Relevancy and Admissibility Of Digital Evidence: A Comparative Study

Shweta
Research Scholar, Jamia Millia Islamia
New Delhi, India

Tauseef Ahmad
Ph.D. Scholar, Jamia Millia Islamia
New Delhi, India

ABSTRACT:

Due to growth and development in technology there has been enormous change in day to day life. It is very easy to communicate through technology which increasing reliance on electronic means of communication, e-commerce and storage of information in digital form. This rise and development of technology has intense effect on legal rules in legal system especially in the field of evidence. This modern technology has generated and created materials that are considered evidence in courts. It caused a need to transform the law relating to information technology and rules of admissibility of electronic evidence both in civil and criminal matters. This paper is an effort to relook the laws of digital evidence & its admissibility and relevancy while appreciating various issues involved with help of case laws & interpretations in India, USA and UK.

I. INTRODUCTION

In today's world digital devices used everywhere. It helps people to communicate locally and globally with ease. Due to which the reliance on electronic means of communication, e-commerce and storage of information in digital form increasing rapidly. It caused a need to transform the law relating to information technology and rules of admissibility of electronic evidence both in civil and criminal matters. Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device. It is any probative information stored or transmitted in digital form that a party to a court case may use at trial. It is "information of probative value that is stored or transmitted in binary form". It is not only limited to that found on computers but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices. The e-evidence can be found in e-mails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories databases, Contents of computer memory, Computer backups, Computer printouts, Global Positioning System tracks, Logs from a hotel's electronic door locks, Digital video or audio files. Digital Evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available[1]

This definition has three elements-

[1] Vivek Dubey, "*Admissibility of Electronic Evidence: An Indian Perspective*"4,FRACIJ (2017).

First, it is intended to include all forms of evidence that is created, manipulated or stored in a product that can, in its widest meaning, be considered a computer, excluding for the time being the human brain.

Second, it aims to include the various forms of devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition will include any form of device, whether it is a computer as we presently understand the meaning of a computer; telephone systems, wireless telecommunications systems and networks, such as the Internet; and computer systems that are embedded into a device, such as mobile telephones, smart cards and navigation systems.

The third element restricts the data to information that is relevant to the process by which a dispute, whatever the nature of the disagreement, is decided by an adjudicator, whatever the form and level the adjudication takes. This part of the definition includes one aspect of admissibility - relevance only - but does not use 'admissibility' in itself as a defining criteria, because some evidence will be admissible but excluded by the adjudicator within the remit of their authority, or inadmissible for reasons that have nothing to do with the nature of the evidence - for instance because of the way it was collected. The last criteria, however, restricts the definition of electronic evidence to those items offered by the parties as part of the fact finding process.[2]

II. DIGITAL EVIDENCE IN INDIA

Due to enormous growth in e-governance throughout the public and private sector, electronic evidence have involved into a fundamental pillar of communication, processing and documentation and various forms of digital evidence are increasingly being use in both civil and criminal litigation. With this Indian courts have developed case law regarding reliance on electronic evidence and have all necessitated amendments in Indian law to incorporate the provisions on the appreciation of digital evidence. The Information Technology Act, 2000 and its amendment are based on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce. The Information Technology (IT) Act 2000 was amended to allow for the admissibility of digital evidence. An amendment to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in electronic world.

As per provision Sec 2(t) of Information Technology Act 2000[3], 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"

[2] Stephen Mason (ed), *" Electronic Evidence"* (Lexis Nexis , 2013).
[3] The Information Technology Act, 2000, No. 21, Acts of Parliament 2000.

A. Electronic Evidence & The Indian Evidence Act 1872[4]

Following sections of Indian Evidence Act, 1872 deals with electronic evidence:-

Section 3 The definition of evidence as given in the Indian Evidence Act, 1872 covers a) the evidence of witness i.e. oral evidence, and b) documentary evidence which includes electronic record produced for the inspection of the court. Section 3 of the Act was amended and the phrase "All documents produced for the inspection of the Court" was substituted by "All documents including electronic records produced for the inspection of the Court". Regarding the documentary evidence, in **Section 59**, for the words "Content of documents" the words "Content of documents or electronic records" have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence.

S.17 Admission Defined.

The definition of 'admission' (Section 17 of the Evidence Act) has been changed to include a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or of relevance.

S.22A. When oral admissions as to contents of electronic records are relevant.—

New Section 22-A has been inserted into 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. So remember until your evidence's admissibility is in question, none of the corroboration that you provide about its genuineness along is going to be valid.

S. 34. Entries in books of accounts including those maintained in an electronic form, regularly kept in the course of business, are relevant.

S. 35 An entry in any public or other official book, register or record or an electronic record made by a public servant in the discharge of his official duty, or by any other person in performance of a duty is kept, is itself a relevant fact,

S. 39. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.

Where there is,— (i) a longer statement, or (ii) a conversation, or (iii) an isolated document, or (iv) a document contained in a book, or (v) a series of letters of papers, the court has discretion to use the relevant portion of the conversation, document, books or series of letters or papers and requires the production of that portion or pages.

[4] Indian Evidence Act, 1872 , No. 1, Acts of Parliament 1872.

In other words, the evidence shall be given of only explanatory or qualifying part of the statement, document, book etc. Same is applicable to electronic record under the section. The statements made in books cannot be relied on unless supported by contemporaneous records.

What evidence is to be given and to be taken is total discretion of the judge. His discretion is always guided by principles of justice, conscience and convenience.

S. 45A. Opinion of Examiner of Electronic Evidence

When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in Section 79 A of the Information Technology Act, 2000, is a relevant fact.

Explanation: For the purposes of this section, an Examiner of Electronic Evidence shall be an expert.

S. 47A. Opinion as to electronic signature where relevant

Opinion given by examiner of electronic evidence regarding any information transmitted or stored in any computer resource or any other electronic or digital form is relevant fact.

S. 67A. Proof as to digital signature

Except in the case of a secure digital signature, if the electronic signature of any subscriber is alleged to have been affixed to an electronic record the fact that such electronic signature is the electronic signature of the subscriber must be proved.

Section 65B of Indian Evidence Act is under focus in the Judicial and Law Enforcement circles.The main points that makes here are:

a) Section 65B (as well as 65A) of Indian Evidence Act refer to the special provisions of the Act in respect of Electronic Documents. Though Section 65 is referring to "Secondary" documents in paper form, there is no such distinction made as to the electronic document.

b) There is no need to distinguish Primary and Secondary and all documents need to be interpreted by a human being which takes the form of a Section 65B certificate.

c) A "Hard disk" which may contain an electronic document also cannot be considered the "Primary Document" since it is only a "Container" and the real Electronic document is an expression in binary language which cannot be read by a human being and needs to be interpreted with the assistance of a binary reading device (Computer + operating system +Application)

d) Section 65B explains the conditions under which an electronic document can be considered as "Admissible" in a Court as a "Document" and it needs to be suitably confirmed for the Court to accept the document, which is often termed as "Section 65B certificate or Statement"

e) Section 65B refers to a process of producing a "Computer Output" of the electronic document which is the evidence to be admitted and such computer output can be either in the form of a "Print Out" or a "Copy".

f) There is a "Process" by which the electronic document becomes the "Computer output" and Section 65B identifies this as the subject activity which needs to be conducted by a person having lawful control over the computer producing such output and that during the period of such production, the Computer should be working properly etc.

g) The focus of Section 65B is the activity of conversion of the electronic document residing inside a system which can be seen by an observer into a "Computer Output".

h) The other clarifications contained in the Section 65B such as that the the Computer Output could be produced by a combination of computers, acting in succession etc as relating to dynamic creation of an electronic document from a data base and routing it through multiple devices onto a final visible form in the computer of the observer and thereafter its porting into a Printer.

i) Considering these interpretations, the Section 65B certification is a "matter of fact" certification to the effect that "What I saw is what I reproduced as a computer output faithfully" and this can be done by any person who is observing an electronic document in his computer and wants it to be produced as an evidence. It is not necessary that a document from yahoo website has to be certified only by a Yahoo server administrator. Similarly, a statement of account downloaded from an ICICI bank website need not be certified only by the ICICI Bank manager but by any person who can lawfully access the document in electronic form.

j) There is also an important distinction that "Content Owner" is different from "Content Viewer" and Section 65B is meant to be produced by a content viewer. On the other hand the content owner in respect of say a Bank statement is the official Bank manager and he can provide a print out as the owner of the content who understands the content and is considered as an "Expert" in the domain. Anybody else who views the document provides a Section 65B certificate that the print out (or a soft copy) is a faithful reproduction.

It is very important that the legal fraternity and the Judiciary interprets the section properly. Any interpretation that only a "Server Administrator" can provide a certificate under Section 65B is considered incorrect. The server administrator can however provide the certificate but it is not mandatory. The Section 65B certifier is like a photographer who captures a photograph of an event and confirms the process of taking the photograph

though he may not be aware of who is there in the picture and what they are doing. It is left to other "Experts" to interpret the "Content" and impute meaning as only a subject matter expert can do.

S. 73A. Proof as to verification of electronic signature

In order to ascertain whether a electronic signature is that of the person by whom it purports to have been affixed, the Court may direct (1) to produce electronic signature certificate,(2) to apply the public key listed in Electronic Signature Certificate and verify the electronic signature.

S. 81A. Presumption as to Gazettes in electronic forms.

The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law.

S. 85A. Presumption as to electronic agreements:

The Court shall presume that every electronic record purporting to be an agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties.

S. 85B. Presumption as to electronic records and electronic signatures.-

Unless contrary is proved, the Court shall presume that the secure electronic record has not been altered and the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record. Nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any electronic signature.

S. 85C Presumption as to Electronic Signature Certificates.-

Unless contrary is proved, the Court shall presume that the information listed in a Electronic Signature Certificate is correct.

S. 88. And S 88A deals with Presumption as to telegraphic messages and to electronic messages

S 88 concerns with the presumption that the message had been forwarded from the telegraph office and such message had been received by the addressee. There is no presumption as to the person who delivered such message for transmission and S 88A concerns with the presumption of electronic message.

S. 90A. Presumption as to electronic records five years old -

Where an electronic record purports to be or is proved to be five years old and is produced from the proper custody, the court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf.

S. 131. Production of documents or electronic records which another person, having possession, could refuse to produce-

No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.

B. Amendments in Evidence Act 1872 & Its Objective

In the *ANVAR CASE*[5], the Supreme Court noted that "there is a revolution in the way that evidence is produced before the court. In India before 2000, electronically stored information was treated as a document and secondary evidence of these electronic 'documents' was adduced through printed reproductions or transcripts, the authenticity of which was certified by a competent signatory. The signatory would identify her signature in court and be open to cross examination. This simple procedure met the conditions of both sections 63 and 65 of the Evidence Act. In this manner, Indian courts simply adapted a law drafted over one century earlier in Victorian England. However, as the pace and proliferation of technology expanded, and as the creation and storage of electronic information grew more complex, the law had to change more substantially. Under the provisions of Section 61 to 65 of the Indian Evidence Act, 1872, the word "Document or content of documents" have not been replaced by the word "Electronic documents or content of electronic documents". Thus, the intention of the legislature is explicitly clear i.e. not to extend the applicability of section 61 to 65 to the electronic record. It is the cardinal principle of interpretation that if the legislature has omitted to use any word, the presumption is that the omission is intentional. It is well settled that the Legislature does not use any word unnecessarily.[6]

In this regard, the Apex Court in *UTKAL CONTRACTORS & JOINERY PVT. LTD.* V. *STATE OF ORISSA*[7] held that "...Parliament is also not expected to express itself unnecessarily. Even as Parliament does not use any word without meaning something, Parliament does not legislate where no legislation is called for. Parliament cannot be assumed to legislate for the sake of legislation; nor indulge in legislation merely to state what it is unnecessary to state or to do what is already validly done. Parliament may not be assumed to legislate unnecessarily."

The IT Act amended section 59 of the Evidence Act, 1872 to exclude electronic records from the probative force of oral evidence in the same manner as it excluded documents. This is the re-application of the documentary hearsay rule to electronic records. But, instead of submitting electronic records to the test of

[5] (2014) 10 SCC 473.
[6] Vivek Dubey, *"Admissibility of Electronic Evidence: An Indian Perspective"*4, FRACIJ (2017).
[7] AIR 1987 SC 1454.

secondary evidence - which, for documents, is contained in sections 63 and 65, it inserted two new evidentiary rules for electronic records in the Evidence Act: section 65A and section 65B. The intention of the legislature is to introduce the specific provisions which has its origin to the technical nature of the evidence particularly as the evidence in the electronic form cannot be produced in the court of law owing to the size of computer/server, residing in the machine language and thus, requiring the interpreter to read the same.[8] Section 65A of the Evidence Act creates special law for electronic evidence - The contents of electronic records may be proved in accordance with the provisions of section 65B. This section performs the same function for electronic records that section 61 does for documentary evidence: it creates a separate procedure, distinct from the simple procedure for oral evidence, to ensure that the adduction of electronic records obeys the hearsay rule. It also secures other interests, such as the authenticity of the technology and the sanctity of the information retrieval procedure. But section 65A is further distinguished because it is a special law that stands apart from the documentary evidence procedure in sections 63 and 65.

Section 65B of the Evidence Act details this special procedure for adducing electronic records in evidence and makes the secondary copy in the form of computer output comprising of printout or the data copied on electronic/magnetic media admissible.

C. Relevancy & Admissibility Of Electronic Evidence In India

Tape Records Whether Electronic Device?

In *R.M MALKANI* V. *STATE OF MAHARASTRA*[9], it was held that the tape is primary and direct evidence of what has been said and recorded. The court made it clear that electronically recorded conversation is admissible in evidence, if the conversation is relevant to the matter in issue and the voice is identified and the accuracy of the recorded conversation is proved by eliminating the possibility of erasure, addition or manipulation. This Court further held that a contemporaneous electronic recording of a relevant conversation is a relevant fact comparable to a photograph of a relevant incident and is admissible as evidence under Section 8 of the Act. There is therefore no doubt that such electronic record can be received as evidence.

Supplying Copy of Electronic Record

State of Punjab v. *Amritsar Beverages Ltd*[10]

S 14(3) of Punjab General Sales Tax Act provided for inspection of books, documents and accounts and their seizure. The officer seizing book, account, register or document shall forthwith grant a receipt to receipt, retaining copy, affixing signature and seal of officer on document and return of books to dealer. But seized

[8] Vivek Dubey, *"Admissibility of Electronic Evidence: An Indian Perspective"*4,FRACIJ (2017).
[9] AIR 1973 SC 57.
[10] AIR 2007 SC 590.

record was cash book, ledger and other registers maintained in hard disk. Hence it was not possible to put signature and seal of official on seized documents. However, a copy was taken from hard disk and hard disk was returned.

It was held that the proper course of action for officers in such circumstances was to make copies of the hard disk or obtain a hard copy, affix their signatures or official seal on the hard copy and furnish a copy to the dealer or person concerned.

Video Conferencing

IN *AMITABH BAGCHI* V. *ENA BAGCHI*[11], sections 65-A and 65-B of Evidence Act, 1872 were analyzed. The court held that the physical presence of person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing. Sections 65-A and 65-B provide provisions for evidences relating to electronic records and admissibility of electronic records, and that definition of electronic records includes video conferencing.

IN *STATE OF MAHARASHTRA* V. *DR PRAFUL B DESAI*[12], the question involved whether a witness can be examined by means of a video conference. 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.

IN *TWENTEITH CENTURY FOX FILM CORPORATION* V. *NRI FILM PRODUCTION ASSOCIATES (P) LTD*[13] certain conditions have been laid down for video-recording of evidence:

• Before a witness is examined in terms of the Audio-Video Link, witness is to file an affidavit or an undertaking duly verified before a notary or a Judge that the person who is shown as the witness is the same person as who is going to depose on the screen. A copy is to be made available to the other side. (Identification Affidavit)

• The person who examines the witness on the screen is also to file an affidavit/undertaking before examining the witness with a copy to the other side with regard to identification.

• The witness has to be examined during working hours of Indian Courts. Oath is to be administered through the media.

[11] 2005 Cal. 11.
[12] AIR 2003 SC 2053.
[13] AIR 2003 KANT 148.

• The witness should not plead any inconvenience on account of time different between India and USA.

• Before examination of the witness, a set of plaint, written statement and other documents must be sent to the witness so that the witness has acquaintance with the documents and an acknowledgement is to be filed before the Court in this regard.

• Learned Judge is to record such remarks as is material regarding the demur of the witness while on the screen.

• Learned Judge must note the objections raised during recording of witness and to decide the same at the time of arguments.

• After recording the evidence, the same is to be sent to the witness and his signature is to be obtained in the presence of a Notary Public and thereafter it forms part of the record of the suit proceedings.

• The visual is to be recorded and the record would be at both ends. The witness also is to be alone at the time of visual conference and notary is to certificate to this effect.

• The learned Judge may also impose such other conditions as are necessary in a given set of facts.

• The expenses and the arrangements are to be borne by the applicant who wants this facility.

Proof of The Digital Signature Of A Person

Section 67A of IEA provides that except in the case of secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is digital signature of subscriber must be proved. It is necessary to prove in manner of proof of electronic record.[14] Section 65B will be applicable.

In *BODALA MURALI KRISHNA* V. *SMT. BODALA PRATHIMA*[15] the court held that, "…the amendments carried to the Evidence Act by introduction of Sections 65-A and 65-B are in relation to the electronic record. Sections 67-A and 73-A were introduced as regards proof and verification of digital signatures. As regards presumption to be drawn about such records, Sections 85-A, 85-B, 85-C, 88-A and 90-A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and digital signatures, as admissible pieces of evidence."

Electronic Messages - Email

IN *DHARAMBIR* V. *CENTRAL BUREAU OF IINVESTIGATION*[16], the court arrived at the conclusion that when Section 65-B talks of an electronic record produced by a computer referred to as the computer output) it would also include a hard disc in which information was stored or was earlier stored or continues to be stored. It

[14] The Information Technology Act, 2000, No. 21, Acts of Parliament 2000.
[15] AIR 2007 (2) ALD 72.
[16] AIR 2008 DLT 289.

distinguished as there being two levels of an electronic record. One is the hard disc which once used itself becomes an electronic record in relation to the information regarding the changes the hard disc has been subject to and which information is retrievable from the hard disc by using a software program. The other level of electronic record is the active accessible information recorded in the hard disc in the form of a text file, or sound file or a video file etc. Such information that is accessible can be converted or copied as such to another magnetic or electronic device like a CD, pen drive etc. Even a blank hard disc which contains no information but was once used for recording information can also be copied by producing a cloned had or a mirror image.

In the landmark decision of United States district court, for *MAYLAND IN LORRAINE* V. *MARKEL AMERICAN INSURANCE COMPANY*[17] held that when electronically stored information is offered as evidence, the following to be ascertained:

1. Is information relevant
2. Is it authentic
3. Is it hearsay
4. Is it original or, if it is a duplicate, is there admissible secondary evidence to support it and
5. Does its probative value survive the test of unfair prejudice ?

In *SOM PRAKASH* V. *STATE OF DELHI*[18]**,** the Supreme Court has rightly observed that "in our technological age nothing more primitive can be conceived of than denying discoveries and nothing cruder can retard forensic efficiency than swearing by traditional oral evidence only thereby discouraging the liberal use of scientific aids to prove guilt." Statutory changes are needed to develop more fully a problem solving approach to criminal trials and to deal with heavy workload on the investigators and judges.

In *SIL IMPORT, USA* V. *EXIM AIDES EXPORTERS, BANGALORE*[19]**,** the Supreme Court held that "Technological advancement like fascimile, Internet, e-mail, etc. were in swift progress even before the Bill for the Amendment Act was discussed by Parliament. So when Parliament contemplated notice in writing to be given we cannot overlook the fact that Parliament was aware of modern devices and equipment already in vogue."

In *STATE* V. *MOHD AFZAL AND ORS*[20]**,** the court held that Computer generated electronic records is evidence, admissible at a trial if proved in the manner specified by Section 65B of the Evidence Act.

[17] 241FRD 534.
[18] AIR 1974 SC 989.
[19] AIR (1999) 4 SC 567.
[20] 2003 DLT 385.

Call Records

In *STATE (NCT OF DELHI)* V. *NAVJOT SANDHU*[21] there was an appeal against conviction following the attack on Parliament on December 13 2001. This case dealt with the proof and admissibility of mobile telephone call records. While considering the appeal against the accused for attacking Parliament, a submission was made on behalf of the accused that no reliance could be placed on the mobile telephone call records, because the prosecution had failed to produce the relevant certificate under Section 65-B(4) of the Evidence Act. The Supreme Court concluded that a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records. The court held that merely because a certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65.

Proof of Contents of C.D

IN *JAGJIT SINGH* V. *STATE OF HARYANA*[22] the speaker of the Legislative Assembly of the State of Haryana disqualified a member for defection. When hearing the matter, the Supreme Court considered the digital evidence in the form of interview transcripts from the Zee News television channel, the Aaj Tak television channel and the Haryana News of Punjab Today television channel. The court determined that the electronic evidence placed on record was admissible and upheld the reliance placed by the speaker on the recorded interview when reaching the conclusion that the voices recorded on the CD were those of the persons taking action. The Supreme Court found no infirmity in the speaker's reliance on the digital evidence and the conclusions reached by him. The comments in this case indicate a trend emerging in Indian courts: judges are beginning to recognize and appreciate the importance of digital evidence in legal proceedings.

In the years that followed, printed versions of CDRs were admitted in evidence if they were certified by an officer of the telephone company under sections 63 and 65 of the Evidence Act. The special procedure of section 65B was ignored. This has led to confusion and counter-claims. For instance, the 2011 case of *AMAR SINGH* V. *UNION OF INDIA*[23] saw all the parties, including the state and the telephone company, dispute the authenticity of the printed transcripts of the CDRs, as well as the authorisation itself.

Currently, in the case of *RATAN TATA* V. *UNION OF INDIA*[24], a compact disc (CD) containing intercepted telephone

[21] AIR 2005 SC 3820.
[22] (2006) 11 SCC 1.
[23](2011) 7 SCC69.
[24] Ratan Tata v. Union of India Writ Petition (Civil) 398 of 2010.

calls was introduced in the Supreme Court without following any of the procedure contained in the Evidence Act.

The recent judgment of the Hon'ble Supreme Court delivered in *ANVAR P.V.* V. *P.K. BASHEER & OTHERS*[25], in CIVIL APPEAL NO. 4226 OF 2012 decided on Sept., 18, 2014, That Computer Output is not admissible without Compliance of 65B,EA overrules the judgment laid down in the *State (NCT of Delhi)* v. *Navjot Sandhu alias Afzal Guru*[26] by the two judge Bench of the Supreme Court. The court specifically observed that the Judgment of Navjot Sandhu supra, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this court, does not lay down correct position and is required to be overruled.

In *SANJAYSINH RAMRAO CHAVAN* V. *DATTATRAY GULABRAO PHALKE*[27] the court relying upon the judgment of Anvar case while considering the admissibility of transcription of recorded conversation in a case where the recording has been translated, it was held that as the voice recorder had itself not subjected to analysis, there is no point in placing reliance on the translated version. Without source, there is no authenticity for the translation. Source and authenticity are the two key factors for electronic evidence.

In the recent judgment, *JAGDEO SINGH* V. *THE STATE AND ORS*[28] pronounced by Hon'ble High Court of Delhi, while dealing with the admissibility of intercepted telephone call in a CD and CDR which were without a certificate u/s 65B Evidence Act, the court observed that the secondary electronic evidence without certificate u/s 65B Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever.

D. Challenges to Authenticity tf Electronic Evidence[29]

a. A claim that the records were altered, manipulated or damaged between the time they were created and the time they appear in court as evidence;

b. The reliability of the computer program that generated the record may be questioned;

c. The identity of the author may be in dispute: for instance, the person responsible for writing a letter in the form of a word processing file, SMS or email may dispute they wrote the text, or sufficient evidence has not been adduced to demonstrate the nexus between the evidence and the person responsible for writing the communication;

d. The evidence from a social networking website might be questioned as to its reliability;

[25] Anvar P.V. v. PK Basheer & others, in civil appeal no. 4226 of 2012.
[26] (2005) 11 SCC 600.
[27] MANU/ SC/0040/2015.
[28] MANU/DE/0376/2015.
[29] Swarupa Dholam "Electronic Evidences and Its Challenges" mja.gov.in/Site/Upload/GR/Article%20on%20Electonic%20evidence.pdf.

e. It might be agreed that an act was carried out and recorded, but at issue might be that the party introducing the evidence has failed to prove that where others might have access to a device (such as a mobile telephone), there was no proof to show that the message was directed to a particular person; or

f. Whether the person alleged to have used their PIN, password or clicked the 'I accept' icon was the person that actually carried out the action.

g. The data on local area networks, and whether there is a need to obtain an image of the complete network, if this is possible. If an image of each computer comprising the network is taken, the issue with networked computers is to demonstrate who had access to which computers at what time, and whether this access is audited. The security mechanisms in place on the network will be an important consideration when proving authenticity.

h. Data from the Internet is also subject to problems, because reliance may be placed on data obtained from remote computers, the computer of an investigator, and perhaps intercepted evidence. With the increased use of cloud computing where data is stored on 'server farms', accessible via the Internet, obtaining a copy of the data may be subject to contractual restrictions, or the data may be stored in another jurisdiction, which in turn may mean it will be necessary to take local legal advice in relation to the obtaining of the data.

i. Where data is being updated constantly, such as transactional data-bases, or websites that are continually updated, this poses problems, as the relevant evidence is point-in-time, which may be extremely difficult to obtain.

j. Authentication of information on social media sites presents its own unique set of issues. Firstly, it can be difficult to establish the author of the document, because social media sites often have a number people writing to the one page. Secondly, proving the identity of an author can be difficult, since it is still possible to create an internet profile without having to prove identity.

E. Effects of Considering Electronic Evidence As Primary And Direct[30]

Blurring the Difference between Primary and Secondary Evidence

By bringing all forms of computer evidence into the fold of primary evidence, the statute has effectually blurred the difference between primary and secondary forms f evidence. While the difference is still expected to apply with respect to other forms of documents, an exception has been created with respect to computers. This, however, is essential, given the complicated nature of computer evidence in terms of not being easily

[30] Relevancy and admissibility of electronic evidence https://www.lawteacher.net/.../relevancy-and-admissibility-of-electronic-law-essays.ph....

producible in tangible form. Thus, while it may make for a good argument to say that if the word document is the original then a print out of the same should be treated as secondary evidence, it should be considered that producing a word document in court without the aid of print outs or CDs is not just difficult, but quite impossible.

a. Making Criminal Prosecution Easier

In light of the recent spate of terrorism in the world, involving terrorists using highly sophisticated technology to carry out attacks, it is of great help to the prosecution to be able to produce electronic evidence as direct and primary evidence in court, as they prove the guilt of he accused much better than having to look for traditional forms of evidence to substitute the electronic records, which may not even exist. As we saw in the Ajmal Kasab case, terrorists these days plan all their activities either face-to-face, or through software. Being able to produce transcripts of internet transactions helped the prosecution case a great deal in proving the guilt of the accused.

Similarly, in the case of *State (NCT of Delhi)* v. *Navjot Sandhu @ Afsan Guru*, the links between the slain terrorists and the masterminds of the attack were established only through phone call transcripts obtained from the mobile service providers.

b. Risk of Manipulation

While allowing all forms of computer output to be admissible as primary evidence, the statute has overlooked the risk of manipulation. Tampering with electronic evidence is not very difficult and miscreants may find it easy to change records which are to be submitted in court. However, technology itself has solutions for such problems. Computer forensics has developed enough to find ways of cross checking whether an electronic record has been tampered with, when and in what manner.

c. Opening Potential Floodgates

Computers are the most widely used gadget today. A lot of other gadgets involve computer chips in their functioning. Thus, the scope of Section 65A and 65B is indeed very large. Going strictly by the word of the law, any device involving a computer chip should be adducible in court as evidence. However, practical considerations as well as ethics have to be borne in mind before letting the ambit of these Sections flow that far. For instance, the Supreme Court has declared test results of narco-analysis to be inadmissible evidence since they violate Article 20(3) of the Constitution. It is submitted that every new form of computer technology that is sought to be used in the process of production of evidence should be subjected to such tests of Constitutionality and legality before permitting their usage.

III. UNITED KINGDOM

There are different rules regarding admissibility of electronic evidence than those applicable to traditional documentary evidence. These provisions are found in the *Civil Evidence Act 1968* and the *Police and Criminal Evidence Act 1984. A* computer-produced document shall be admissible as evidence of the statement contained therein, provided the proponent demonstrates its authenticity. The party who wishes to tender an electronically-produced document as evidence must establish that:[31]

a. the document was prepared during a period over which the computer regularly stored or processed information;

b. over the relevant period of time, information of this type was regularly supplied to the computer;

c. the computer was operating properly; and

d. the information contained in the statement reproduces information supplied to the computer

If one of these conditions is not met, the document is simply inadmissible as evidence.

In addition to proving the authenticity of the document, the proponent of an electronically-produced document must also demonstrate its reliability, through the production of a certificate signed by a person responsible for the operation of the computer

As for probative weight of computer-produced evidence, **section 6** of the *Civil Evidence Act 1968* requires that in estimating the weight of the document, the Court must examine the contemporaneity of the recording of the information with the events described in that record, and the motive of any person to misrepresent the facts recorded.

Section 8[32] of the *Civil Evidence Act* establishes that the Rules of Court must require that the proponent of such evidence give notice to its adversary of its intention to use electronically-produced evidence.

Section 69[33] of the *Police and Criminal Evidence Act 1984* provides that computer-produced evidence is admissible in criminal proceedings as long as there exists no reasonable grounds for believing that the statement it contains is inaccurate because of improper use of the computer and that, at all material times, the computer was operating properly or that the malfunction did not affect the

[31] Civil Evidence Act, 1968.
[32] Civil Evidence Act, 1968.
[33] Police and Criminal Evidence Act, 1984.

production of the document or the accuracy of the statement. Finally, section 69 of the *Police and Criminal Evidence Act 1984* requires that the Rules of Court concerning giving notice are satisfied.

IN *R.* V. *SPIBY*[34], the Court of Appeal held that printouts from an automatic telephone call logging computer installed in a hotel were admissible as they constituted real evidence. The Court concluded that in the absence of evidence to the contrary, the machine is held to be in working order at the material time.

In *CAMDEN LONDON BOROUGH COUNCIL* V. *HOBSON*[35], the Court stated that computer-generated evidence constituted real evidence if the statement originated in the computer. It would then be admissible as the record of a mechanical operation in which human information had played no part; however, a statement originating from a human mind and subsequently processed by a computer would be inadmissible as hearsay. Proof of the reliability of a computer-generated document is also a crucial condition to its admissibility. The Lords found that the inaccuracy did not affect the processing of the information supplied to the computer. Section 69 of the Police and Criminal Evidence Act 1984 should be interpreted according to its purpose so as to not exclude otherwise accurate evidence. Lord Hoffman concluded that:

IV. UNITED STATES

The *Federal Rules of Evidence* provide the requirements for the authentication of documentary evidence, a prerequisite step for the admission of such evidence. The *Federal Rules of Evidence* deal with authentication without distinguishing between computer-generated evidence and other forms of documentary evidence. One must then conclude that the requirements for traditional documentary evidence also apply to computer-generated evidence[36].

***Federal Rule of Evidence* 901** [37] describes authentication as a condition precedent to admissibility, "satisfied by evidence sufficient to support a finding that a matter in question is what its proponent claims". If a document is produced by a process or system, one must demonstrate that such process or system produces an accurate result".

IN *KING* V. *STATE EX. REL MURDOCH ACCEPTANCE CORP*[38], the Supreme Court of Mississippi suggested that hardware is reliable in light of its general use and reliance in the business community. However, the Court, in this case, established guidelines for the admissibility of computer-generated business

[34] [19911 Chin_ L.R. 199 (C.A.Cr.D.).
[35] *The Independent*, January 28, 1992, 24 (Clerkenwell Magistrate's Court).
[36] Federal Rules of Evidence, 2015.
[37] Federal rules of Evidence 901.
[38] 222 So. (2d) 393 (Miss. 1969).

records. These guidelines included proof that the computing equipment was recognized as standard equipment, that the entries were made in the regular course of business, contemporaneously the event recorded, and that foundation testimonies satisfied the Court that the source of information method and time of preparation was such as to indicate its trustworthiness and justify its admission'

Although these guidelines are very similar to those established by ***Federal Rule of Evidence*** **803(6)**[39], modern case law has been more generous with the admission of computer-generated evidence, shifting the debate towards the probative weight of such documentary evidence. In *UNITED STATES* V. *LINN*[40], the testimony of a hotel Director of Communications was sufficient to authenticate a record of telephone calls as he was on duty when the computer recorded the call in question.

In *UNITED STATES* V. *CATABRANIS*, the Court admitted into evidence business records, although it was demonstrated that they contained inaccuracies. The Court held that these inaccuracies affected the weight and not the admissibility of the records.

V. CONCLUSION

Due to enormous growth in e-governance throughout the Public & Private Sector and ecommerce activities Electronic Evidence have involved into a fundamental pillar of communication, processing and documentation. The government agencies are opening up to introduce various governance policies electronically and periodical filings to regulate and control the industries are done through electronic means. These various forms of Electronic Evidence/ Digital Evidence are increasingly being used in the judicial proceedings. At the stage of trial, Judges are often asked to rule on the admissibility of electronic evidence and it substantially impacts the outcome of civil law suit or conviction/acquittal of the accused. The Court continue to grapple with this new electronic frontier as the unique nature of evidence, as well as the ease with which it can be fabricated or falsified, creates hurdle to admissibility not faced with the other evidences.

The various categories of electronic evidence such as CD, DVD, hard disk/ memory card data, website data, social network communication, email, instant chat messages, SMS/MMS and computer generated documents poses unique problem and challenges for proper authentication and subject to a different set of views. Maintaining the integrity of electronic evidence throughout the process of investigation and trial presents different problems from the handling of traditional physical or documentary evidence.

The challenges with respect to the admissibility and appreciation of electronic evidence, India still has a long way to go in keeping pace with the developments globally. Although the amendments were introduced to

[39] Federal rules of Evidence 803 (6).
[40] 880 F.2d 209 (9th Cir. 1988).

reduce the burden of the proponent of records, they cannot be said to be without limitations. It is clear that India has yet to devise a mechanism for ensuring the eracity of contents of electronic records, which are open to manipulation by any party by obtaining access to the server or space where it is stored.

The admission of electronic evidence along with advantages can also be complex at the same time. It is upon the courts to see that the whether the evidence fulfils the three essential legal requirements of authenticity, reliability and integrity. After Anvars case decision by the Supreme Court laying down the rules for admissibility of electronic evidence it can be expected that the Indian courts will adopt a consistent approach, and will execute all possible safeguards for accepting and appreciating electronic evidence.