** LAW MANTRA THINK BEYOND OTHERS**

**(I.S.S.N 2321- 6417 (Online) Ph: +918255090897 Website:** [**journal.lawmantra.co.in**](http://www.journal.lawmantra.co.in)

**E-mail:** [**info@lawmantra.co.in**](mailto:info@lawmantra.co.in)[**contact@lawmantra.co.in**](mailto:contact@lawmantra.co.in)

**LAW PERTAINING TO ELECTRONIC EVIDENCE [[1]](#footnote-2)\***

The Indian Evidence Act, 1872 contains set of rules and regulations regarding admissibility of evidence in the Indian Courts of law. The British Parliament passed Indian Evidence Act in 1872 setting up a path-breaking judicial measure by changing traditional legal systems of different social groups and communities. Since then from time to time amendments are made in the Indian Evidence Act to make it compatible with changing times. The court proceedings and the judicial system is based on the facts and the evidence as produced before courts. Even in the era of kings and rulers, when any matter laid before them each party were insisted to have proceed with facts and evidence they have to prove their allegations or strategy. Same analogy has been adopted by Panchayats & courts although with care and caution due to high technological advancement, with this aspects one has to see the rights of individual, rights of victim, admissibility of evidence and to support & strengthen the coordination and cooperation between investigating and prosecution and to prevent miscarriage of justice. However, with the advent of new technologies, regulatory agencies are increasingly harnessing the power of digital technologies to meet the informational demands of rulemaking and to expand public involvement in policymaking. Governments are increasingly adopting technological means, shifting from walls to webs.[[2]](#footnote-3)

The Information Technology Act was originally passed on 17th October 2000 with one of the aim to provide legal recognition to digital/electronic evidence. Hence, amendments were made in the Indian Evidence Act regarding collection and production of digital evidence in the court of law.

Evidence Act fundamentally describes two type of evidence i.e.[[3]](#footnote-4)

1) Oral evidence and

2) Documentary evidence.

As per amended provision **Section 3(2)** of evidence Act electronic evidence is documentary evidence.

“(2) All documents including electronic records produced for the inspection of the Court], such documents are called documentary evidence.”

Further if we refer another provision it is contained in **Section 2(t)** of Information Technology Act 2000 electronic record means;

“(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;”

So, if we refer above-mentioned definitions in the light of the provisions incorporated under **Section 65-A & 65-B** of evidence Act; Electronic Evidence is one another type of documentary evidence which is if duly proved in the manner provided in **section 65-B**, can be considered as strong evidence.

Before elaborate discussion of Electronic evidence it is required to be get a flash back up on the structure of evidence Act and also the principles of law for adducing, relying and considering evidence.

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. Due to the enormous growth in electronic correspondence, electronic writings (also known as e-evidence) have evolved into a fundamental pillar of communication in today’s society. Electronic communications have revolutionized how the world does business, learns about and shares news, and instantly engages with friends and family. Ninety one percent of today’s online adults use some form of electronic communication regularly in their everyday lives. [[4]](#footnote-5)Not surprisingly, various forms of electronic evidence (i.e., e-evidence) are increasingly being used in both civil and criminal litigation. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.[[5]](#footnote-6)

Electronic evidence can be found in emails, 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,

Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics. The goal of computer forensics is to explain the current state of a digital artifact. The term digital artifact can include: a computer system storage medium (hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image), or even a sequence of packets moving over a computer network. 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.[[6]](#footnote-7)

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. 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. The definition of 'evidence' has been amended to include electronic records. The definition of 'documentary evidence' has been amended to include all documents, including electronic records produced for inspection by the court.

During trials, judges are often asked to rule on the admissibility of electronic evidence. How the court rules on questions of admissibility could substantially impact the outcome of a civil lawsuit or determine the difference between conviction or acquittal of a defendant. This unique form of evidence typically falls into one of five distinct categories: 1) Website Data; 2) Social Network Communications and Postings; 3) Email; 4) Text Messages; 5) Computer Stored/Generated Documents.

As courts continue to grapple with this new electronic frontier it is important to stress that electronic evidence is subject to the same rules of evidence as paper documents. However, the unique nature of e-evidence, as well as the ease with which it can be manipulated or falsified, creates hurdles to admissibility not faced with other evidence.

A four-step analytical framework stated below governs admissibility of electronic evidence. Because e-evidence is subject to manipulation and questions of authorship are often hotly disputed, the requirement to “authenticate” is usually the most difficult to overcome. Each of the five categories of electronic evidence—Website Data, Social Network Communications and Postings, Email, Text Messages, and Computer Stored/Generated Documents—poses unique problems and challenges for proper authentication and deserves independent consideration.[[7]](#footnote-8)

Whenever the admissibility of e-evidence is called into question, the court and attorneys should apply the following four-step analytical framework.[[8]](#footnote-9)

* **“Authenticate or Identify.”** authentication means the party offering the electronic evidence must present sufficient evidence to support a finding that the exhibit in question is what the proponent claims it to be. The most common method of authentication is the use of testimony by a witness with knowledge that the exhibit is what it claims to be.
* **“Hearsay or Not?”** Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to “prove the truth of the matter asserted.” If the statement is being offered to prove that the assertion is true then the statement is hearsay and is not admissible unless a recognized hearsay exception applies pursuant to statute.
* **“Relevant” and Not “Unfairly Prejudicial”?**relevant evidence “means evidence having any tendency to make the existence of a fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.” If the offer has any tendency (even a slight tendency) to make the existence of a fact more probable than it would be without the evidence, it is relevant.
* **Not “Privileged” Communication?**It identifies various communications (e.g., husband-wife; attorney-client; doctor-patient; clergy, etc.) that are considered “privileged” and thus, not admissible unless the privilege is deemed waived[[9]](#footnote-10)

**Section 3** of the Evidence Act, 1872 defines evidence as under: "Evidence" - Evidence means and includes:

1) all statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;

2) all documents including electronic records produced for the inspection of the court. Such documents are called documentary evidence.

The term 'electronic records' has been given the same meaning as that assigned to it under the ITAct.IT Act provides for"data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche". 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. 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.[[10]](#footnote-11)

In India, the change in attitude came with the amendment to the Indian Evidence Act in 2000. **Sections 65A and 65B** were introduced in to the chapter relating to documentary evidence**. Section 65A** provides that contents of electronic records may be admitted as evidence if the criteria provided in **Section 65B** is complied with. **Section 65B** provides that shall be considered documents, thereby making it primary evidence, if the computer which produced the record had been regularly in use, the information fed into the computer was part of the regular use of the computer and the computer had been operating properly. It further provides that all computer output shall be considered as being produced by the computer itself, whether it was produced directly or indirectly, whether with human intervention or without. This provision does away with the concept of computer evidence being hearsay.

Thus, with the amendments introduced into the statute, electronic evidence in India is no longer either secondary or hearsay evidence, but falls within the best evidence rule.

New **sections 65-A and 65-B** are introduced to the Evidence Act, under the Second Schedule to the IT Act**. Section 65-A** provides that the contents of electronic records may be proved in accordance with the provisions of **Section 65-B**. **Section 65-B** provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic form, 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 65-B are satisfied.

**Section 65-B(1)** states that if any information contained in an electronic record produced from a computer (known as computer output) has been copied on to an optical or magnetic media, then such electronic record that has been copied 'shall be deemed to be also a document' subject to conditions set out in **Section 65-B(2)** being satisfied. Both in relation to the information as well as the computer in question such document 'shall be admissible in any proceedings when 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’.

The conditions specified in **Section 65-B(2)** are:

1. Firstly, the computer should have produced the computer output containing the information during the period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer.

2. The second requirement is that it must be shown that during the said period, the information of the kind contained in electronic record or of the kind from which the information contained is derived was 'regularly fed into the computer in the ordinary course of the said activity'.

3. A third requirement is that during the material part of the said period, the computer should have been operating properly and that even if it was not operating properly for some time that break should not affect either the record or the accuracy of its contents.

4. The fourth requirement is that the information contained in the record should be a reproduction or derived from the information fed into the computer in the ordinary course of the said activity.

Under **Section 65-B(4)**, the certificate which identifies the electronic record containing the statement and describes the manner in which it was produced giving the particulars of the device involved in the production of that record and deals with the conditions mentioned in **Section 65-B(2)** and is signed by a person occupying a responsible official position in relation to the operation of the relevant device 'shall be evidence of any matter stated in the certificate’.

Entries in books of account, including those maintained in electronic form, An entry in any public or other official book, register or by a public servant in the discharge of official duty in the performance of a duty specially enjoined by the law of the country in which such book, register, or record or an electronic record is kept are the relevant facts as per **Section 34 and 35** of evidence Act

As it is already laid down provision u/s45 regarding the relevancy of expert opinion referred to in **Section 79A** of I.T Act, now we have **Section 45A** to consider opinion given by an examiner of electronic evidence regarding any information transmitted or stored in any computer resource or any other electronic or digital form is also relevant fact.

As like other expert opinions, court may rely up on the opinion of an examiner who has given in the manner prescribed under **Section 79A** of I.T.ACT.

Further, when the court has to form an opinion as to the electronic signature of any person, the opinion of the certifying Authority, which has issued the electronic Signature Certificate, is also relevant under **Section 47A** of evidence Act.

The Court analyzing the admissibility of electronic record in light of the judgment pronounced in **Navjot Sandhu’s** case observed that:[[11]](#footnote-12)

“….It appears, the court omitted to take note of **Sections 59 and 65A**, while dealing with the admissibility of electronic record in that case. **Sections 63 and 65** have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by **Sections 65A and 65B**. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this court in Navjot Sandhu case (supra), does not lay down the correct legal position. It requires to be overruled and we do so…”

**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.

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 **Section 8Se** of the Evidence Act, 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.[[12]](#footnote-13)

Under 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.

In ***State (NCT of Delhi) vs. Navjot Sandhu (AIR 2005 SC 3820)[[13]](#footnote-14)***

In this significant judgment, the Supreme Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and also the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible.[[14]](#footnote-15)

The judgment would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anticorruption where the reliance is being placed on the audio-video recordings which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD are being forwarded without a certificate U/s 65B Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. It was further observed that all these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. 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.

In the anticorruption cases launched by the CBI and anticorruption/Vigilance agencies of the State, even the original recording which are recorded either in Digital Voice Recorders/mobile phones are not been preserved and thus, once the original recording is destroyed, there cannot be any question of issuing the certificate under Section 65B(4) of the Evidence Act. Therefore in such cases, neither CD/DVD containing such recordings are admissible and cannot be exhibited into evidence nor the oral testimony or expert opinion is admissible and as such, the recording/data in the CD/DVD’s cannot become a sole basis for the conviction.

In the aforesaid Judgment, the Court has held that Section 65B of the Evidence Act being a ‘not obstante clause’ would override the general law on secondary evidence under Section 63 and 65 of the Evidence Act. The Section 63 and Section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65A and 65B of the Evidence Act. The Constitution Bench of the Supreme Court overruled the judgment laid down in the **State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru[(2005) 11 SCC 600** 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 required to be overruled.

The only options to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence court or it’s copy by way secondary evidence U/s 65A/65B of Evidence Act. Thus, in the case of CD, DVD, Memory Card etc. containing secondary evidence, the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible

It has thus been seen that with the increasing impact of technology in everyday life, the production of electronic evidence has become a necessity in most cases to establish the guilt of the accused or the liability of the defendant. The shift in the judicial mindset has occurred mostly in the past twenty years and most legal systems across the world have amended their laws to accommodate such change.

Further, when society is largely utilized computers and even investigation seeks help of gadgets which product of modern electronic technology prosecution is need to be armed with latest technological knowledge and basics of admissibility of electronic evidence as well.

In India, all electronic records are now considered to be documents, thus making them primary evidence. At the same time, a blanket rule against hearsay has been created in respect of computer output. These two changes in the stance of the law have created paradigm shifts in the admissibility and relevancy of electronic evidence, albeit certain precautions still being necessary. However, technology has itself provided answers to problems raised by it, and computer forensics ensure that manipulations in electronic evidence show up clearly in the record. Human beings now only need to ensure that electronic evidence being admitted is relevant to the fact in issue and is in accordance with the Constitution and other laws of the land.

Electronic communications will continue to revolutionize how the world does business and how individuals instantly engage with friends and family. E-evidence is undeniably a critical new evidentiary frontier which has left both judges and attorneys struggling to understand how the admissibility of this new information fits into existing legal paradigms. Despite this uncertainty, one thing is clear: the use of e-evidence will continue to play an ever-increasing critical role in both civil and criminal litigation. Because e-evidence can have a substantial impact at trial, it is vitally important for attorneys and the court to stay in touch with ongoing legal and technological developments. It is strongly recommended that admissibility issues involving electronic evidence be raised and discussed with the court prior to commencement of trial.

1. **\*Mr.** **Sahil Tandon., BBA LL.B(Hons.), Symbiosis Law School, Noida.** [↑](#footnote-ref-2)
2. Arora, N. (2015). *Admissibility of Electronic Evidence : Challenges for Legal Fraternity | A Platform to discuss & analyse Financial and Cyber ForensicsA Platform to discuss & analyse Financial and Cyber Forensics*. *Neerajaarora.com*. Retrieved 28 March 2015, from http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/ [↑](#footnote-ref-3)
3. http://www.lawyersclubindia.com/articles/Electronic-Evidence-and-its-admissibility-5703.asp#.VRZHxVsxHos [↑](#footnote-ref-4)
4. <http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/> [↑](#footnote-ref-5)
5. Pendleton, H. (2013). *Admissibility of Electronic Evidence: A New Evidentiary Frontier | Bench and Bar of Minnesota*. *Mnbenchbar.com*. Retrieved 28 March 2015, from <http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/> [↑](#footnote-ref-6)
6. RANA, D. (2015). *Electronic Evidence and its admissibility*. *Lawyersclubindia*. Retrieved 28 March 2015, from <http://www.lawyersclubindia.com/articles/Electronic-Evidence-and-its-admissibility-5703.asp#.VRZHxVsxHos> [↑](#footnote-ref-7)
7. Rahurkar, S. (2013). *Indian Evidence Act and Digital Evidence | ClubHACK Magazine*. *Chmag.in*. Retrieved 28 March 2015, from <http://www.chmag.in/article/apr2013/indian-evidence-act-and-digital-evidence> [↑](#footnote-ref-8)
8. <http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/> [↑](#footnote-ref-9)
9. Singh, V. (2015). *Special law of Electronic Evidence: Supreme Court Clarifies the Necessity to comply with Section 65B of Evidence Act - IndiaLaw*. *IndiaLaw*. Retrieved 28 March 2015, from <http://www.indialaw.in/special-law-electronic-evidence-supreme-court-clarifies-necessity-comply-section-65b-evidence-act/> [↑](#footnote-ref-10)
10. http://www.lawyersclubindia.com/articles/Electronic-Evidence-and-its-admissibility-5703.asp [↑](#footnote-ref-11)
11. <http://www.indialaw.in/special-law-electronic-evidence-supreme-court-clarifies-necessity-comply-section-65b-evidence-act/> [↑](#footnote-ref-12)
12. <http://www.hcmadras.tn.nic.in/jacademy/article/Electronic%20Evidence%20PSJ.pdf> [↑](#footnote-ref-13)
13. (2011). Retrieved 28 March 2015, from <http://www.hcmadras.tn.nic.in/jacademy/article/Electronic%20Evidence%20PSJ.pdf> [↑](#footnote-ref-14)
14. http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/ [↑](#footnote-ref-15)