contest the admissibility of computer-generated evidence. Ajileye asserts that for any objection under section 84 against electronic evidence to be legitimate, it must center on concerns about the document's authenticity as well as the dependability and integrity of the computer that generated it [11]. In Nigeria, the use of digital evidence in court is still relatively new. Before 2011, electronic evidence was largely inadmissible in legal proceedings [12]. This was because electronic documents could not pass as documents under the provisions of the repealed Evidence Act [13].

This deficiency is one of the factors that informed the promulgation of the Evidence Act 2011 which expanded the meaning of document to cover electronic documents [14]. Electronic documents are now admissible in legal proceedings in Nigeria, so long as they pass the test of admissibility enshrined in section 84 of the Evidence Act. The Supreme Court held in *Kubor & Anor v Dickson & Ors* [15] that a party wishing to rely on electronic evidence must do more than just tender it from the bar. To demonstrate the requirements outlined in section 84(2) of the Evidence Act 2011, evidence pertaining to the device's use must be shown. In this case, the Supreme Court of Nigeria also held that electronic evidence is inadmissible if it does not meet the requirements outlined in section 84(2) of the Evidence Act 2011. In *Nnamani v FBN & Anor* [16], the Court of Appeal, held that where there is no evidence on oath to fulfill the conditions prescribed in section 84 of the Evidence Act, electronically generated documents are inadmissible. The Court of Appeal per Obande Festus Ogbuinya JCA, delivering the lead judgment held thus:

Exhibit B1, failed to satisfy the conditions adumbrated in section 84 of the Evidence Act, 2011, as there was no scintilla of evidence from first respondent in that regard. The glaring absence of such evidence desideratum in satisfaction of those conditions afflicts its admissibility. Put starkly, it is made inadmissible, since it was tendered from the Bar, without further evidence from a witness to meet the conditions.

Where compliance with the express provision of section 84 of the Evidence Act cannot be established, the computer generated evidence is for all intents and purposes inadmissible. Without adhering to section 84(2) of the Evidence Act 2011, the requirements outlined in that section cannot be waived, nor can parties agree to the admission of such documents [17]. In *Brila Energy Ltd. v FRN* [18], Otisi JCA held that the provisions of section 84 which outlines the requirements for admitting in evidence any electronically generated document, are crucial in figuring out whether a document originating from a computer is admissible. The primary goal of these requirements is to verify and authenticate the dependability of the computer that produced the evidence that is sought to be tendered. It is necessary to prove that a device was operating correctly and was not misused before any statement in a document produced by the device could be admitted in evidence. As a result, evidence related to the device's use must be tendered

to demonstrate compliance with the pre-conditions outlined in section 84(2).

The same court ruled that the production of an authentication certificate is an additional need for the admissibility of digital evidence under section 84(4) of the Act. The Court of Appeal held in *Usman & Ors v Sani & Ors* [19], per Hussein Mukhtar (JCA} that the production of an authentication certificate under section 84(4) is merely an additional requirement of solemn affirmation that the mandatory pre-conditions under section 84(2) were duly satisfied; it is not a replacement for these conditions. In *Davou v COP* [20], the court ruled that before a computer-generated document can be admitted, an authentication certificate must be produced. Failure to do so therefore rendered Exhibit P6A and P6B (Pictures generated with computers) inadmissible.

Section 84 of the Evidence Act is *impari materia* with section 69 of the English Police and Criminal Evidence (PACE) Act 1984 [21]. There is a plethora of cases now in Nigeria, on the admissibility of electronically generated evidence. But the courts are more concerned with the casual, literal satisfaction of section 84 of the Evidence Act. Once the pleading or oral evidence states that the computer was working properly at the relevant time, backed up by a certificate of authenticity vindicating the pre-conditions in section 84(2), the evidence is admissible irrespective of whether or not the computer was actually or really working properly at the time the evidence was produced. Nigerian courts appear to be paying only lip services to section 84 of the Evidence Act in the aspect of authentication and admissibility of computer-generated evidence.

Nigerian courts appear to be guided by the English court's decision in *R v Spiby* [22], decided under section 69 of PACE Act which is *impari materia* with section 84 of the Evidence Act 2011, as amended, where it was held that a hotel manager was competent to provide testimony to meet the conditions in section 69 of the PACE Act that a computer was working properly at the relevant time. When interpreting section 69 of PACE Act in *R v Shepherd* [23], the House of Lords held that oral testimony from someone who is familiar with the device's operation can satisfy the requirement of the section without the necessity for a digital expert. It is submitted that this is a liberal approach to the construction of section 69 of PACE Act with regard to the reliability of the computer. The sources of digital evidence are highly technical and complex. The nature of digital evidence is remarkably different from traditional documents. Forensic science is required for the proper handling of electronic evidence, from identifying, preserving and analysing electronic evidence, to presentation of same in judicial proceedings as reliable, authentic, and admissible.

The Court of Appeal appears to have followed the liberal approach adopted by English courts in *R v Spiby* and *R v Shepherd,* in *Blaize v FRN* [24], when it held that the owner of a cybercafé was competent to testify on the trustworthiness of a computer. The approach of the court is that once pleading or certificate vindicates literally the conditions stipulated in section 84(2) of the Evidence Act 2011, the evidence is admissible, irrespective of whether or not the integrity, validity, and reliability of the device is established by forensic science. Stoykova [25], regrets that electronic evidence is progressively tendered and admitted by courts without scientific certification of the digital forensic techniques, procedures, or tools used. Ajileye, argues that the decision of the Supreme Court in *Dickson v Silva* [26], sets the precedent that leads to the suggestion that trial courts adopt a liberal approach in applying section 84(2) of the Evidence Act and that what should be paramount to court is whether or not the evidence of a witness broadly speaking, substantially meets all the preconditions outlined in section 84(2). If it does, the document should be admitted in evidence [27]. The liberal approach makes mockery of the forensic nature and technical sources of digital evidence. It throws over board the checks and balances birthed by section 84(2) of the Evidence Act aimed at guaranteeing the validity, reliability, integrity, and authenticity of digital evidence and has the potential of leading to the conviction of innocent suspects as shown by the English case of *Bates v The Post Office Ltd* [28].

Two opportunities presented themselves to the Nigerian courts to give forensic science its place under section 84(2) of the Evidence Act in determining the reliability of the computers that generated electronic evidence as pre-condition for admissibility of the evidence. These are the related cases of *Rowaye v FRN* [29] and *Brila Energy Ltd v FRN* [30], In *Brila Energy Ltd v FRN*, a sister case to *Rowaye v FRN*, Jubril Rowaye was the *alter ego* of the company-Brila Energy Ltd. Both Jubril Rowaye and Brila Energy Ltd stood trial jointly at Lagos State High Court and were convicted as charged. As allowed by law, both Jubril Rowaye and Brila Energy Ltd appealed the judgment of the trial High Court separately. The points of law taken up before the Court of Appeal Lagos Division in *Brila Energy Ltd v FRN* and *Rowaye v FRN,* were the same and decided the same way *mutatis mutandis*. The same panel of Honourable Justices heard the appeals and dismissed them on the same day. The issue of utmost importance in both cases for the purpose of this article is the admissibility of Lloyd's List Intelligence Report, Exhibits P23 to P25. The Appellant contended that the admission in evidence of exhibit P23 and P25 on the strength of the certificate of Economic and Financial Crimes Commission (EFCC) computers which was utilised to upload information from Lloyd's website, failed to satisfy the requirement of section 84 of the Evidence Act, which prescribed for the certification of the device utilised to produce the information uploaded to the database; as against the device utilised in accessing or copying the information. Consequently, it was argued that the exhibits were not admissible and ought not to have been admitted by the lower courts. The Court of Appeal upheld the decision of the trial court which presumed the trustworthiness of Lloyd's computer, as Lloyd's List Intelligence Report has a world class reputation and is conclusive of authenticity of Exhibits P23 and P25. In *Rowaye v FRN,* the Court of Appeal upheld the trial court's presumption of the trustworthiness of Lloyd's List Intelligence Report as one, having world class reputation and as such conclusive on the status of the documents. Unlike as it is obtainable in Canada, England and Wales, section 84 of the Evidence Act does not give room for presumption. Instead of requiring evidence to establish the trustworthiness of Lloyd's computer, the court presumed Lloyd's computer was working properly and correctly at the time the relevant evidence was produced. This lip service paid by the Nigerian courts to the requirements of section 84 as pre-

conditions for admissibility of computer-generated evidence have the capacity to birth injustice as seen in *Bates v The Post Office Ltd*. The researchers argue that the liberal approach adopted by Nigerian courts is meant, most essentially, to compensate the want of in-depth knowledge of computer forensics.

Law is meant to birth justice, not injustice. The cardinal principle of criminal law is, instead of punishing one criminal without justification, let ten offenders go scot free. In the golden words of Blackstone, 'the law holds that it is better that ten guilty persons escape, than one innocent to suffer' [31]. Benjamin Franklin gave this maxim of justice, a higher threshold when he stated thus: 'that it is better 100 guilty person escape, than for one innocent to suffer', is a maxim that has long been generally accepted [32]. The high standard of proof that is usually required in criminal proceedings reflects this principle [33]. The outlined benefits derivable from applying the liberal approach is nothing in comparison with the consequence of wrongful conviction due to unnoticed computer failures as in *Bates v The Post Office Ltd*. While not undermining the inconveniences associated with the conservative approach, which makes Nigerian courts resort to the liberal approach which admits electronic evidence on the tendering of same just merely upon casual and artificial fulfillment of the pre-conditions for admissibility prescribed by section 84(2) and (4) of the Evidence Act, leaving what is to be done with the evidence as a matter of weight, there is the need to find a balance between both approaches in a way that will guarantee the ultimate and overwhelming end of justice. This balance will forestall the injustice that the accused persons suffered in *Bates v The Post Office Ltd.* There is the need to find a balance that will either totally obliterate or reduce the ills associated with the conservative approach. That way, justice will not be sacrificed on the altar of expediency and or convenience.

2. The United States of America

In the Federal Courts of the USA, authentication of evidence is governed by Rule 901(a) of the Federal Rules of Evidence, which provides that to satisfy the requirements of authenticity or pinpointing a piece of evidence, the advocate must generate evidence sufficient to support a conclusion that the piece of evidence is what the advocate claims it is [34]. Authentication is a prerequisite antecedent to the admission of evidence, and evidence must be proved to be authentic in order to be admitted [35].

The most helpful authentication guidelines under rule 901(b) for digital evidence are:

1. 901(b)(1) - a witness who has firsthand knowledge that the evidence is what it claims to be; (ii) 901(b)(3) - a comparison of the evidence with a specimen that has been verified by an expert witness or a fact-finder;
2. (iii) 901 (b) (4) -the item of evidence's appearance, details, substance, internal patterns, or other distinctive qualities, along with all the circumstances;
3. (iv) 901(b)(5) for audio recording, an opinion identifying a person's voice, whether heard directly or via electronic transmission or recording, based on hearing that voice previously; and
4. (v) 901(b)(9) - evidence describing a procedure or system of demonstrating that it yields accurate results.

Federal Rule of Evidence 902 gives examples of self-authentication, in which testimony or other external evidence is not required for authentication. These examples include:

1. 902(5) - a book, pamphlet, or other document that appears to have been published by a government agency;
2. 902(6) - printed items posing as a magazine or newspaper. The 'online edition' of the majority of newspapers and magazines may be accessible for self-authentication;
3. 902(11) and (12) - verified copies of documents of routinely conducted activities, both domestic and foreign [36].

Few cases of the USA will be considered to buttress the multi-faceted rules of authentication of electronic evidence. In *Anderson v United States* [37], the defendant witness admitted that the disputed document included emails he provided to an undercover agent in accordance with Rule 901(b)(1). The whole email discussion between him and the undercover agent was included in the document, which was sent from his email address. The court determined that this was adequate evidence of genuineness. Emails that were difficult to identify on their own were authenticated in *United States v Safavan* [38], using Rule 901(b)(3) which stipulates that the trier of facts may authenticate evidence using 'specimens which have been authenticated'— in this case, emails that have undergone independent authentication. In *United States v Simpson* [39], chat-room log, in which user 'stavron' revealed his email address and identified himself as the defendant, was utilised to verify later emails sent from that account in accordance with rule 901(b)(4). The government attempted to authenticate text messages sent from two Skytel pages, each belonging to a defendant in the case of *United States v KilPartick* [40]. This was because text messages transmitted from the defendant's devices are automatically saved on Skytel's systems without editing capabilities, a Skytel record-custodian confirmed that the government-provided text message had not been and could not be altered in any way. According to rule 901(b)(9), the court determined that this demonstration was adequate.

A number of cases were cited in *Williams v Long* [41] suggesting that posts on official websites are self-authenticating. The United States Court of Appeals for the 4th District ruled in *United States v Hassan* [42] that Facebook posts that included YouTube videos were self-authenticating under rule 902(11) provided that they were accompanied by a certificate from Google and Facebook custodians confirming that the Facebook page and YouTube videos had been maintained as business record in the course of regularly conducted business activities. The Huntsville Times website (Al. Com) news stories 'could be found self-authenticating at trial' as held by the court *sua sponte* in *White v City of Birmingham* [43].

Authenticity is what is meant by trustworthiness in this decision. Such evidence must be genuine in order for the court to accept it. According to the court, when it comes to electronic documents, the circumstances surrounding the record's preservation during the retention period should be prioritised in order to guarantee that the authenticated document is identical to the one that was initially created. Also, logical questions go beyond identifying the specific

computer hardware and software that are being used. It is crucial to follow the organisation's policies and procedures when using the equipment database and programs. The question of whether records have changed since they were created is relevant to the structure and implementation of backup systems and audit procedures for ensuring the database's ongoing integrity, as well as how changes are logged or recorded in the database and how access to the relevant database is controlled [44].

In the USA, certification is increasingly used to verify the authenticity of electronic evidence. On December 1, 2017, the new Federal Rules of Evidence amendment went into effect. Regulation 902, the self-authentication regulation, now has two more sub-divisions. The first clause permits machine-generated data to be self-authenticated if a certificate created by a qualified individual is submitted. For a copy of data extracted from an electronic device, media, or file, the second clause offers a comparable certification process. These regulations are comparable to Federal Rules of Evidence Rules 901(11) and 901(12), which allow a foundation witness to certify that a business record is authentic [45].

3. South Africa

Even though it has been proposed that the relevance of the evidence should be the determining factor in whether it should be admitted or rejected, South Africa continues to use an exclusionary approach to evidence. This implies that even relevant evidence in civil and criminal cases may be eliminated if it is problematic in the sense that the time lost by requesting a court to consider it or the potential prejudice from revealing it during a trial exceed its value as evidence. A court can save time by using an exclusionary strategy, which avoids requiring it to consider evidence that it cannot rely on. Electronic evidence is undeniably problematic. According to Schmidt and Zeffertt, '...in leaving paper, we have also left almost all guarantees of authenticity and reliability' [46]. Hofman supports Schmidt and Zeffertt's argument that, like other types of evidence, a court must account for intentional or unintentional human error when using electronic evidence [47]. Defective software and device breakdown are additional risks associated with electronic evidence. Additionally, compared to traditional documents, electronic evidence may be more difficult to detect for tampering.

The African Law Commission has been experimenting with electronic evidence since 1976, when the Appellate Division refused to accept computer-generated bank records as evidence in *Narlis v South African Bank of Athens* [48], it was decided that the admission of computer printouts was not covered by section 34 of the Civil Proceedings Evidence Act 25 of 1965. Although the clause allowed for the acceptance of a statement made by a person in a document under certain conditions, a computer is not regarded as a person. To control the admissibility of digital evidence, the Computer Evidence Act 57 of 1987 was passed [49]. The law has failed to accomplish its goal mainly because of an unduly cautious approach that places too much weight on authenticity and dependability [50]. Therefore, a number of conditions must be fulfilled before admissibility is attained. Additionally, the Computer Evidence Act did not control criminal trials; it solely applied to civil procedures.

Therefore, immediate legislative action was needed. The Electronic Communication and Transaction Act (ECT) Act of 2002 (ECT Act), which entered into effect on August 30, 2002, provided statutory relief. Before the ECT Act, South Africa had no laws pertaining to electronic evidence [51]. However, the law of evidence is only specifically addressed in section 15 of the ECT Act. It is recommended that a South African court interpreting the ECT Act's provisions with regard to electronic evidence do so as a functional equivalent of the legislation controlling other forms of evidence, even though section 15 of the Act does not necessarily extend outside of the commercial realm.

The South African common and statutory laws govern admissibility of electronic evidence. No special rules of evidence govern electronic evidence in criminal proceedings. The admissibility of electronic evidence in criminal proceedings is the functional equivalent of traditional evidence.

4. England and Wales

In England and Wales, court considers computer as a matter of law to have been working correctly, unless there is evidence to the contrary [52]. Therefore, evidence produced by computer is regarded as authentic, unless there is evidence to the contrary. This manner of treating evidence is known as a 'rebuttable presumption'. A court will presume a computer to be working perfectly, unless a person can prove otherwise. The aim of a presumption which allocates the onus of proof [53], is to alleviate the need of proof of every item of evidence adduced in court or to reduce the need for evidence in relation to some issues [54]. This assumption presents a challenge to those challenging evidence generated by a computer system. The challenge is insurmountable, especially when a large institution operates the system. The Post Office Horizon scandal clearly exposes the problem and harm that may result. From 1999, the Post Office prosecuted hundreds of postmasters and Post Office employees for theft and fraud, based on evidence produced by the Horizon Computer System, showing shortfalls in their branch account. In these trials, the Post Office relied on the presumption that the computers were working properly. Hundreds of postmasters and others were convicted, sentenced to prison, fined, or had their assets confiscated.

In the December 2019 judgment of the trial of these postmasters and others, - *Bates v The Post Office Ltd (No. 6 Horizon Issues)* [55], Mr. Justice Fraser concluded that it was possible that software errors in Horizon could have caused apparent deficits in the branch account rather than being due to theft or fraud. Following this decision, the Criminal Cases Review Commission referred an unprecedented number of convictions to the Court of Appeal, based on the alleged shortfalls in Horizon's accounts. Appeal Courts have overturned more than 70 convictions as at 2024. More convictions are set to be overturned in what is likely to be the biggest miscarriage of justice in British history.

Without the group litigation, the fundamental unreliability of the software in the Post Office's Horizon computer system software, would not have been discovered, because previous challenges to Horizon's accuracy, were unable to rebut the presumption of reliability of digital evidence. The legal presumption applied in practice, is widely misunderstood as to the nature of computer failures. The presumption has been the cause of widespread injustice. It is urgent that the presumption be realistically assessed, to avoid any further or continuing injustice [56].

Comparative Analysis of Authenticity Rules among Selected Jurisdictions

Prior to its repeal in 1999 by the Youth Justice and Criminal Evidence Act, Section 69 of the PACE Act governed the admissibility of electronic evidence in England and Wales. Section 69 of the PACE Act is *impari materia* with section 84 of the Nigerian Evidence Act 2011 as amended. As a prerequisite to the admissibility of electronic evidence under the PACE Act, the party introducing the evidence must demonstrate the integrity of the electronic system by or in which the electronic document was recorded or saved. Trials-within-trials were then carried out to verify the authenticity of electronic documents before they could be admitted [57]. In *R v Minors (Craig)* [58], Styn J, as he was then known, outlined the Court of Appeal's position on the subject of computer-generated evidence:

> The course adopted by the judge in the appeal before us prompts us to refer to the procedure that should be adopted in a matter where there is disagreement as to the admissibility of a computer generated document. It is clear that in such a case, a judge ought to adopt the procedure of embarking on trial within trial.

England and Wales substituted proof with presumption, with the enactment of the Youth Justice and Criminal Evidence Act 1999, which repealed section 69 of the PACE Act. Both computer device and computer-generated evidence are now presumed to be authentic in England and Wales. The device and the device-generated document are authentic, unless the contrary is proved. Unfortunately the defence, in most cases where the device belongs to the prosecution, lack access to such device and in turn, access to facts with which to challenge the authenticity of the electronic evidence. Consequently, as seen in *Bates v The Post Office Ltd*, such evidence is admitted without interrogating the integrity of the system device, as well as the authenticity of the document generated by such device. This is a liberal approach to the admissibility of electronic evidence. Electronic documents are admitted without any ado, on the presumption that they are authentic, and then precedent to judgment, determine the weight to attach to them.

This liberal approach was adopted by England and Wales, in order to circumvent the cost and time constraints associated with proving the authenticity of the computer device precedent to admissibility, which the researchers call the conservative approach. *Bates v The Post Office Ltd* credibly leads to the conclusion that the liberal approach to the admissibility of electronic evidence has an enormous potential to sacrifice justice on the altar of convenience and expediency.

Nigeria belongs to the liberal school with regard to the rule on admissibility of electronic evidence. Section 84 of the Evidence Act 2011, as amended is conservative in nature, as it requires a party adducing electronic evidence, as a pre-condition to its admissibility, to establish that the device which generated the document and the document are authentic. Section 84 of the Evidence Act 2011, as amended, gives computer forensics its place in assuring the integrity, reliability, validity and authenticity of electronic documents, before their admissibility. There is no presumption of authenticity under section 84 of the Evidence Act. Unfortunately, in construing section 84 of the Evidence Act, Nigerian courts consistently adopt the liberal approach, applicable in England before 1999 and afterwards. For many reasons, including cost, and time constraints and particularly the prevalent want of in-depth knowledge of computer forensics associated with the conservative approach, Nigerian courts give cosmetic approach to the interpretation of section 84 of the Evidence Act 2011.

In Nigeria, all that is needed for a piece of electronic evidence to be admitted in evidence, is for the pleadings to vindicate literally, cosmetically the pre-conditions for admissibility stated in section 84(2) of the Evidence Act, backed by a certificate of authenticity required by section 84(4) thereof, whether or not in reality the computer device was in a proper working condition at the time it generated the document, knowing fully-well that a faulty device will produce a fallacious document, as seen in *Bates v The Post Office*. This approach, drawing inferences from *Bates v The Post Office Ltd* has the potential to work grave injustice on accused persons or defendants in Nigeria.

In South African criminal proceedings, the admission of electronic evidence is not governed by any particular rule of evidence. Electronic evidence is treated as the functional equivalent of traditional evidence in cybercrime trials. In South Africa, the collection, preservation, and presenting of evidence for use in criminal prosecutions are not governed by any procedure. The authenticity and integrity requirements for admissibility of paper documents, extended to digital evidence are concerned with electronic documents themselves, not the computer devices that generated or produced them. The implication of this without expressly saying so, is that computers are presumed infallible. But computer devices and software are not isolated from failure, which failure invariably affects the generated evidence, as seen in *Bates v The Post Office*. South Africa had the compliment of the Computer Evidence Act, albeit, applicable only to civil proceedings, but repealed same due to a number of stringent conditions to be met before electronic evidence became admissible under it. South Africa therefore belongs to the liberal school with regard to admissibility of digital evidence with its concomitant room for injustice to defendants.

Under the liberal approach, electronic evidence is presumed to be authentic on tendering, except there is a substantial opposition to the admission of same. In most cases, the computer devices are in possession of the prosecution. How can the defence raise any substantial opposition on the integrity and authenticity of such computer devices in such circumstance, as to warrant their rejection? Electronic evidence most often than not is admitted in evidence on the tendering of same, as the defence will not know the history of performance and/or the status of the computer device that generated a piece of evidence, in order to raise any meaningful opposition to its admissibility. In these situations, all that remains is the weight that should be given to the evidence. Again the defence cannot effectively challenge the credibility or probability of such evidence in order to render it worthless. The implications for justice for the defendants, are grave under the liberal approach.

Multi–faceted rules of authenticity operate in the USA. These rules are conservative in nature, as they all ensure that authenticity is treated as a pre-condition to admissibility of electronic evidence. These rules ensure that authenticity of electronic evidence is established before admissibility and

not as a matter of weight. If the electronic document is not authentic, it is rejected on the tendering of same. In the USA, both the device that produced the electronic evidence and the electronic evidence (document) must be proved to be authentic before that evidence is admitted. Otherwise, it will be rejected. There are numerous regulations in place to assist the courts in determining the authenticity of electronic evidence as a pre-condition for its admissibility [59]. Irrespective of the cons associated with the conservative approach, the USA will not sacrifice justice on the altar of convenience and expediency, as obtainable in England and Wales, and Nigeria.

The rules of authenticity in the USA engenders growth in the field of forensic science or computer forensics, since forensic science is what helps to identify, gather, preserve and analyse electronic evidence; and is the panacea to the complexities associated with the unconventional nature and technical sources of electronic evidence. The conservative approach ensures that justice is always served, especially to defendants in criminal matters, and as such, is in tandem with that noble maxim of justice, that it is better to let ten criminals escape justice, than to punish one innocent person.

Recommendations

Sequel to the foregoing, it is recommended, that Nigerian courts give vent to the real essence of section 84 of the Evidence Act and treat authenticity of digital evidence as pre-admissibility matter, as obtains in the USA. In order to obviate the challenges associated with the conservative approach to authenticity, which informed resort to the liberal approach by the Nigerian courts, and make the conservative approach operational in Nigeria, this article recommends the two-stage approach, suggested by Paul Marshall and others [60]. This two-stage approach will enhance justice by circumventing the challenges of time and costs associated with the conservative approach, while preventing unjust experiences of defendants in cybercrime prosecutions, similar to those in *Bates v The Post Office Ltd*.

It is, also, recommended that the Evidence Act of 2011 be further modified to include a self-authentication rule, which would eliminate the necessity for external testimony or evidence to authenticate, as is the case in the USA [61].

Lastly, it is recommended that the best way to guarantee the acceptance of digital evidence in different countries is to standardise digital forensics procedures.

Conclusion

Electronic evidence and its admissibility are newly emerging areas of the law in Nigeria. The enactment of the Evidence Act 2011, as amended, marked the beginning of Nigeria's actual journey in the area of digital evidence and its admissibility. Section 84 of the Evidence Act 2011, as amended lists mandatory pre-conditions to the admissibility of digital evidence. From cases so far decided by courts in Nigeria on the admissibility of digital evidence, a cosmetic approach to the construction of section 84 of the Evidence Act 2011, as amended has crystallised. While England and Wales, Nigeria, and South Africa belong to the liberal school of thought that treat authenticity as a post-admissibility matter, the United States belongs to the conservative school of thought, which treat authenticity as a pre-admissibility matter. This paper appraised the implication of the liberal and conservative approaches to authenticity as a rule of admissibility for justice and finds that while the conservative school esteems justice above inconvenience and high costs, the liberal school sacrifices justice on the altar of convenience and expediency. This article finds the conservative approach better and superior to the liberal approach, as it serves the end of justice, and recommends the conservative approach to construction of section 84 of the Evidence Act, 2011 as amended, to the Nigerian courts.

References

1. Mason S., 'The Characteristics of Electronic Evidence' in Mason S. (ed) Electronic Evidence: Disclosure, Discovery and Admissibility (LexisNexis Butterworth, 2007) 23.
2. ibid.
3. US-CERT, 'Computers Forensics', <https://www.cisa.gov> accessed 30 March 2023; NITDA, 'Standard for Digital and Computer Forensic in Nigeria'<https://www.pdffiller.com>accessed 30 March 2023.
4. Prahlow J., Forensic Pathology for Police, Death Investigators, Attorneys and Forensic Scientists (Springer, 2010) 17-33.
5. Casey E., Digital Evidence and Computer Crimes (3rdedn, Elsevier Inc., 2011) 21.
6. Oettinger W., Learn Computer Forensics (2nd edn, Packt Publishing Limited, 2022) 57.
7. Casey (n 5) 482.
8. Wh. 2371211 E. D. (Pa. June 10. 2008).
9. 200 F.3d 627 (2000).
10. Ajileye A. O., Electronic Evidence (Samok Printers, 2019) 105.
11. ibid.
12. FRN v Fani Kayode (2010) 14 NWLR (Pt. 1214) 481. See also Nuba Commercial Farms v NAL Merchant Bank (2003) FWLR (Pt. 145) 661; UBA v Sani Abacha Foundation for Peace and Unity; (2004) 3 NWLR (Pt. 861) 516.
13. The Evidence Act, Cap 112, LFN 1990.
14. Evidence Act 2011 s 258.
15. (2012) LPELR – 9817 Supreme Court (SC).
16. (2013) LPELR- 22828 Court of Appeal (CA).
17. Rosehill Limited v Guarantee Trust Bank CA/K/243/2014; A. O Ajileye, A Compendium of Cases on Electronic Evidence (vol. 1. Jurist Publication Series (JPS), 2020) 242-263.
18. (2018) LPELR- 43926 (CA).
19. (2019) LPELR-48897 (CA).
20. (2019) LPELR - 4703 (CA).
21. Repealed by the Youth Justice and Criminal Evidence Act, 1999.
22. (1991) CLR 199.
23. (1993) 1 All ER 225.
24. (2017) 6 NWLR (Pt.1560) 90.
25. R. Stoykova, 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence' <https://www.sciencedirect.com> accessed 23 March 2023.
26. (2017) 7 NWLR (Pt. 1567) 167.
27. Ajileye (n 10) 236.
28. (2019), EWHC 340 (QB).
29. (2018) LPELR-45650 (CA).
30. Brila's case (n 18).
31. Blackstone W., Commentaries on the Laws of England

(9th edn, Garland Pub, 1978) 338.
32. Franklin B., Respectfully Quoted: Dictionary of Quotations (Dover Publications, 1989).
33. Rizolli M. and Saraceno M., 'Better that Ten Guilty Persons Escape: Punishment Cost Explain the Standard of Evidence'<https://www.jstor.ors/stable/42003107> accessed 8th September 2023.
34. Federal Rules of Evidence 2023 r 901 (a).
35. United States v Vayner F. 3d WL 4942227 (2d Cir. 2014).
36. ibid.
37. U.S. Dist. Lexis 166799 (N.D. G9. 2014).
38. 435 F. Supp 2d.36 40 (D. D. C 2006).
39. 152 F. 3dd 124 (10th Cir. 2014).
40. U. S. Dist. Lexis 110166 (E. D. Mich. 2012).
41. 585 F. Supp. 2d.679, 686- 88 n. 4 (D. Md 2008).
42. 742. F. 3d. 104, 132-134 (4th Cir. 2014).
43. U.S. Dist. Lexis 39187 (ND Ala. Mar. 27, 2015).
44. Osipitan T., 'Admissibility of Electronic Evidence: The Imperatives of Oral Evidence and Certificate of Authentication' being a Paper delivered at the National Judicial Institute Workshop on 21 May 2018.
45. ibid.
46. ibid.
47. ibid.
48. 1976 (2) SA 573 (A) at 575.
49. 49. Watney, M. 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position (2009) (1) Journal of Information, Law & Technology (JILT) <HTTP://go.warwickiac.u/c/jilt> accessed 7 March 2024.
50. ibid.
51. Hofman J., 'South Africa' in S. Mason ed. Electronic Evidence: Disclosure, Discovery and Admissibility (Butterworth, 2007) 459.
52. Criminal Justice Act 2003 s 129 (2).
53. Cross R., and Tapper C., On Evidence (13thedn, Oxford University Press, 2018).
54. Mason S., 'England and Wales' in S. Mason (ed) Electronic Evidence: Disclosure, Discovery and Admissibility (1st edn, LexisNexis Butterworth, 2007) 210.
55. Bate's case (n 28).
56. Gaze B., 'The Legal Rule that Computers Are Presumed to be Operating Correctly-Unforeseen and Unjust Consequences' <https://www.benthomsgaze.org/2022> accessed 30 August 2023.
57. R v Robson (Benard Jack) (1972) 1 WLR 1; R v Harris (Gordon Frederick) (1972) 56 Cr. App Rep 450.
58. (1989) 1 WLR 441.
59. Federal Rules of Evidence 2023 r 901(a-b); 902 (1-12).
60. Gaze (n 56).
61. Federal Rules of Evidence 2023 r 902 (5-12).