ARTICLE:

The Supreme Court of India re-defines admissibility of electronic evidence in India

By **Tejas Karia, Akhil Anand and Bahaar Dhawan**

Relevance of electronic evidence

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.

This increased use of technology, however, poses challenges accommodating and reflecting the new age developments in laws across jurisdictions, which in turn has provided the much required impetus to the emergence and appreciation of digital evidence. Keeping up with the times, requisite amendments were also made to Indian laws in the year 2000 with introduction of the Information Technology Act, 2000 ('IT Act'), which brought in corresponding amendments to existing Indian statutes to make digital evidence admissible. The IT Act, which is based on the UNCITRAL Model Law on Electronic Commerce, led to amendments in the Indian Evidence Act, 1872 ('Evidence Act'), the Indian Penal Code, 1860 ('IPC') and the Banker's Book Evidence Act, 1891.

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.

While the admissibility of electronic evidence in legal proceedings is not new in India, with the passage of time, the safeguards employed for enabling the production of documents have changed substantially, especially since the storage and use of electronic information has increased and become more complex. Recently, the Supreme Court of India in case of *Anvar P. K. vs. P.K Basheer &Ors.*,[1] overruled the earlier decision the case of the *State (NCT of Delhi) v Navjot Sandhu*,[2] also popularly known as the 'Parliament Attacks' case. The Supreme Court redefined the evidentiary admissibility of electronic records to correctly reflect the provisions of the Evidence Act by reinterpreting the application of sections 63, 65 and 65B.

A brief background of the Evidence Act and the underlying principles of evidence will help the reader to understand and appreciate the real purport and implications of the decision of Supreme Court in its true spirit and the manner in which digital records can be adduced as evidence in Indian courts.[3]

Principles and salient provisions of the Evidence Act

Conventionally, 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 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.

While primary evidence of the document is the document itself, 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

[1] (2014) 10SCC 473.
[2] (2005) 11 SCC 600.
[3] See also Manisha T. Karia and Tejas D. Karia, 'India' (Chapter 13) in Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).

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 (i) is in hostile possession; (ii) or has been proved by the prejudiced party itself or any of its representatives; (iii) is lost or destroyed; (iv) cannot be easily moved, i.e. physically brought to the court; (v) is a public document of the state; (vi) can be proved by certified copies when the law narrowly permits; and (vii) is a collection of several documents.

With the advent of the digitisation of documents, the hearsay rule faced further challenges and dilution. With increased digitization of documents, evidence was now mostly electronically stored which meant greater propensity for adducing secondary evidence in case of digital evidence.[4]

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. Printed reproductions or transcripts of the electronic record would be prepared and its authenticity was certified by a competent signatory, who would identify their signature in court and be open to cross examination. However, this procedure was rather archaic, based on the law drafted a century ago, and did not include the meta data where it was available, such as the header information in e-mails, for instance. This long drawn procedure was also open to abuse and did not ensure the authenticity of the record. It became clear that the electronic- record can no longer be treated on the same footing as that of regular documents. It was time to introduce new provisions to deal exclusively with evidence that is available in digital form. As the pace and proliferation of technology expanded, the creation and storage of electronic information grew more complex, the law had to change more substantially.

Admissibility of electronic records

The Evidence Act has been amended from time to time, especially to provide for the admissibility of electronic records along with paper based documents as evidence in the Indian courts. Some of the significant amendments include granting electronic records the status of documents for the purpose of adducing evidence.[5] The definition of 'admission'[6] was changed to include a statement, oral or documentary, or contained in electronic form, which suggests any inference as to any fact in issue or relevant fact, while section 22A was inserted to provide for the relevancy of oral evidence as to the contents of electronic records. It provides that oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic records that are produced is in question.

Perhaps the most important amendment to the Evidence Act has been the introduction of sections 65A and 65B under the second schedule of the IT Act,[7] which provides for a special procedure for adducing evidence in relation to electronic records. Section 65B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record (whether it be the contents of a document or communication printed on a paper, or stored, recorded, copied in optical or magnetic media produced by a computer), is deemed to be a document and is admissible in evidence without further proof of the production of the original, providing the conditions set out in section 65B for the admissibility of evidence are satisfied, which have been set out as under:

> 1. At the time of creation of the electronic record, the computer output containing the information was produced from a computer that was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer.
>
> 2. During the period, the kind of information contained in the electronic record was regularly fed in to the computer in the ordinary course of the activities.

[4] For an essay on this issue, see Stephen Mason, 'Electronic evidence and the meaning of 'original'' *Amicus Curiae* The Journal of the Society for Advanced Legal Studies Issue 79 Autumn 2009 26-28, available at http://sas-space.sas.ac.uk/2565/.

[5] Section 3 of the Indian Evidence Act, 1872.
[6] Section 17 of the Indian Evidence Act, 1872.
[7] Section 92 of the Information Technology Act, 2000.

3. Throughout the material part of the period, the computer was operating properly or, if not, the computer was out of operation for some period, but it was not such to affect the electronic record or the accuracy of the contents.

4. The electronic record bears the information that is a reproduction of the original electronic record.

Section 65B (4) mandates the production of a certificate of authenticity of electronic evidence which is signed by a responsible person who was responsible for the computer on which the electronic was created or stored, in order to certify the qualifications set out above. The certificate must uniquely identify the original electronic record, describe the manner of its creation, describe the particulars of the device that created it, and certify compliance with the conditions of sub-section (2) of section 65B. Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of section 65B.

Risk of manipulation and compliance with the provisions of section 65B of the Evidence Act

Despite the mandatory nature of these conditions, the law has been applied inconsistently. For instance, the certificate of authenticity has not always been filed with the electronic records in legal proceedings. For instance, in the case of *State (NCT of Delhi) v. Navjot Sandhu*,[8] the Supreme Court had held that courts could admit electronic records such as printouts and compact discs (CDs) as prima facie evidence without authentication. This case dealt with the proof and admissibility of the records of mobile telephone calls. The accused made a submission that no reliance could be placed on the mobile telephone records because the prosecution had failed to produce the relevant certificate under section 65B(4) of the Evidence Act and that the procedure set out in section 65B of the Evidence Act was not followed. The Supreme Court concluded that a cross examination of the competent witness acquainted with the functioning of the computer during the relevant time and manner in which the printouts of the call records were taken was sufficient to prove the call records. As a result, the printouts and CDs were not compared to the original electronic record or certified at the time of adducing it as evidence.

This trend of ignoring the special procedure prescribed for adducing electronic records as evidence was seen even in subsequent cases. For instance, the case of *Ratan Tata v. Union of India*[9] 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.

Unfortunately, the lower judiciary in India are largely technologically unreliable, and do not appreciate the authenticity issues or ensure safeguards while allowing the admission of electronic evidence, barring a few exceptions.[10] These decisions of the Supreme Court set up a further precedent for the lower judiciary to appreciate the special procedure prescribed for electronic evidence.

The decisions set out above lost sight of the fact that it was precisely for the reason that printed copies of the electronic records would be vulnerable to manipulation and abuse that the legislature promulgated a special procedure for adducing electronic records as evidence in court.[11] Since the Evidence Act provides all forms of computer outputs to be admissible as evidence, the courts, ignoring the provisions of section 65B(4), have ignored and overlooked the intrinsic nature of electronic evidence and exposed digital evidence to the risk of manipulation. In this respect, the courts in India have not taken up the discussion on this topic by Mason. Therefore, for a very long period, unless the credibility of the digital evidence itself was in question, courts have not raised any apprehension regarding the authenticity or require the intervention of forensic teams to determine the veracity of the record, and electronic records filed in the court were premised to be correct without being subject to any checks and balances.

Briefly, the position regarding authentication in the United States of America is not consistent. A series of

[8] (2005) 11 SCC 600.

[9] Writ Petition (Civil) 398 of 2010 before Supreme Court of India.

[10] Perhaps the judicial authorities might like to read the following: In particular, see Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 16 – 24 and Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 23 – 28.

[11] See how courts in other jurisdictions deal with these issues: Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), chapter 4.

tests advocated by Professor Imwinkelried[12] were followed in *In re Vee Vinhnee, debtor, American Express Travel Related Services Company, Inc. v Vee Vinhnee*,[13] but no consideration has been given to the criticisms of part of this test.[14] In England and Wales, the approach tends to consider the other evidence surrounding the facts of the case to determine authenticity,[15] and in Singapore, reliance is made on section 3(1) of the Singapore Evidence Act (Cap 97, 1997 Rev ed.), which provides for the admissibility of digital evidence. The new regime in Singapore after the Evidence (Amendment) Act 2012, provides that rules of best evidence and the rules on authentication applies to electronic evidence in the same manner as any other item of evidence.[16]

Mandatory authentication of digital evidence

Over the years, with increased exposure to electronic records, there has been a progression from an age of treating electronic records as ordinary documents. However, it took nine years before the Supreme Court conclusively decided that documentary evidence in the form of an electronic record can be proved only in accordance with the procedure set out under section 65B of the Evidence Act. In *Anvar P. K. vs. P.K Basheer &Ors.*,[17] the Supreme Court overruled the decision in the case of *Navjot Sandhu*,[18] and redefined the evidentiary admissibility of electronic records to correctly reflect the letter of the Evidence Act by re-interpreting the application of sections 63, 65 and 65B of the Evidence Act. In this case, Mr P.V. Anwar had filed an appeal, who had lost the previous Assembly election in Kerala, and contended that his opponent P. K. Basheer, MLA had tarnished his image and had indulged in character assassination and the defamatory content was recorded in songs and on CDs.

The Supreme Court declined to accept the view that the courts could admit electronic records as prima facie evidence without authentication. It was held that in the case of any electronic record, for instance a CD, VCD, chip, etc., the same must 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. Hence, 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, at [15], 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.'

The progressive and disciplined approach of the Indian courts in ensuring compliance of the safeguards for relying on digital evidence is a result of a proper recognition and appreciation of the nature of electronic records itself. This is a landmark decision for India in the methods of taking evidence, 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 fudged and tampered electronic records from being relied upon, albeit certain precautions for authenticity of the electronic records will continue to be necessary. Therefore, the computer generated electronic record cannot be solely relied upon, because there is a possibility of it being hampered and should be used as a corroborative evidence.

The need for additional safeguards

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

[12] Edward J. Imwinkelried, *Evidentiary Foundations* (LexisNexis, 2005), para 4.03[2].
[13] 336 B.R. 437 (9th Cir. BAP 2005).
[14] Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 4.24.
[15] Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 4.26; see also chapter 10.
[16] Daniel Seng and Bryan Tan, 'Singapore' (chapter 17) in Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).
[17] (2014) 10 SCC 473.
[18] (2005) 11 SCC 600.

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. This is an additional condition that has been provided under the Evidence (Amendment) Act, 1996 of Singapore.

For instance, a bailiff's report can often be relied upon as a suitable means for proving a certain facts in France. The French jurisprudence on this issue has developed to provide a number of technical conditions that the bailiff should comply with while making statements about web sites so as to uphold that the probative value of his certified report.[19]

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.[21]

Paradigm shift – but a long way to go

Although the changes are certainly a leap in the right direction and help towards a paradigm shift in the legal framework, however, given 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. From the foregoing, 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.

Conclusion

It is clear that the admission of electronic evidence is the norm across all jurisdictions, rather than the exclusion. Along with advantages, the admissibility of electronic records can also be complex – although some jurisdictions have imposed the requirements regarding admissibility as in India.[22] It is, thus, upon the 'keepers of law', the courts to see that the correct evidence is presented and administered so as to facilitate a smooth working of the 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. Hopefully, with the Supreme Court having re-defined the rules, the Indian courts will adopt a consistent approach, and will execute all possible safeguards for accepting and appreciating electronic evidence.

Tejas Karia is a member of the editorial board

[19] Tim Van Canneyt and Christophe Verdure, 'Bailiffs on the internet and the validity of their certified reports: Lessons learned from the French and Belgian courts', 7 *Digital Evidence and Electronic Signature Law Review*, (2010) 71 – 76.

[20] It should be noted that the term 'reliability' is not correct, for which see Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), chapter 5.

[21] A number of jurisdictions in Europe have court-appointed digital evidence specialists, for which see Stephen Mason, ed, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008).

[22] For which see Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012, chapter 4.c