MedCrave
Step into the World of Research
Forensic Research & Criminology International Journal

Proceeding

Open Access
CrossMark

Admissibility of electronic evidence: an Indian perspective

Abstract

This article begins with the concept and meaning of electronic evidence. Further the principles of the evidence act has been explained with amendments in regard to electronic evidence. Several decisions of the Indian Supreme Court have been cited in reference to the admissibility of electronic evidence. Finally the safeguards and procedure which needs to be adopted by the Indian judiciary in handling electronic evidences.

Volume 4 Issue 2 - 2017

Vivek Dubey
Dr. H.S.Gour Vishwavidyalaya Sagar University, India

Correspondence: Vivek Dubey, School of Law, Dr. H.S.Gour Vishwavidyalaya Sagar University, Madhya Pradesh - 470003, India, Tel 8358800320, Email vivekdub@gmail.com

Received: February 27, 2017 | **Published:** March 14, 2017

Introduction

The 21st century saw a technological revolution which enthralled not only India but the whole world. The use of computers is not limited to established organizations or institutions but available to every individual at swipe of a finger. Information Technology has eased out almost every humanized action. In this age of cyber world as the application of computers became more popular, there was expansion in the growth of technology. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. This increasing reliance on electronic means of communications, e-commerce and storage of information in digital form has most certainly caused a need to transform the law relating to information technology and rules of admissibility of electronic evidence both in civil and criminal matters in India. The proliferation of computers and the influence of information technology on society as whole, coupled with the ability to store and amass information in digital form 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.[1]

With the change in law, Indian courts have developed case law regarding reliance on electronic evidence. Judges have also demonstrated perceptiveness towards the intrinsic 'electronic' nature of evidence, which includes insight regarding the admissibility of such evidence, and the interpretation of the law in relation to the manner in which electronic evidence can be brought and filed before the court.[2] Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence it is vital that the determination of its relevance, veracity and authenticity be ascertained by the court and to establish if the fact is hearsay or a copy is preferred to the original. Digital Evidence is "information of probative value that is stored or transmitted in binary form". Evidence 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.[3]

Meaning of electronic evidence

The type of evidence that we are dealing with has been variously described as 'electronic evidence', 'digital evidence' or 'computer evidence'. The word digital is commonly used in computing and electronics, especially where physical-world information is converted to binary numeric form as in digital audio and digital photography.[4] Definitions of digital evidence include 'Information of probative value stored or transmitted in binary form; and 'Information stored or transmitted in binary form that may be relied on in court. While the term 'digital' is too wide, as we have seen the use of 'binary' is too restrictive, because it only describes one form of data. Electronic evidence : data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.[5] This definition has three elements. First, it is intended to include all forms of evidence that is created, manipulated

[1]Available at, https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali-, last accessed on 15 feb 2017.
[2]The Supreme Court of India re-defines admissibility of electronic evidence in India by Tejas Karia, Akhil Anand and Bahaar Dhawan.
[3]Available at https://www.linkedin.com/pulse/electronic-evidence-digital-cyber-law-india-adv-prashant-mali-, last accessed on 10 feb 2017.
[4]Electronic Evidence and its Challenges by Dr. Swaroopa Dholam.
[5]Ibid.

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.[6]

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.[7]

Electronic evidence and the Indian evidence act 1872

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.[8] 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".[9] 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. Traditionally, the fundamental rule of evidence is that direct oral evidence may be adduced to prove all facts, except documents. The hearsay rule suggests that any oral evidence that is not direct cannot be relied upon unless it is saved by one of the exceptions as outlined in sections 59 and 60 of the Evidence Act dealing with the hearsay rule. However, the hearsay rule[10] is not as restrictive or as straightforward in the case of documents as it is in the case of oral evidence. This is because it is settled law that oral evidence cannot prove the contents of a document, and the document speaks for itself. Therefore, where a document is absent, oral evidence cannot be given as to the accuracy of the document, and it cannot be compared with the contents of the document. This is because it would disturb the hearsay rule (since the document is absent, the truth or accuracy of the oral evidence cannot be compared to the document). In order to prove the contents of a document, either primary or secondary evidence must be offered.[11]

While primary evidence of the document is the document itself,[12] it was realized that there would be situations in which primary evidence may not be available. Thus secondary evidence in the form of certified copies of the document, copies made by mechanical processes and oral accounts of someone who has seen the document, was permitted under section 63 of the Evidence Act for the purposes of proving the contents of a document. Therefore, the provision for allowing secondary evidence in a way dilutes the principles of the hearsay rule and is an attempt to reconcile the difficulties of securing the production of documentary primary evidence where the original is not available. Section 65 of the Evidence Act sets out the situations in which primary evidence of the document need not be produced, and secondary evidence - as listed in section 63 of the Evidence Act - can be offered. This includes situations when the original document

1. Is in hostile possession.
2. Or has been proved by the prejudiced party itself or any of its representatives.
3. Is lost or destroyed.
4. Cannot be easily moved, i.e. physically brought to the court.
5. Is a public document of the state.
6. Can be proved by certified copies when the law narrowly permits; and
7. Is a collection of several documents.[13]

Electronic document

As documents came to be digitized, the hearsay rule faced several new challenges. While the law had mostly anticipated primary

[6]Burkhard Schafer and Stephen Mason, The characteristics of electronic evidence in digital format, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013.

[7]Infra note 18.

[8]Section 3 of the Indian Evidence Act, 1872.

[9]The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000.

[10]Hearsay evidence is anything said outside a court by a person absent from a trial, but which is offered by a third person during the trial as evidence. The law excludes hearsay evidence because it is difficult or impossible to determine its truth and accuracy, which is usually achieved through cross examination. Since the person who made the statement and the person to whom it was said cannot be cross examined, a third person's account of it is excluded. There are a few exceptions to this rule which need no explanation here.

[11]Anvar v. Basheer and the New (Old) Law of Electronic Evidence - The Centre for Internet and Society, available at http://cisindia.org/internetgovernance/blog/anvarvbasheernewoldlawofelectronicevidence last accessed on 10/02/2017.

[12]Section 62 of the Indian Evidence Act, 1872.

[13]Manisha T. Karia and Tejas D. Karia, 'India' (Chapter 13) in Stephen Mason, ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012).

evidence (i.e. the original document itself) and had created special conditions for secondary evidence, increasing digitisation meant that more and more documents were electronically stored. As a result, the abduction of secondary evidence of documents increased.[14] In the Anvar case,[15] 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.[16] 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.[17] In this regard, the Apex Court in Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa[18] 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 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.[19] 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.[20] 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. Sub-section (2) lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used:

1. At the time of the creation of the electronic record, the computer that produced it must have been in regular use,
2. The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer,
3. The computer was operating properly; and,
4. The duplicate copy must be a reproduction of the original electronic record.

The Section 65B of the Evidence Act makes the secondary copy in the form of computer output comprising of printout or the data copied on electronic/magnetic media admissible. It provides:[21] Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media, produced by a computer shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Sec. 65B (2)

The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used; Information was fed in computer in the ordinary course of the activities of the person having lawful control over the computer; The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy; Information reproduced is such as is fed into computer in the ordinary course of activity.[22]

Sec.65 B (3)

The following computers shall constitute as single computer

1. By a combination of computers operating over that period; or
2. By different computers operating in succession over that period; or
3. By different combinations of computers operating in succession over that period; or
4. In any other manner involving the successive operation over that period, in whatever order, of one or more
5. In any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

[14]Supra note 12.

[15]Anvar P. K. vs. P.K Basheer &Ors. (2014) 10 SCC 473

[16]Supra note 12.

[17]E-Evidence in India by Prashanti, available at www.legalservicesindia.com, last accessed on 09/02/2017.

[18]Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa reported as AIR 1987 SC 1454.

[19]Supra note 18.

[20]Section 65-A of the Indian evidence Act, 1872: Special provisions as to evidence relating to electronic record.

[21]Section 65B provides for 'Admissibility of Electronic Records'.

[22]Section 65 B (2) of the Indian Evidence Act, 1872 lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used.

Sec. 65B (4)

Regarding the person who can issue the certificate and contents of certificate, it provides the certificate doing any of the following things: identifying the electronic record containing the statement and describing the manner in which it was produced; giving the particulars of device, dealing with any of the matters to which the conditions mentioned in subsection (2) relate and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.[23] This contention is further strengthened by the insertion words "Notwithstanding anything contained in this Act" to Section 65A & 65B, which is a non obstante clause, further fortifies the fact that the legislature has intended the production or exhibition of the electronic records by Section 65A & 65B only. A non obstante clause is generally appended to a Section with a view to give the enacting part of the Section, in case of conflict, an overriding effect over the provision in the same or other act mentioned in the non obstante clause. It is equivalent to saying that despite the provisions or act mentioned in the non obstante clause, the provision following it will have its full operation or the provisions embraced in the non obstante clause will not be an impediment for the operation of the enactment or the provision in which the non obstante clause occurs. The aforesaid principles of interpretation with respect to the non obstante clause in form of "Notwithstanding anything contained in this Act" is further supported by the Hon'ble Apex Court in Union of India and Anr., v. G.M. Kokil and Ors.[24] observed "It is well known that a non obstante clause is a legislative device which is usually employed to give overriding effect to certain provisions over some contrary provisions that may be found either in the same enactment or some other enactment, that is to say, to avoid the operation and effect of all contrary provisions." Further, the Hon'ble Apex Court in the case cited as Chandavarkar Sita Ratna Rao v. Ashalata S. Guram,[25] explained the scope of non obstante clause as "It is equivalent to saying that in spite of the provision of the Act or any other Act mentioned in the non obstante clause or any contract or document mentioned the enactment following it will have its full operation".

Non application the special legal provisions

The special law and procedure created by sections 65A and 65B of the Evidence Act for electronic evidence were not used. Disappointingly, the cause of this non-use does not involve the law at all.[26] India's lower judiciary - the third tier of courts, where trials are undertaken - is vastly inept and technologically unsound. With exceptions, trial judges simply do not know the technology the IT Act comprehends. It is easier to carry on treating electronically stored information as documentary evidence. The reasons for this are systemic in India and, I suspect, endemic to poor developing countries. India's justice system is decrepit and poorly funded. As long as the judicial system is not modernized, India's trial judges will remain clueless about electronic evidence and the means of ensuring its authenticity.[27] By bypassing the special law on electronic records, Indian courts have continued to apply the provisions of sections 63 and 65 of the Evidence Act, which pertain to documents, to electronically stored information. Simply put, the courts have basically ignored sections 65A and 65B of the Evidence Act. Curiously, this state of affairs was blessed by the Supreme Court in Navjot Sandhu (the Parliament Attacks case),[28] which was a particularly high-profile appeal from an emotive terrorism trial. On the question of the defence's challenge to the authenticity and accuracy of certain call data records (CDRs) that the prosecution relied on, which were purported to be reproductions of the original electronically stored records, a Division Bench of Justice P. Venkatarama Reddi and Justice P. P. Naolekar held.

According to Section 63, secondary evidence means and includes, among other things, "copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies". Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. It is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the court. That is what the High Court has also observed at para 276. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service-providing company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts based on his personal knowledge.[29]

Electronic evidence and the indian supreme court

In Som Prakash vs. State Of Delhi,[30] 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 vs. Exim Aides Exporters, Bangalore,[31] 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 vs. Mohd. Afzal And Ors,[32] the court held that Computer generated electronic records is evidence, admissible at a trial if proved in the

[23]Section 65B (4) of the Evidence Act lists additional non-technical qualifying conditions to establish the authenticity of electronic evidence. This provision requires the production of a certificate by a senior person who was responsible for the computer on which the electronic record was created, or is stored. The certificate must uniquely identify the original electronic record, describe the manner of its creation, describe the device that created it, and certify compliance with the technological conditions of sub-section (2) of section 65B.

[24]Union of India and Anr., v. G.M. Kokil and Ors. [(1984)SCR196].

[25]Chandavarkar Sita Ratna Rao v. Ashalata S. Guram [(1986) 3SCR866].

[26]Prior to 2000 in India, electronically stored information was dealt with as a document, and secondary evidence of electronic records were adduced as 'documents' in accordance with section 63 of the Evidence Act.

[27]Supra note 12.

[28]State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.

[29]Available at www.cidap.gov.in/.../State_(N.C.T._Of_Delhi)_vs_Navjot_Sandhu@_Afsan_Guru_o., Last accessed on 11/02/2017.

[30]Som Prakash vs. State Of Delhi AIR 1974 SC 989, 1974 Cri. LJ 784, MANU/SC/0213/1974.

[31]SIL Import, USA v vs. Exim Aides Exporters, Bangalore MANU/SC/0312/1999, (1999) 4 SCC 567.

[32]State vs. Mohd. Afzal And Ors (2003) DLT 385, 2003(71)DRJ 17.

manner specified by Section 65B of the Evidence Act. In State vs. Navjyot Sandhu[33] 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. The Supreme Court's finding in Navjot Sandhu case[34] raised uncomfortable questions about the integrity of prosecution evidence, especially in trials related to national security or in high-profile cases of political importance. The state's investigation of the Parliament Attacks was shoddy with respect to the interception of telephone calls. The Supreme Court's judgment notes in prs. 148, 153, and 154 that the law and procedure of wiretaps was violated in several ways.[35]

The Evidence Act mandates a special procedure for electronic records precisely because printed copies of such information are vulnerable to manipulation and abuse. This is what the veteran defence counsel, Mr. Shanti Bhushan, pointed out in Navjot Sandhu where there were discrepancies in the CDRs led in evidence by the prosecution. Despite these infirmities, which should have disqualified the evidence until the state demonstrated the absence of mala fide conduct, the Supreme Court stepped in to certify the secondary evidence itself, even though it is not competent to do so. The court did not compare the printed CDRs to the original electronic record. Essentially, the court allowed hearsay evidence. This is exactly the sort of situation that section 65B of the Evidence Act intended to avoid by requiring an impartial certificate under sub-section (4) that also speaks to compliance with the technical requirements of sub-section (2).[36] When the lack of a proper certificate regarding the authenticity and integrity of the evidence was pointed out, this is what the Supreme Court said in pr. 150: Irrespective of the compliance of the requirements of Section 65B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely, Sections 63 and 65. It may be that the certificate containing the details in sub-section (4) of Section 65B is not filed in the instant case, but that 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 and 65.[37]

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[38] 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,[39] a compact disc (CD) containing intercepted telephone calls was introduced in the Supreme Court without following any of the procedure contained in the Evidence Act. In Avnish Bajaj vs. State,[40] the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider was raised. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

The trend of ignoring the special procedure prescribed for adducing electronic records as evidence was seen even in subsequent cases. For example the case of Ratan Tata v. Union of India[41] was another case where a CD containing intercepted telephone calls was introduced in the Supreme Court without following the procedure laid down under section 65B of the Evidence Act. In Anvar vs. Basheer,[42] the court held that Section 65B of the Evidence Act has been inserted by way of an amendment by the Information Technology Act, 2000. In as much it is a special provision which governs digital evidence and will override the general provisions with respect to adducing secondary evidence under the Evidence Act. In 2007, the United States District Court for Maryland handed down a landmark decision in Lorraine v. Markel American Insurance Company[43] 241 FRD 534 (D. Md. 2007) that clarified the rules regarding the discovery of electronically stored information. In American federal courts, the law of evidence is set out in the Federal Rules of Evidence. Lorraine held when electronically stored information is offered as evidence, the following tests need to be affirmed for it to be admissible:

1. Is the 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 a small way, Anvar does for India what Lorraine did for US federal courts. In Anvar, the Supreme Court unequivocally returned Indian electronic evidence law to the special procedure created under section 65B of the Evidence Act. It did this by applying the maxim generalia specialibus non derogant ("the general does not detract from the specific"), which is a restatement of the principle lex specialis derogat legi generali ("special law repeals general law"). The Supreme Court held that the provisions of sections 65A and 65B of the Evidence Act created special law that overrides the general law of documentary evidence. Proof of electronic record is a special provision introduced by the IT Act amending various provisions under the Evidence Act. The very caption of Section 65Aof the Evidence Act, read with Sections 59 and 65B is sufficient to hold that the special provisions on evidence relating to electronic record shall be governed by the procedure prescribed under Section 65B of the Evidence Act. That is a complete code in itself. Being a special law, the general law under Sections 63 and 65 has to yield. By doing so, it disqualified oral evidence offered to attest secondary documentary evidence. The Evidence Act does not contemplate or permit the proof of an

[33]State vs. Navjyot Sandhu AIR 2005 SC 3820.
[34]Supra note 29.
[35]Supra note 30.
[36]Anvar v. Basheer and the New (Old) Law of Electronic Evidence - The Centre for Internet and Society available at, http://cisindia.org/internetgovernance/blog/anvarvbasheernewoldlawofelectronicevidence, last accessed on 21/02/2017.
[37]Ibid.
[38]Amar Singh v. Union of India (2011) 7 SCC 69.
[39]Ratan Tata v. Union of India Writ Petition (Civil) 398 of 2010.
[40]Avnish Bajaj vs. State (Bazee.com case) 2008(105)DRJ 721 MANU/DE/0851/2008.
[41]Ratan Tata v. Union of India, Writ Petition (Civil) 398 of 2010 before Supreme Court of India.
[42]Anvar vs. Basheer AIR 2015 SC 180, MANU/SC/0834/2014.
[43]Lorraine v. Markel American Insurance Company 241 FRD 534 (D. Md. 2007).

electronic record by oral evidence if requirements under Section 65B of the Evidence Act are not complied with, as the law now stands in India.[44]

The scope for oral evidence is offered later. Once electronic evidence is properly adduced according to section 65B of the Evidence Act, along with the certificate of sub-section (4), the other party may challenge the genuineness of the original electronic record. If the original electronic record is challenged, section 22A of the Evidence Act permits oral evidence as to its genuineness only. Note that section 22A disqualifies oral evidence as to the contents of the electronic record, only the genuineness of the record may be discussed. In this regard, relevant oral evidence as to the genuineness of the record can be offered by the Examiner of Electronic Evidence, an expert witness under section 45A of the Evidence Act who is appointed under section 79A of the IT Act. In Sanjaysinh Ramrao Chavan vs. Dattatray Gulabrao Phalke.[45] 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 vs. The State and Ors[46] 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.

Conclusion

Strict compliance with section 65B is now mandatory for persons who intend to rely upon e-mails, web sites or any electronic record in a civil or criminal trial before the courts in India. This outlook of the Supreme Court of India is to ensure that the credibility and evidentiary value of electronic evidence is provided for, since the electronic record is more susceptible to tampering and alteration. In its judgment, Kurian J observed, that: 'Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.' Therefore, the computer generated electronic record cannot be solely relied upon, because there is a possibility of it being hampered. The Indian Evidence Act could be further amended to rule out any manipulation - at least for the purposes of presuming prima facie authenticity of the evidence of the electronic record - by adding a condition that the record was created in the usual way by a person who was not a party to the proceedings and the proponent of the record did not control the making of the record. By ensuring that the record was created by a party who was adverse in interest to the proponent of the record, and the record was being used against the adverse party, the risk of the manipulation of the records would be reduced significantly. This is because, it is argued, no disinterested party would want to certify the authenticity of the record which to his knowledge had been tampered with. The law also needs to creatively address the requirement of the burden being on the proponent to provide testimony as to the author of a document to determine whether there was any manipulation or alteration after the records were created, the reliability of the computer program that generated the records, 20 and whether the records are complete or not. The courts also have to be mindful that data can be easily forged or altered, and section 65B of the Evidence Act does not address these contingencies. For instance, when forwarding an e-mail, the sender can edit the message. Such alterations are often not detectible by the recipient, and therefore a certificate of a third party to the dispute may not always be a reliable condition to provide for the authenticity of the document.

Serious issues have been raised in the digital world due to malpractices such as falsification of information and impersonation, in relation to the authenticity of information relied upon as evidence. It raises queries as to how it is possible to prove the creation and transmission of electronic communication by one party when the party's name as the author of the post could have been inserted by anyone. Perhaps, it may be prudent for the courts or the government to set up a special team of digital evidence specialists who would assist the courts and specifically investigate the authenticity of the electronic records. 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 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 veracity 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.

Acknowledgments

None.

Conflicts of interest

None.

[44]Supra note 43.

[45]Sanjaysinh Ramrao Chavan vs. Dattatray Gulabrao Phalke MANU/SC/0040/2015.

[46]Jagdeo Singh vs. The State and Ors. MANU/DE/0376/2015.