

Recent trends in admissibility of electronic evidence: challenges for legal fraternity

*Prem Pratap Singh Chauhan**

Advanced technology and evolution of communication systems have substantially transformed the process of exchanging information in all spheres. The use of digital media in unlawful activities has increased so dramatically that investigation of any criminal activity nowadays produce electronic evidence. However, the rapid growth in the number of cases involving electronic evidence has all-too-often found law enforcement and the judiciary not advanced enough to deal with the new issues evolving out of such evidence. The gathering, conservation, communication and presentation of the digital evidence must fulfil legal requirements for the admissibility of the evidence.¹ Electronic evidence which has been collected during investigation that is not in conformity with the law would be declared inadmissible and be ruled out of court.

Electronic Evidence and the Indian Evidence Act 1872

The kinds of evidence that we are dealing with in this article has been variously described as 'electronic evidence', 'digital evidence' or 'computer evidence'. Digital Evidence is “information of probative value that is stored or transmitted in binary form”.²

Section 3 of Indian Evidence Act, 1872 fundamentally describes two types of evidence -

- a) the evidence of witness i.e. oral evidence, and
- b) documentary evidence which includes *electronic records produced for the inspection of the court*. Section 3 of the Evidence Act was amended by virtue of Section 92 of Information Technology Act, 2000 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”.

* Student VI Semester; National Law University & Judicial Academy, Assam

1. Olivier Leroux, *Legal admissibility of Electronic Evidence*, 18 IRLCT. 193, 202 (2004).

2. Eoghan Casey, *Digital Evidence and Computer Crime 7-8 (3d Ed, 2011)*.

Electronic Record-

As per Section 2(t) of the Information Technology Act, 2000, the wider connotation has been given to an electronic record. Sec 2(t) defines 'electronic record' as meaning, “data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro film”.

Legal Recognition of Electronic Records (Section 4 of the IT Act)

Where any law provides that information or any other matter shall be in writing or typewritten or in printed form, then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is- (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference.

Admissions in Electronic Form-

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

Relevancy of Oral Evidence regarding Electronic Evidence-

Section 22A of Evidence Act provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question.

In the context of documentary evidence, in Section 59 of Evidence Act, for the words “Content of documents” the words “Content of documents or electronic records” have been substituted.

Admissibility of Electronic Evidence

New Sections 65A and 65B of Evidence Act are inserted to incorporate the admissibility of electronic evidence in the Evidence Act under the Second Schedule to the IT Act, 2000. Section 5 of the Evidence Act defines that evidence can be given regarding only facts that are at issue or of relevance. Further, ***Section 136 empowers a judge to decide on the matter of the admissibility of the evidence.***

Section 65A of Evidence Act provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B .

Section 65B of Evidence Act provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record, is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that all conditions set out in Section 65B are satisfied.³

Conditions for the Admissibility of Electronic Evidence

Section 65B (1)

States that if any information contained in an electronic record produced from a computer (known as computer output) has been copied on to a 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 65B(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.'

Section 65B (2)-

- (a) At the time of creation of the electronic records, the computer that produced it must have been in regular use;
- (b) The kind of information contained in the electronic record must have been regularly and ordinarily fed into the computer;⁴
- (c) The computer was operation properly; and,
- (d) The duplicate copy must be a reproduction of the original electronic record.

Section 65B (4) -

Regarding the person who can issue the certificate and contents of certificate, it provides the certificate doing any of the following things:

- (a) Identifying the electronic record containing the statement;
- (b) Describing the manner in which the electronic record was produced;

3. *Smt. K.B. Agarwal, Admissibility of Electronic Record, Video Recording,, Computer Outputs, Maharashtra Judicial Academy (Jun. 20, 2017, 10:04 AM), <http://mja.gov.in/Site/Upload/GR/final.html>.*

4. *Vivek Dubey, Admissibility of Electronic Evidence: An Indian Perspective, FRCLJ, Mar. 2017, at 1, 3.*

- (c) Furnishing the particulars of the device involved in the production of that record.
- (d) Dealing with the applicable conditions mentioned under Section 65B (2) of the Evidence Act; and
- (e) Signed by a person occupying a responsible official position in relation to the operation of the relevant device.

By referring to the above mentioned definitions in the light of the provisions incorporated under section 65A & 65B of the Evidence Act, **electronic evidence** is now another kind of documentary evidence which is *if duly proved in the manner provided in Sec 65-B*, can be considered as a strong evidence.

Compulsory authentication of Digital Evidence

Over the years, with increased exposure to electronic evidences, there has been a progression from an age of treating electronic evidences as ordinary documents. However, it took the period of nine years before the Supreme Court conclusively decided that documentary evidence in the form of an electronic record can be proved only in conformity with the procedure set out under section 65B of the Evidence Act.

A path breaking case law on electronic evidence is discussed below providing an insight into the proof of electronic evidence.

Anvar P.V. vs. P.K. Basheer & Ors⁵

Fact- Mr. P.V. Anwar filed an appeal, who had lost the previous Assembly election in Kerala, and contended that respondent Mr. Basheer was involved in tarnishing his image and his character by producing songs containing defamatory content on Compact Disk (Cds).

Issue- Can courts admit electronic records as prima facie evidence without authentication?

Held- The Supreme Court declined to accept the admissibility of the electronic records as prima facie evidence without authentication in the court of law. It was held that in regard to any electronic record, for instance a CD, VCD, chip, etc., the same must be accompanied by the certificate according to the terms of section 65B obtained at the time

5. *Anvar P.V. vs. P.K. Basheer & Ors*, (2014) 10 SCC 473 (India).

of the taking the document, without which, the secondary evidence pertaining to that electronic record is inadmissible. Hence, strict compliance with section 65B is now mandatory for admissibility of the e-mails, web sites or any electronic record in a civil or criminal trial before the courts in India.

Analysis-

(1) In this case, the Supreme Court overruled the decision in the case of *Navjot Sandhu*,⁶ and redefined the evidentiary admissibility of electronic evidences to correctly reflect the letter of the Evidence Act by reinterpreting the application of sections 63, 65 and 65B of the Evidence Act.

(2) This view 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 judgement, Kurian J observed, at, 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.”

(3) This progressive and disciplined approach of Indian courts is a consequence of a proper recognition and appreciation of the nature of electronic records itself. This is landmark decision as it will not only save the courts time wasted in parties attempting to prove the electronic records through secondary oral evidence in form of cross examinations, but also discourage the admission of forged and tampered electronic records.⁷

Recent Trends in Admissibility of the Electronic Evidences

1. Admissibility of Interviews as Evidence: All digital evidence presents the possibility of alteration or fabrication. From an evidentiary standpoint, a traditional authentication foundation, however minimal, likely will suffice for admissibility.⁸

6. *State (N.C.T. Of Delhi) vs. Navjot Sandhu@Afsan Guru*, (2005) 11 SCC 600 (India).

7. *Tejas Karia. et al, The Supreme Court of India re-defines admissibility of electronic evidence in India*, 12 DEESLR. 33, 36 (2015).

8. *Fredric Lederer, The New Courtroom: the Intersection of Evidence and Technology; Some Thoughts on the Evidentiary Aspects of Technologically Produced or Presented Evidence*, 28 SWUL. 1, 5 (1999).

In several recent rulings, our superior courts, by interpreting **Section 273 of the Criminal Procedure Code** in the light of the technological advancements, held that recording of evidence through **video conferencing** would be perfectly legal in the court of law.

In *State of Maharashtra vs. Dr. Praful B Desai*,⁹ the question whether a witness can be examined by means of a video conference was discussed. The Apex Court observed that:

“Video conferencing is a real advancement of science and technology which permits seeing, hearing and talking with someone who is non-physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of 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”.

This Apex Court decision has been followed as precedent in other High Court rulings (e.g. *Amitabh Bagchi vs Ena Bagchi*)¹⁰ more recently, the High Court of Andhra Pradesh in *Bodala Murali Krishna vs. Bodala Prathima*,¹¹ held that necessary precautions must be taken to identify the witness and ensure the accuracy of the equipment being used. In addition, any party wishing to avail itself of the facility of video conferencing must meet the entire expense.

In *Jagjit Singh vs. State of Haryana*,¹² the Hon'ble Supreme Court considered the digital evidence in the form of interview transcripts from the Zee News television channel and 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 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.**

9. *State of Maharashtra v. Dr. Praful B Desai*, AIR 2003 SC 2053 (India).

10. *State of Maharashtra v. Dr. Praful B Desai*, AIR 2005 Cal 11 (India).

11. *Bodala Murali Krishna v. Bodala Prathima*, 2007 (2) ALD 72 (India).

12. *Jagjit Singh v. State of Haryana*, (2006) 11 SCC 1 (India).

2. Admissibility of Skype as Evidence:

In **Dasam Vijay Rama Rao v. M. Sai Sri**,¹³ the Hon'ble High Court of Telangana and Andhra Pradesh permitted the use of skype technology for appearance of party in court. It held as follows:

“Technology, particularly, in the information sector has improved by leaps and bounds. Courts in India are also making efforts to put to use the technologies available. Skype is one such facility, which is easily available. Therefore, the Family Courts are justified in seeking the assistance of any particular case. For that purpose, the parties can be permitted to be represented by a legal practitioner, who can bring a mobile device. By using the skype technology, parties who are staying abroad can not only be identified by the Family Court, but also enquired about the free will and consent of such party.

This will enable the litigation costs to be reduced greatly and will also save precious time of the Court. Further, the other party available in the Court can also help the Court in not only identifying the other party, but would be able to ascertain the required information.”

3. Admissibility of e-mail as Evidence:

In **Abdul Rahaman Kunji vs. The State of West Bengal**,¹⁴ the Hon'ble High Court of Calcutta while deciding the admissibility of email held that an email downloaded and printed from the email account of the person can be proved by virtue of Section 65B read with Section 88A of Evidence Act. The testimony of the witness to carry out such procedure to download and print the same is sufficient to prove the electronic communication.

Their Lordship further observed, inter alia, that an electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under section 65B are satisfied as observed in the P.V. Anvar case.

4. Admissibility of Cell-phone recording- Evidentiary Value as Evidence:

In **State (NCT of Delhi) vs. Navjot Sandhu @Afsan Guru**,¹⁵ there was

13. *Dasam Vijay Rama Rao vs. M. Sai Sri, C.R.P. No. 1621 of 2015 (India).*

14. *Abdul RahamanKunji vs.The State of West Bengal, MANU/WB/0828/2014 (India).*

15. *State (NCT of Delhi) v. NavjotSandhu @Afsan GAIR 2005 SC 3820 (India).*

an appeal against conviction following the attack on Parliament on December 13, 2001. This case dealt with the proof and admissibility of call records of the mobile telephone. 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 call records of the telephone records, because the prosecution had failed to produce the relevant certificate under Section 65B (4) of the Indian Evidence Act. The Supreme Court held as follows:

“150. ... irrespective of the compliance with the requirement of section 65B, which is a provision dealing with admissibility of the electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely, section 63 & 65. It may be that the certificate containing the details in Sub-section (4) of section 65B is not filed in the instance case, but that does not mean that secondary evidence can't be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely, sections 63 & 65 of the Evidence Act”.

5. Admissibility of Telephone call in a CD and CDR:

In *Jagdeo Singh vs. The State and Ors*,¹⁶ the Hon'ble High Court of Delhi, while considering with the admissibility of intercepted telephone call in a CD and CDR which were without a certificate under section 65B of the Evidence Act, the court observed that the secondary electronic evidence without certificate under section 65B of the Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever.

6. Admissibility of Interview telecasted on TV channels as Evidence:

The Apex Court has added a new, and significant, chapter to the conservative criminal jurisprudence and given a role to the media in criminal trials by ruling that interviews given by an accused to TV channels could be considered evidence by courts, whereby enhancing the power of the already powerful media. No doubt such a decision is a fabulous step in the direction of curtailing the misuse of the freedom of speech, which in the recent years has been used to mislead the investigation process. Still there are serious issues that need to be deliberated as to how such a scenario will fit into the existing evidence mechanism.

¹⁶. *Jagdeo Singh v. The State and Ors*, MANU/DE/0376/2015 (India).

In *Sharad Yadav and Ors. v. Union of India (UOI) and Anr*,¹⁷ Shri Sharad Yadav in an interview recorded in Hindi, had admitted having received a sum of Rs. 3 lac from one Jain and the said interview was telecasted on Doordarshan after due editing. Hindi version of said interview has been produced before the Court, which is as follows:

“MUJHE CHMMAN BHAI PATEL KE SAATH EK JAIN AIYA THA USNE TEEN LAKH RUPEEYE DIYE HAIN AUR WOH TEEN LAKH RUPEEYE JO CHANDE KE AIYE HAIN WOH MAIN NE KISKO DIYE HAIN PARTY KI TARAF SE WOH BHI LIKHA HUWA HAI”

In this case, it was observed that , the aforesaid video recorded interviews of Shri SharadY adav do not amount to confessions and can't, therefore, be used to complete the offence, with which Shri Yadav was charged. In this case, considering the dicta as observed in *Palvinder Kaur v. State of Punjab*¹⁸ and *CBI v. V.C. Shukla and Ors*,¹⁹ it was further observed that “it would be unfair to admit only the statements against interest while excluding part of the same interview or series of interviews.”

In *Sajid beg Asif beg Mirza v. State of Gujarat*,²⁰ the Supreme Court dismissed Mirza's petition saying, There is no merit in it. However, it said, “it goes without saying that the relevance and admissibility of the statement, if any, given by accused before the media persons shall be considered at the appropriate state in the trial.” Once the “shall” word is used in the direction, then the trial court will definitely consider the admissibility.

Analysis:

The Supreme Court verdict saying that TV interviews can be used as evidence in a case where it has been given, gives more weight to the saying 'Think before you speak'. While this verdict gives more muscle to the media, will it deter the accused from make controversial statements to media. In this light, the Apex Court's order that the trial court could consider admissibility of statements given by an accused to the media, is not only a significant leap in law but also a trend-setter.

17. *SharadYadav and Ors. vs. Union of India (UOI) and Anr*, 1999 (51) DRJ 371 (India).

18. *PalvinderKaur v. State of Punjab*, AIR 1954 SC 354 (India).

19. *CBI v. V.C. Shukla and Ors*, (2000) 52 DRJ 247 (India).

20. *SajidbegAsifbeg Mirza v. State of Gujarat*,(2007) 1 GLH 400(India).

Challenges to Legal Fraternity

The different categories of electronic evidence such as website data, social network communication, e-mail, SMS/MMS and computer generated documents poses unique problem and challenges to legal fraternity for proper authentication and subject to a different set of views. Some of the major challenges are as follows:

(1) Authentication of electronic evidence:

The authentication of digital evidence is one of the biggest challenges that courts have to deal. It has to make sure that the records were not manipulated, altered or damaged between the time they were created and put forward in courts. Justice Muralidhar in one of his speeches, once pointed out:

“One of the advantages of electronic evidence is the ease with which it can be replicated, but the challenge is how to preserve it and how to make back up records. The possibility of originals getting lost, damaged, or destroyed is a very real one.”

Providing the reliability to the evidence from social networking sites sometimes become a questionable task for the courts because firstly establishing the author of the document can be difficult since there are number of people writing on one page of social media sites.

(2) Lack of Readiness:

It is one of the multidimensional concepts that includes technical infrastructure, the process for receiving, playing, storing, retaining and accessing digital evidences. Mainly each court has its different level of readiness in order to handle digital evidence. Many Indian courts do not have essential readiness as it was recognised by the Supreme Court in the *State of Punjab vs. Amritsar Beverages Ltd.*,²¹ -

“There are a lot of difficulties faced by investigating officers due to lack of scientific expertise and insight into digital evidences techniques. The court also noted that IT Act does not deal with all types of problems and hence the agencies are seriously handicapped in some respects.”

21. *State of Punjab vs. Amritsar Beverages Ltd*, AIR 2007 SC590 (India).

(3) Privacy:

Despite being long struggled with the issue of privacy in other areas, a new concern has been raised by the digital video evidence. It regularly captures the video of those parties that are not even parties to the case. Though individual may not necessarily have an expectation of privacy in public places, but many may feel being included as a bystander in video evidence violates cultural expectations of reasonable anonymity. In solution to this, in most of the cases, the privacy concerns used to redecorate or blur out the faces of bystanders before the video being present in court as evidence. But for handling the increasing work load of such issue, the strict redaction policies are needed.

(4) Transporting and storing digital evidence:

Proper considerations should be taken on the methods by which any electronic evidences should be transported and stored which is a challenge for most of the courts due to lack of proper infrastructure and readiness. While transporting and storing the information, full security should be taken to ensure that it is not altered or manipulated. Proper and appropriate storage conditions should be provided in order to protect the hardware and digital evidences from dirt, fluids, humidity, temperature and strong magnetic fields.

How far is it successful?

1. Delivering Simple and Speedy Justice System

In a decision reported in *Mohd. Hussain @ Julpikar Ali vs. State (Government of NCT of Delhi)*, Hon'ble Supreme Court has observed as follows:

“A speedy justice and fair trial to a person accused of a crime are integral part of Article 21; they are imperatives of the dispensation of justice”.

Thus, the admissibility of digital/ electronic evidence has accelerated the proceedings of the courts in bringing the justice mainly in most complicated cases.

2. Making Criminal Prosecution Easier

Talking about terrorism, recent terrorist attack are caused by using

highly sophisticated technology. For prosecution, it becomes much easier to produce electronic evidence in courts as compared to the traditional forms of evidence which may not even exist.

Conclusion

In 21st Century, we saw rapid rise in the field of information and communication technology. The expanding horizons of science and technology have thrown new challenges to the legal fraternity. Storage, processing and transmission of data on magnetic and silicon medium become cost effective and also easy to handle whereas the conventional means of record and data processing become outdated. Therefore, law had to respond and gallop with the technical advancement.

The appropriate amendments in Evidence Act, incorporated by Indian judiciary show pro-activism. Now, it is needed that the law enforcement agencies and investigating officers have to update themselves with the authentication process prescribed by the court regarding the admissibility of electronic evidences so that impediments in trial procedures can be successfully overcome. The foremost requirement of recent times is the proper training of law enforcement agencies in handling cyber related evidence and correct application of procedure and sections of Evidence Act while presenting such evidence in court.

India has to go a long way in keeping pace with the developments globally. 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. The court has to see that the correct evidence is presented and administered so as to facilitate a smooth working of legal system. Sound and informed governance practices along with scrutiny by the courts must be adopted to determine whether the evidence fulfils the three essential legal requirements of authenticity, reliability and integrity. With an optimistic view, the Supreme Court having re-defined the rules, the Indian courts should adopt a consistent approach, and will execute all possible safeguards required for accepting and appreciating electronic evidence.

Let me conclude this paper with a suggestion that there must be a Digital Evidence Act for regulation on incident response.
