Volume 20, No. 1
2017

ISSN 0189 0255

The Nigerian Law Journal

CONTENTS

The *NIS ISO* Social Responsibility Guidance Standard Mantra for All Organisations	**Felicia Nwanne Monye**	1
Revisiting the Traditional Irac Organisational Structure for Legal Analysis: Towards A Multidisciplinary Approach	**Oghenemaro Festus Emiri** **Ayuba Giwa** **Jonathan Ehusani**	31
An Overview of the Process of Constitutionalising Existing Laws under the 1999 Constitution	**Akeem Olajide Bello**	77
Conceptual Differentiation in the Definitions of Law of Rape	**Obi Peter Okonkwo**	91
Revisiting the Effects of Colonialism on the Development of Customary Laws in Nigeria	**Oluwabusayo T. Wuraola** **Hameenat Bukola Ojibara**	108
Domestic Terrorism and the Application of International Humanitarian Law in Protecting Internally Displaced	**Babatunde I.O.** **Omidoyin T.J.**	123
Legal Approach to Causes and Consequences of Oil Spillage in Nigeria	**Rose Ohiama Ugbe** **Anthony Ekpoudo**	145
Advancing Charitable Trust as a Model for Governance of Bio-Banking Research in Nigeria	**Simisola O. Akintola**	169
Policing the Police: The Role of Media in Monitoring the National Assembly in the Discharge of Their Duties	**Ngozi J. Udombana**	187
Admitting Computer-Based Evidence in Nigeria: Resonances from South Africa, India and the U.K.	**Ikenga K.E. Oraegbunam**	201
Mechanisms for Recovery and Repatriation of Stolen Assets under the United Nations Convention against Corruption	**Ifeolu J. Koni**	242
Analysis of Nexus between Redundancy and Industrial Democracy in Labour Relations	**David Tarh-Akong Eyongndi**	261

Vol. 20, No. 1, 2017

EDITORIAL BOARD

1. Professor Adeniyi I. Olatunbosun, Editor-In-Chief of the Nigerian Law Journal (NLJ), Dean, Faculty of Law, University of Ibadan. tunbosuniyi@yahoo.com 08037253088
2. Professor Timothy Yerima, Deputy Editor in Chief, NLJ, Faculty of Law, Kogi State University. tfyerimah1@yahoo.com 08068472564
3. Professor Y. Y. Bambale, Member Editorial Board, NLJ, Dean, Faculty of Law, Ahmadu Bello University, Zaria. yybambale@yahoo.com 08034529872
4. Dr Maryam Ishaku Gwangndi, Member, Editorial Board, NLJ, University of Maiduguri, kamaldaud@yahoo.com 07036925241
5. Dr Osita Ogbu, Member, Editorial Board, NLJ, Dean, Anambra State University ositaogbu2005@yahoo.com 08039143119
6. Dr. M. D. Mahmud, Member Editorial Board, NLJ, Dean, Usman Danfodio University, Sokoto. muawiyadahiru1968@gmail.com 08036043054
7. Mr. Bob Osamor, LL.B, BL, LL.M, Member Editorial Board, NLJ, DG Nigerian Law School, Enugu Campus, bobosamor2@yahoo.com 08037038828
8. Dr. Elijah Oluwatoyin Okebukola, Member & Secretary Editorial Board, NLJ, Faculty of Law, Nasarawa State University, Keffi. elijah.okebukola@gmail.com 08104512103

This Journal should be cited as (2017), Vol. 20, N0.1 Nig, L.J.

Published in 2017 by
The Nigerian Association of Law Teachers,
The Secretariat,
The Nigerian Association of Law Teachers,
C/o Professor Adeniyi I. Olatunbosun
Faculty of Law, University of Ibadan, Ibadan, Nigeria

ISSN 0189 0255

© 2017 The Faculties of Law of Nigerian Universities, the Nigerian Law School, and the Nigerian Institute of Advanced Legal Studies

Printed by Yinkatec Printers Nigeria Ltd,
No. 25 Adelaja Street, Mokola, Ibadan
Email: yinkatec@yahoo.com yinkatec@gmail.com
Phone: 234 806 7971 788, 234 807 5434 106

Layout and Design by:
Davidolladustries, david@davidollad.com, Mobile: +2347038406891

Articles

The *NIS ISO* Social Responsibility Guidance Standard Mantra for All Organisations – ***Felicia Nwanne Monye*** 1

Revisiting the Traditional Irac Organisational Structure for Legal Analysis: Towards A Multidisciplinary Approach ***Oghenemaro Festus Emiri, Ayuba Giwa, and Jonathan Ehusani*** 31

An Overview of the Process of Constitutionalising Existing Laws under the 1999 Constitution - **Akeem Olajide Bello** 77

Conceptual Differentiation in the Definitions of Law of Rape ***Obi Peter Okonkwo*** 91

Revisiting the Effects of Colonialism on the Development of Customary Laws in Nigeria ***Oluwabusayo T. Wuraola and Hameenat Bukola Ojibara*** 108

Domestic Terrorism and the Application of International Humanitarian Law in Protecting Internally Displaced Persons in Nigeria - ***Babatunde I.O.*** **and** ***Omidoyin T.J.*** 123

Legal Approach to Causes and Consequences of Oil Spillage in Nigeria - ***Rose Ohiama Ugbe and Anthony Ekpoudo*** 145

Advancing Charitable Trust as a Model for Governance of Bio-Banking Research in Nigeria – ***Simisola O. Akintola*** 169

Policing the Police: The Role of Media in Monitoring the National Assembly in the Discharge of Their Duties – ***Ngozi J. Udombana*** 187

Admitting Computer-Based Evidence in Nigeria: Resonances from South Africa, India and United Kingdom – ***Ikenga K.E. Oraegbunam*** 224

Mechanisms for Recovery and Repatriation of Stolen Assets under the United Nations Convention against Corruption – ***Ifeolu J. Koni*** 242

Analysis of Nexus between Redundancy and Industrial Democracy in Labour Relations – ***David Tarh-Akong Eyongndi*** 261

Call for Papers 284

10

Admitting Computer-Based Evidence in Nigeria: Resonances from South Africa, India and United Kingdom

Ikenga K.E. Oraegbunam*

Abstract

Use of computers and computer-related systems is fast replacing the traditional method of writing and documentation. Communication, financial transactions, voting, and even criminality, to say the least, find in computers an easy medium. The courts are therefore confronted with the challenges of technical advances, especially as they relate to the treatment of electronically generated evidence. No doubt, the question of admissibility of evidence in a court of law or tribunal is crucial to any trial, civil or criminal, as it can determine the outcome of a case one way or the other. How a court countenances or discountenances a particular piece of evidence is therefore of utmost significance. This paper seeks to examine the nature and extent of the conditionality for the admission of electronically generated evidence under the Nigerian Evidence Act 2011. The study compares its findings with similar provisions under Indian, South African, and English laws with a view to chatting the way forward for the improvement of Nigeria justice system.

Keywords: Computer-based evidence, Admissibility, Nigeria, South Africa, India, English law

1. Introduction

Evidence Act 2011 repealed the Evidence Act[1] that came into force in 1945. The need to enact the Act, no doubt, bordered on the exigency that is created by the advancement in Information and

* Ikenga K.E. Oraegbunam. PhD (Law), PhD (Phil.), PhD (Rel. & Soc.), MEd, BTh, BL, Senior Lecturer and Ag Head, Department of International Law and Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, P.M.B. 5025, Awka, Anambra State, Nigeria. Email:

Communications Technology (ICT).[2] Issues of admissibility of computer print-outs of banks' statement of accounts, video tapes, compact disks, and the like materials caused long debates in Nigerian courts, thereby advancing a negative toll on precious judicial time needed, as it were, for much desired dispensation of legal justice. The result was that courts and judicial panels differed among themselves as to the admissibility of electronically generated evidence. Hitherto, the definition of 'documents' did not seem to cover computer programmes and products. Judicial activism was highly demanded in order to exploit the principle of judicial notice which recognizes progress in science and technology, *inter alia*, to admit in evidence computer generated resources. But even at that, the atmosphere of the old evidential regime could not allow the activist judges to attach much weight to the evidence as it was often classified as secondary merely. This state of affairs held sway for almost seven decades even when human activities and transactions were fast growing soft and paperless. The result became for a long time an ugly legal monster and constituted a clog in the wheel of judicial progress and justice dispensation.

The Evidence Act 2011 provides for the admissibility of electronic and computer generated evidence and widens the scope of the definition of documents to include computer print-outs, compact disks, electronic messages, video tapes, and so on. Hence, document now includes – (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 disc, 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] Similarly, for the first time in Nigerian evidence statute, the word computer is defined as 'any device for storing and processing information, and any reference to information being derived from other information is a reference to

[2] Evidence is the item 23 of the Exclusive Legislative List in Part I of the Second Schedule of the Constitution of the Federal Republic of Nigeria, 1999 (as amended).

[3] Evidence Act, 2011, section 258.

its being derived from it by calculation, comparison or any other process'[4].

This paper seeks to examine the nature and extent of the conditionality for the admission of electronically generated evidence under the Nigerian Evidence Act 2011. The study compares its findings with similar provisions under Indian, South African, and English laws with a view to chatting the way forward for the improvement of Nigeria justice system.

2. Conditions for Admissibility of Electronic Evidence under Section 84 (2) & (4) of the Evidence Act

The admissibility of statements in documents produced by computer is governed in Nigeria by section 84 of the Evidence Act 2011. The provisions of section 84 are summarized thus: Subsection (1) makes a computer generated statement admissible in both civil and criminal proceedings. Subsection (2) provides for the conditions to be fulfilled, which are that the computer must be in regular use to store or process information of activities carried on over that period; that such supply was made regularly, in the ordinary course of business; that the computer was operating properly, or where it was not, that it was not such as to affect the accuracy of the statement; that the information derived was supplied in the ordinary course of those activities. Subsection (3) provides for the ways in which the computer(s) performed the function. This could be by a combination of computers; or different computers operating in succession; or different combinations of computers operating in succession; or in any other manner involving the successive operation, whatever order, and shall be treated as constituting a single computer. Subsection (4) provides for the proof of any statement produced by a computer to be given in evidence, to be made by a certificate to that effect. Subsection(5) provides that information supply to a computer may be made either directly or by means of any appropriate equipment; that information duly supplied to a computer though outside the ordinary course of activities shall be deemed to be appropriately done, though, depending on the circumstances of the case.

Besides, the Evidence Act 2011 has resolved the primary-secondary evidence controversy in respect of computer generated documents. Section 85 permits the content of a document to be proved either by primary or secondary evidence, while section 88 is categorical in providing that documents (as distinct from contents) shall be proved

[4] Ibid.

Communications Technology (ICT).[2] Issues of admissibility of computer print-outs of banks' statement of accounts, video tapes, compact disks, and the like materials caused long debates in Nigerian courts, thereby advancing a negative toll on precious judicial time needed, as it were, for much desired dispensation of legal justice. The result was that courts and judicial panels differed among themselves as to the admissibility of electronically generated evidence. Hitherto, the definition of 'documents' did not seem to cover computer programmes and products. Judicial activism was highly demanded in order to exploit the principle of judicial notice which recognizes progress in science and technology, *inter alia*, to admit in evidence computer generated resources. But even at that, the atmosphere of the old evidential regime could not allow the activist judges to attach much weight to the evidence as it was often classified as secondary merely. This state of affairs held sway for almost seven decades even when human activities and transactions were fast growing soft and paperless. The result became for a long time an ugly legal monster and constituted a clog in the wheel of judicial progress and justice dispensation.

The Evidence Act 2011 provides for the admissibility of electronic and computer generated evidence and widens the scope of the definition of documents to include computer print-outs, compact disks, electronic messages, video tapes, and so on. Hence, document now includes – (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 disc, 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] Similarly, for the first time in Nigerian evidence statute, the word computer is defined as 'any device for storing and processing information, and any reference to information being derived from other information is a reference to

[2] Evidence is the item 23 of the Exclusive Legislative List in Part I of the Second Schedule of the Constitution of the Federal Republic of Nigeria. 1999 (as amended).

[3] Evidence Act, 2011, section 258.

its being derived from it by calculation, comparison or any other process'[4].

This paper seeks to examine the nature and extent of the conditionality for the admission of electronically generated evidence under the Nigerian Evidence Act 2011. The study compares its findings with similar provisions under Indian, South African, and English laws with a view to chatting the way forward for the improvement of Nigeria justice system.

2. Conditions for Admissibility of Electronic Evidence under Section 84 (2) & (4) of the Evidence Act

The admissibility of statements in documents produced by computer is governed in Nigeria by section 84 of the Evidence Act 2011. The provisions of section 84 are summarized thus: Subsection (1) makes a computer generated statement admissible in both civil and criminal proceedings. Subsection (2) provides for the conditions to be fulfilled, which are that the computer must be in regular use to store or process information of activities carried on over that period; that such supply was made regularly, in the ordinary course of business; that the computer was operating properly, or where it was not, that it was not such as to affect the accuracy of the statement; that the information derived was supplied in the ordinary course of those activities. Subsection (3) provides for the ways in which the computer(s) performed the function. This could be by a combination of computers; or different computers operating in succession; or different combinations of computers operating in succession; or in any other manner involving the successive operation, whatever order, and shall be treated as constituting a single computer. Subsection (4) provides for the proof of any statement produced by a computer to be given in evidence, to be made by a certificate to that effect. Subsection(5) provides that information supply to a computer may be made either directly or by means of any appropriate equipment; that information duly supplied to a computer though outside the ordinary course of activities shall be deemed to be appropriately done, though, depending on the circumstances of the case.

Besides, the Evidence Act 2011 has resolved the primary-secondary evidence controversy in respect of computer generated documents. Section 85 permits the content of a document to be proved either by primary or secondary evidence, while section 88 is categorical in providing that documents (as distinct from contents) shall be proved

[4] Ibid.

by primary evidence except in the cases mentioned in the Evidence Act as where, going by section 89, 'the original of the document is in the possession or power of the person against whom the document is sought to be proved, or the original has been destroyed or lost, or the original is not easily movable, or the original is a public document within the meaning of section 102, or the original consists of numerous account or other documents which cannot conveniently be examined in court and the fact to be proved is the general result of the whole collection, or the document is an entry in a banker's book'. Hence, In addition to other forms of primary evidence provided in section 86 (1) – (3), section 86 (4) goes to make specific provision regarding the subject matter of this study by including computer generated evidence into the league of primary evidences:

> Where a number of documents have all been made by one uniform process, as in the case of printing, lithography, photography, *computer* or other electronic or mechanical process, each shall be primary evidence of the contents of the rest; but where they are all copies of a common original, they shall not be primary evidence of the contents of the original (italics mine).

Section 87(b) of the Act then provides that copies made from the original by mechanical or electronic processes, which in themselves ensure the accuracy of the copy, and copies compared with such copies shall be secondary evidence. By the combined effect of sections 86 (4) and 87 (b), it would appear that the Supreme Court decision in *Anyaebosi v. R.T Briscoe*[5] to the effect that a computerized statement constitutes secondary evidence of the original is no longer tenable. Computerized statements are now clearly primary evidence.

On proof of execution of documents, section 93 of the Act provides as follows:

> (1) If a document is alleged to be signed or to have been written wholly or in parts by a person, the signature or the hand writing of so much of the document as is alleged to be in that person's handwriting must be proved to be in his handwriting.
>
> (2) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.
>
> (3) An electronic signature may be proved in any manner, including by showing that a 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.

5 *Anyaebosi v. R.T Briscoe* (1987) 6 SC 15.

The Evidence Act 2011 is thus welcome in Nigeria. The provisions on the admissibility of computer generated evidence and more as primary, provision on the acceptability of electronic signature, and the inclusion of computer files and programmes into the definition of documents are a milestone not only in combating cybercriminality which veritable medium is the computer and computer-related devices, but also towards integrating Nigeria into the one-world order *vide* the globalization process.

The conditions are thus:

a. The document containing the statement must be produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities. Such activities must be regularly carried on over that same period;
b. The information supplied to the computer in the ordinary course of those activities must be of the kind contained in the statement or the kind from which the information contained in the statement was derived;
c. The computer was in proper working condition throughout the material part of the period. Where it was not, it must be shown that the fault was not such as to affect the production of the document or the accuracy of its contents; and
d. The information contained in the statement must be reproduced or derived from information supplied to the computer in the ordinary course of those activities.

An illustration may be helpful. If A and B are parties to a proceeding and A is relying on electronically generated evidence to prove that B a bank manager laundered money, before the evidence becomes admissible A must show that-

a. The document containing the statement (evidence) was produced by a computer used regularly to store or process information of the banking activities, the banking activities must have been carried on regularly over the period in question;
b. The information supplied to the computer over the period is the same kind of information sought to be proved by the statement in the document, that is, record of cash transactions;
c. The computer was working properly; if not, that the fact that it was faulty did not affect the authenticity of the document, that is, its production and accuracy of its contents; and
d. The information contained in the statement (evidence) was reproduced or derived from the information supplied to the computer.

The jurisprudence of the above conditions is founded on the fact that it is easy to create, alter or destroy electronic evidence as computers are manipulable devices. What these conditions have done is to prevent a situation where parties to a suit will take advantage of these frail features of electronically generated evidence by cooking up evidence favourable to their case before coming to court. This purpose is achieved by the implication of expressions such as 'used regularly to store or process information' 'ordinary course of activities' and 'activities regularly carried on over that period'. The implication of these expressions is that the information contained in the statement sought to be adduced in evidence would be of events or activities which occurred before the suit was instituted and at a time where neither of the parties had the possibility of such suit in mind, hence, the evidence will be unbiased and accurate.

Besides, due to the uniqueness of this type of evidence and its frail features portrayed above, section 84 (4) provides a special form through which it can be tendered in evidence. Thus, by virtue of section 84 (4) where electronic evidence is sought to be tendered in evidence, it should be accompanied with a certificate:

a. identifying the document containing the statement and describing manner in which it was produced
b. giving such particulars of the device used to produce the document, for the purpose of showing that the document was produced by a computer.

Furthermore in view of subsection (2) the certificate 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, as the case may be. It is sufficient if the matter

stated in the certificate is made to the best of the knowledge and belief of the person stating it.

3. Admissibility of Electronically Generated Evidence in some Foreign Jurisdictions

As was the case in Nigeria, technological development took the evidence law of some foreign jurisdictions unawares. Within a few years, most evidence laws across the globe became obsolete and needed amendments to come to terms with societal changes and realities. However, unlike Nigeria some of these jurisdictions responded quickly to these changes. An overview of three of such jurisdictions may be *apropos*.

India

The Indian experience may be illustrative. The Indian Evidence Act, 1872 did not provide for the admissibility of electronic evidence. However, the law courts in India devised and developed principles so that such evidence may be received in law courts and acted upon. Though the relationship between law and technology was not an easy one, the law was always bent in favour of technology whenever it was necessary. In India, the earliest case in which the issue of admissibility of electronically generated evidence came into consideration was *Rupchand v Mahabir Prasad*[6]. In this case, though the court declined to treat tape-recorded conversation as a document within the meaning of section 3 (65) of the General Clauses Act it allowed it to be adduced as evidence under section 155(3) of the Evidence Act as 'previous statement to shake the credibility of a witness'[7]. The Apex court in *Ziyauddin Burhanuddin Bukhari v Brijmohan Ramdas Mehta*[8], took a radical step in favour of electronic evidence when it held that electronic evidence (tape-recorded speeches) were 'document as defined by section 3 of the Evidence Act'. This decision among other things set the tone for the eventual amendment of the Indian Evidence Act, 1872.

The Indian Evidence Act was eventually amended by the Information Technology (IT) Act, 2000[9]. The IT Act is based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce. It also

---

6 *Rupchand v Mahabir Prasad* AIR 1956, Punjab 173.
7 Indian courts also interpreted the law to accommodate electronic evidence in the following *cases S.S Pratap Singh v. State of Punjab*, AIR 1964, SC 72; *Yusufalli Esmail Nagree v State of Maharashtra*, AIR 1962, SC 147.
8 *Rupchand v Mahabir Prasad* AIR 1975, SC 1788.
9 Its commencement date was 17th day of October 2000.

amended the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891. These amendments reformed the traditional concept of evidence. Section 2(r) of the IT Act is relevant in this respect. It defines information in electronic form as information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device. Under section 2(t) 'electronic record' means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. Section 92 of the Act read with Schedule (2) amends the definition of 'evidence' as contained in section 3 of the Indian Evidence Act. The amended definition is thus:

> Evidence means and includes:
>
> (1)all statements which the court permits or requires to be made before it by witness, in relation to matters of fact under inquiry such statement is called oral evidence;
> (2)all documents including electronic records produced for the inspection of the court; such documents are called documentary evidence.

Further changes to India's Evidence Act in relation to electronic evidence include[10] provisions on admission and admissibi'ity of digital evidence. The definition of 'admission'[11] was changed to include a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or relevance. New section 22A was inserted into the Evidence Act to provide for the relevancy of oral evidence regarding the contents of electronic records. It provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question.

New Sections 65A and 65B were introduced to the Evidence Act under the Second Schedule to the IT Act. New provision, section 65A, provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B. Section 65B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record (i.e., the contents of a document or communication printed on paper that has

[10] T.Karia, *Digital Evidence: An Indian Perspective*, February 10, 2009. Retrieved from www.internationallawoffice.com/newsletters/detail Last visited on 14-07-15.

[11] Section 17 of the Evidence Act.

been stored, recorded and copied in optical or magnetic media produced by a computer ('computer output')), is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set out in Section 65B(2) to (5) are satisfied. It should be noted that these conditions are in *pari materia* with the conditions for admissibility of electronically generated evidence stipulated in section 84 (2) to (5) of our Evidence Act, 2011.

Furthermore, under Indian law on the admissibility of digital evidence, before a computer output is admissible in evidence, the following conditions as set out in Section 65(B) (2) must be fulfilled:

> (2) The conditions referred to in subsection (1) in respect of a computer output shall be the following, namely:
> (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
> (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
> (c) throughout the material part of the said period the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
> (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period the function of

Section 65B (4) provides that in order to satisfy the conditions set out above, a certificate of authenticity signed by a person occupying a responsible official position is required. Such certificate will be

evidence of any matter stated in the certificate[12]. The certificate must also deal with any of the matters to which the conditions for admissibility relate.

There is also no gainsaying that generally, a fact which is relevant and admissible need not be construed as a proven fact. The judge must appreciate the fact in order to conclude that it is a proven fact. The exception to this general rule is the existence of certain facts specified in the Indian Evidence Act that can be presumed by the court. The Indian Evidence Act has been amended to introduce various presumptions regarding digital evidence. These presumptions are: Under the provisions of Section 81A of the Evidence Act(as amended), the court presumes the genuineness of electronic records purporting to be from the Official Gazette or any legally governed electronic record, provided that the electronic record is kept substantially in the form required by law and is produced from proper custody. Again, Section 84A of the Evidence Act provides for the presumption that a contract has been concluded where the parties' digital signatures are affixed to an electronic record that purports to be an agreement. More still, Section 85B of the Evidence Act provides that where a security procedure has been applied to an electronic record at a specific time, the record is deemed to be a secure electronic record from such time until the time of verification. Unless the contrary is proved, the court is to presume that a secure electronic record has not been altered since obtaining secure status. The provisions relating to a secure digital signature are set out in Section 15 of the IT Act:

> A secure digital signature is a digital signature which, by application of a security procedure agreed by the parties at the time that it was affixed, is:
> - unique to the subscriber affixing it;
> - capable of identifying such subscriber; and
> - created by a means under the exclusive control of the subscriber and linked to the electronic record to which it relates in such a manner that if the electronic record was altered, the digital signature would be invalidated.

[12] The certificate must:
- identify the electronic record containing the statement;
- describe the manner in which it was produced; and
- give such particulars of any device involved in the production of the electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer.

It is presumed that by affixing a secure digital signature the subscriber intends to sign or approve the electronic record. In respect of digital signature certificates[13], it is presumed that the information listed in the certificate is correct, with the exception of information specified as subscriber information that was not verified when the subscriber accepted the certificate.

There is also a presumption in respect of electronic messages. By virtue of the provisions of Section 88A, it is presumed that an electronic message forwarded by a sender through an electronic mail server to an addressee corresponds with the message fed into the sender's computer for transmission. However, there is no presumption regarding the person who sent the message. This provision presumes only the authenticity of the electronic message and not the sender of the message. Yet another presumption is with regard to five-year old electronic records. Hence, the provisions of Section 90A of the Evidence Act make it clear that where an electronic record is produced from custody which the court considers to be proper and purports to be or is proved to be five years old, it may be presumed that the digital signature affixed to the document was affixed by the signatory or a person authorized on behalf of the signatory. An electronic record can be said to be in proper custody if it is in its natural place and under the care of the person under whom it would naturally be. At the same time, custody is not considered improper if the record is proved to have had a legitimate origin or the circumstances of the particular case are such as to render the origin probable. The same rule also applies to evidence presented in the form of an electronic copy of the *Official Gazette*.

It is also good to note that there are changes to Banker's Book Evidence Act. The definition of 'banker's book' has been amended to include the printout of data stored on a floppy disc or any other electro-magnetic device[14]. Section 2A provides that the printout of an entry or a copy of a printout must be accompanied by a certificate stating that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager, together with a certificate from a person in charge of the computer system, containing a brief description of the computer system and the particulars of its safeguards.

[13] Section 85c of the Indian Evidence Act, *1872*.
[14] Ibid, section 2(3).

Again, a number of offences were introduced under the provisions of the First Schedule of the IT Act, which amended the Penal Code with respect to offences for the production of documents that have been amended to include electronic records. The range of additional offences includes:

- absconding to avoid the production of a document or electronic record in a court[15];
- intentionally preventing the service of summons, notice or proclamation to produce a document or electronic record in a court[16];
- intentionally omitting to produce or deliver up the document or electronic record to any public servant[17];
- fabricating false evidence by making a false entry in an electronic record or making any electronic record containing a false statement, and intending the false entry or statement to appear in evidence in judicial proceedings[18];
- the destruction of an electronic record where a person hides or destroys an electronic record or obliterates or renders illegible the whole or part of an electronic record with the intention of preventing the record from being produced or used as evidence[19]; and
- making any false electronic record[20].

Another innovative step taken by Indian courts is the admission of examination of a witness by video conference. In *State of Maharashtra v. Dr Praful B Desai*[21] the question of whether a witness can be examined by means of a video conference was brought before the court for determination. The Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. The court allowed the examination of a witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence.

15 Indian *Penal Code*, section 172.
16 Ibid, section 173.
17 Ibid, section 175.
18 Ibid., sections 192 and 193.
19 Ibid., section 204.
20 Ibid., sections 463 and 465.
21 *State of Maharashtra v. Dr Praful B Desai* (2003) 4 SCC 601.

These legislative changes and the courts' positive approach to recognizing and appreciating digital evidence indicate that India is making progress with respect to the admissibility and appreciation of digital evidence.

South Africa

The Indian experience is not an isolated case. A brief overview of South African regime may prove this assertion. The South Africa law of evidence consists of common and statutory law[22]. The South African system like every other legal system lagged behind technological development. The need for regulative intervention was highlighted with the decision in *Narlis v. South African Bank of Athens*[23]. In this matter it was held that section 34 of the Civil Proceedings Evidence Act 25 of 1965 did not provide for admissibility of issues relating to computer printouts. The section provided for the admissibility under specific circumstances of a statement made by a person in a document, but a computer was not regarded as a person. The Computer Evidence Act 57 of 1983 was therefore placed on the statute book to regulate the admissibility of computer evidence. The Act did not achieve its purpose mainly due to an over captious approach in placing a high premium on authenticity and reliability. As a result, a number of requirements had to be met before admissibility could be achieved. The Computer Evidence Act was also only applicable to civil proceedings, leaving criminal proceedings unregulated. Urgent legislative intervention was therefore required.

The statutory relief came in the form of the Electronics Communications and Transaction Act 25 of 2002 (hereafter referred to as the ECT Act)[24]. It provided for various legal issues including the admissibility of electronic evidence. Section 15 of the ECT Act provides for the admissibility and evidential weight of a data message as electronic evidence. A data message means data generated, sent, received or stored by electronic means and includes

(a) voice, where the voice is used in automated transaction; and
(b) a stored record.[25]

22 M. Watney, "Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position", *2009(1) Journal of Information, Law and Technology (JILT)*, p.3. Retrieved from http://go.warwick.ac.uk/jilt/2009-1/watney-pdf . Last visited on 08-04-15.
23 *Narlis v. South African Bank of Athens* 1976(2) SA 573 (A).
24 It came into operation on 30 August 2002.
25 Electronic Communications and Transactions Act, section 1.

Data is defined as the electronic representation of information.[26] Under the South Africa rules of evidence there are three traditional means of proof, namely: witnesses, objects (real evidence) and documents[27]. There is no consensus as to what form of evidence electronic evidence is and the requirements for its admissibility, that is, whether it is a real evidence or documentary evidence. However, the arguments advanced by legal authors[28] and the court[29] favour the treatment of electronic evidence as documentary evidence. In South Africa, before electronic evidence is admitted, one will have to first look at the facts of the particular case and determine what type of evidence the data message (electronically generated evidence) represents[30]. Once the type of evidence has been determined, a two-phased procedure will be applicable, namely:

(i) To determine the admissibility of the electronic evidence during a trial-within-a-trial and if the evidence is found to be admissible.
(ii) The evidential weight of the evidence has to be determined.

The trial-within-a-trail procedure reflects the exclusionary approach to evidence operative in South Africa. According to Hoffman, 'exclusionary approach can mean a time-consuming 'trial-writer-a-trial' before a court decides whether to admit or exclude the evidence; on the other hand, an exclusionary can save time by not requiring a court to look at evidence on which it will not be able to rely.'[31] After the evidence is determined as being admissible, the presiding judge has to decide the evidential weight to attach thereto. In determining the evidential weight of electronic evidence the judge shall be assisted by the guidelines stipulated in section 15(3) of the ECT act, which provides thus:

In asserting the evidential weight of a data message, regard must be had to:

(a) the reliability of the manner in which the data message was generated, stored or communicated;
(b) the reliability of the manner in which the integrity of the data message was maintained;
(c) the manner in which its originator was identified; and

[26] Ibid.
[27] M. Watney, op cit, p.3.
[28] Schmidt and Rademeyer, *Law of Evidence*, Lexis Nexis Butterworths, Durban, 2006, p.11.
[29] *S v. De Villers* (1993(1) SACR 574 (Nm)).
[30] *S v. Ndiki* [2007] 2 All SA 185 (CK).
[31] J. Hofman as cited in M.Watney, op.cit, p. 4.

(d) any other relevant factor.

Under the South African Law of evidence, a data message (electronic evidence) may qualify as either documentary or real evidence. The rules of evidence applicable to the specific kind of evidence should find application after determination of the kind of evidence at hand. Consequently, rules of evidence applied to electronic evidence are subjective as seen above. As a result of this, some authors have canvassed that a hybrid of the evidential rules applicable to documentary and real evidence should govern the admissibility of data messages. However, this suggestion is not generally supported because if differential treatment is applied between information in electronic format and that in written format, it will either result in discriminating against those transacting electronically or giving them an unfair advantage.[32]

England

More still, like every other legal system, England had its fair share experience of trying to catch up with the pace of technological development. Initially, a proposition was posited which tended to put electronic evidence within the ambit of hearsay evidence. However, commercial needs always drove the courts to include electronically generated evidence as an exception to the general rule on hearsay.[33]

In England, a distinction is made between admission of electronic evidence in civil litigation and in criminal proceedings. In civil litigation, there are no requirements which must be met before a document (which would include a digital document) can be admitted in evidence[34]. The position is a little different in criminal cases, as the House of Lords in *R v. Shepherd*[35], decided that the provisions of section 69 of the Police and Criminal Evidence Act (PACE) 1984 apply to all computer records, whether they are hearsay or not[36].

[32] Ibid, p.11.
[33] W. Claydon, *Computer Evidence-General*. Retrieved from www.swarb.co.uk/law/lvh.html. Last visited on 17-04-12.
[34] House of Lords-Science and Technology Committee Fifth Report. Retrieved from www.parliament.the – stationary-office.co.uk/pa.htm . Last visited on 17-04-12.
[35] *R v. Shepherd* (1993) All ER 225.
[36] House of Lords- Science and Technology Committee, *op cit* .

Section 69 of PACE refers to the admissibly of evidence from a computer, and requires assurances about whether the equipment was being used properly and was functioning normally at the time. The implication of section 69 is that any party relying on computer evidence has to provide oral or written certification of the reliability of the computer[37]. Section 69 provides thus:

> 1. In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown:
> a. that there is no reasonable ground for believing that the statement is inaccurate because of improper use of the computer;
> b. that at all material times, the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents, and
> c. that any relevant conditions specified in rules of court under subsection (2) below are satisfied.
> 2. Provision may be made by rules of court requiring that in any proceedings where it is desired to give a statement in evidence by virtue of this section such information concerning the statement as may be required by the rules shall be provided in such form and at such time required.

4. Conclusion and Recommendations

This paper has analyzed the legal position of electronically generated evidence as well as its admissibility in legal proceedings in Nigeria, India, South Africa, and England. The study observed that law needs to keep pace with technological and electronic advance. In Nigeria, prior to the repeal of the old Evidence Act, the admissibility status of electronically generated evidence was hanging in the balance. This worked great hardship on Nigeria judicial process as the legal system scrambled to keep up with the speed of technological development. The efforts of the courts in the face of this challenge are highly commendable. Some judges rose up to their responsibilities and made judicial pronouncements furnished with logical *ratio decidendi* on an issue which the existing law did not put into perspective. Though these pronouncements could be said to be controversial in light of the Supreme Court conflicting *dicta* in the cases of *Esso W.A v T.O.*

[37] Ibid.

Oyegbola[38] and *Yesufu v ACB*[39], at the time it was enough to hold the reins and ensure a level of stability in the law of evidence as it relates to electronic evidence. In the light of the above, it became pertinent for a legislative intervention, as it was obvious that justice was being miscarried by relying on an Evidence Act that has grown otiose and anachronistic. This intervention was also clamoured for by legal writers, lawyers, judges and every other concerned party who have all criticized the inertness of the legislature[40].

Bearing in mind the novelty of the law providing for the admissibility of electronic evidence in Nigerian legal system, the need for the courts to tread carefully and cautiously in its application cannot be overstressed. This is because judicial pronouncements by superior courts made on the basis of this law would set a new *stare decisis* (binding precedent) for lower courts to follow and reaching such decisions erroneously would frustrate the purpose of the provision. In applying the provisions of section 84, a comprehensive study and understanding of its provision must be done. It may be necessary for the courts to make recourse to foreign jurisdictions where electronic evidence has since been admissible, in order to share in their experience and learn from the mistakes they have made in admitting electronically generated evidence. Hence, the interpretation of Section 84 of the Evidence Act 2011 may need to draw strength from the decisions of English and Indian courts, given the paucity of judicial authorities on the subject in Nigeria. In applying these foreign authorities, courts should, nevertheless, ensure that only current authorities and legislation are applied and relied upon in their decisions.

Furthermore, the frailty and manipulability of electronic evidence and electronic devices respectively must always be borne in mind by the courts when handling electronic evidence. Thus the condition for admissibility provided for in section 84 (2) must be strictly adhered to so as to reduce the possibility of admission of inadmissible and inaccurate electronically generated evidence by the court. It is however strongly suggested that the use of video conferencing in examining a witness and provisions for presumptions regarding digital evidence expressed in the Indian law of evidence should be adopted *mutatis mutandis* into Nigerian law of evidence.

[38] *Esso West Africa Inc v. T. Oyegbola* (1969) 1 NMLR, 194
[39] *Yesufu v. ACB* [1976] 1 ANLR (pt 1) 328; (1976) 4 SC 1 at 16
[40] *Ibid.*

The Legislature should go beyond just making electronically generated evidence admissible in the Evidence Act; it should also enact other laws which regulate e-transactions and fight e-crimes. Corresponding amendments and/or reviews should be made of such laws like Copyright Act, Freedom of Information Act, Money Laundering (Prohibition) Act, Examination Malpractice Act, Economic and Financial Crimes (Establishment) Act, Taxation laws and other such laws against which the emergence of computer and the Internet has posed veritable challenge. Thus, there needs to be a holistic overhaul of the relevant legal regime for synergy in implementation.

Regular workshops, seminars and even institutions should be put in place to educate and train judges, lawyers and every other personnel in the judicial system on the nature and handling of electronically generated evidence. These workshops and seminars should be made mandatory by the Nigeria Bar Association so that in no distant time Nigeria will have a computer literate legal society. In addition, the Council of Legal Education should introduce a course bordering on electronically generated evidence as part of the law school's curriculum so that the school, henceforth, would start producing a new generation of computer literate legal practitioners. Practical implementation of these suggestions in addition to correct interpretation and application of the Evidence Act 2011 would be a recipe for curbing, for instance, cyber criminality, promoting e-commerce, and generally improving justice delivery in Nigeria.