PSYCHOLOGY AND EDUCATION (2021) 58(5), ISSN 1553 -6939
Article Received: 22th November, 2020; Article Revised: 26th March, 2021; Article Accepted: 26th April, 2021

Revisiting the Admissibility of Electronic Evidence: Indian Jurisdictions & Notes from Other Countries

Nibras Salim Khudhair
Law Department- Al Kunooze University College
Basra, Iraq
Email: nibras.s@kunoozu.edu.iq

Abstract

Admissibility of electronic evidence in Indian courts is regulated under section 65B of the Evidence Act, 1871.[1]Section 65B(2) details the criteria for admission of electronic evidence before a court of law and section 65B(4) requires mandatory certification of the same .Such provisions followed the judgement in *Anvar v. Basheer*[2]where the Supreme Court had overturned a previous SC judgement in *State (NCT of Delhi) v. Navjot Sandhu*[3]. In the latter case, it was ruledthat a piece of electronic evidence did not need to comply with criteria under section 65B(2) and the same could be admitted through sections 63 and 65[4]. The former case overruled the latter judgement subjecting the admission of electronic evidence exclusive to the provisions under section 65B. While this solves the problems related with the integrity of electronic evidence in certain civil cases, it has been argued in this article that the same leads to the exclusion of a large amount of authentic electronic evidence from the consideration of the courts. This article investigates the development in other jurisdictions and taking cues from the prevalent admission procedures for electronic evidence in the UK, the USA, and Canada, concludes that the Indian system too needs a balanced approach that (i) does not exclude the vast amount of evidence in electronic form in cases where meeting all the criteria under section 65B may not be feasible, and (ii) ensures the integrity of the evidence at the same time.

[1]Indian Evidence Act 1872, s 65B.
[2]Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.
[3]State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600.
[4]Indian Evidence Act 1872, s 63, 65.

Introduction

In the late 1990s, India's information technology sector grew at a breakneck rate. The exponential development of a digital means of communication has presented new legal challenges to Indian courts and policymakers, especially in the area of electronic proof admissibility. The growing use of electronic media, e-commerce, and automated data storage has necessitated changes to the legislation governing information technology and the laws governing the admissibility of electronic evidence in courts. This expanded use of technology, on the other hand, presents difficulties in accommodating and representing modern age trends in laws across jurisdictions, which has fuelled the appreciation of digital data.

The material preserved or registered on paper was the subject of traditional photographic evidence evidentiary standards. The widespread use of information processing, on the other hand, has transformed the way we process and archive data. Several civil and criminal courts have relied on this evidence as a credible foundation. With the degree to which information technology has infiltrated our transactions, a regulatory system that prevents a significant amount of data from being admitted as evidence would have a negative impact on the litigation process. Around the same time, questions about the technology's possibility of manipulation must be addressed because, unlike paper documents, which have a tangible corporeal existence, electronic records are simply a set of digits and are rarely manifested in a physical manner. To keep up with the times, the Information Technology Act of 2000 was enacted, along with necessary revisions to the Indian Penal Code, 1860, the Banker's Book Evidence Act, 1891, and the Indian Evidence Act, 1872, thatincorporated modern IT into the legal framework.

Indian courts have established case law on the use of electronic proof as a result of the reform of law. Judges have also shown an understanding of the electronic value of testimony, with insight into its admissibility. Although the evidentiality of electronic records before a court of law isn’t new in Indian courts, the protections used to allow the processing of records have evolved significantly over time, particularly as the storing and usage of electronic content has grown, become more nuanced, and more vulnerable to coercion. Balancing these two issues is at the core of every regulatory system for electronic data admissibility– (i)ensuring a

considerable volume of material is not entirely omitted from the court's consideration, and (ii) ensuring that electronic procedures can be manipulated.

Background

The universal law of proof is that clear oral evidence, with the exception of records, can be used to prove any facts. It seems to imply that any oral testimony that isn't direct can't be trusted because it falls under one of the exceptions specified in the Evidence Act's sections 59 and 60, which deal with the hearsay clause. In the case of letters, though, the hearsay rule is not as rigid or as clear as it is in the case of oral testimony. As it is well established that oral testimony cannot validate the contents of a text, and the document speaks for itself, this is the case. As a result, in the absence of a record, oral testimony cannot be provided as to the document's authenticity or compared to the document's contents.

While the text itself is primary evidence, it has been recognized that there might be times when the same can't be readily accessible. Therefore, for the purposes of demonstrating the contents of an evidence, supplementary testimony in the authentic electronic copy of the evidence, those produced through physical methods, and oral versionsfrom someone who might have witnessed the event are admittedas per clause 63. As a result, the clause for accepting secondary testimony dilutes the hearsay rules in an effort to reunite the complexities and ensure that the reproduction of facts keeps the originality of the event intact. Clause 65A of the Act specifies that the original copy may not be required to be reproduced before the court in case when the same may not be very practical. Authentic copies of original evidence are dealt with in section 63. It covers cases in which the original text may be (a) under hostile possessions; (b) or have been proven as compromised; (c) is missing; (d) might not be portable so as to transport it physically; (e) is a state-owned public document; (f) may be confirmed by authenticated copies where the statute strictly permits, and; (j) is a compilation of many documents. With the digitization of records, the hearsay law was subjected to new threats. With the growing conversion of records into digital form, testimony was now more or less stored in digital form, implying a higher proclivity for adducing evidence in electronic form.

Prior to 2000, electronic evidence was treated on par with conventional evidence. These were reproduced into physical formats such as in print or optical disk form for compliance under clause 63. Since the legislation was drafted about a

century prior to the time we're talking about, it was obvious that the same had failed to keep pace with the changing technology. Furthermore, reproducing electronic evidence in printed format produced some of its own challenges such as the meta data, even when available, was not reproduced along with the content of the evidence. Such admissions were not subject to latter conditions of section 65B(2) introduced in the 2002 amendment and were thus susceptible to be abused. It was thus now the time to revise evidence laws and the criteria for admission of electronic evidence. The creation and storing of electronic records became more complex with advancement in technology and thus proved to be more difficult to be incorporated into the legal framework of India.

Indian Evidence (Amendment) Act, 2002

The Evidence Act has been updated many times over the years, most recently to enable electronic archives to be used as evidence alongside paper papers in Indian courts. The status of electronic archives as documentation for the purposes of adducing testimony is one of the most important amendments. Section 22A was added to allow for the relevance of oral version of the event, and criteria for their admissibility was amended to incorporate any argument, whether spoken or written, that implies any reference to the event under scrutiny. Oral version about the content of the evidence are not valid until the originality of the same is established. The incorporation of section 65A and section 65B along the enactment of the Information Technology Act, 2002, allows for a separate method to admit evidence in electronic form, which is also perhaps the most significant revisions to the Act. Section 65B states that any information stored in a digital form, whether it be the content or the meta-data, is to be admitted as proof without being subject to other clauses under sections 63 and 65 of the Act.

Section 65B requires that the reproduced data contains the original and authentic information as it was originally created/stored in the computer. One of the conditions is that the computer must have been in regular use by the lawful authority and functioned properly. Second, the type of information stored in the electronic database was constantly fed into the machine in the normal course of business during the time. The third critical criterion is that the machine must have been operational for the majority of the year, or if not, it must have been out of commission for a period of time, but not

long enough to impair the electronic record or the integrity of the contents. Finally, the material on the electronic record must be a copy of the actual electronic record.In order to get a piece of electronic evidence admitted before a court of law, section 65B(4) makes it mandatory to obtain a certificate issued by the lawful owner of the computer that stored the information in order to validate the copy of the evidence as an authentic copy of the original file saved on the computer. The certificate must uniquely classify the original electronic document, explain how it was made, describe the specifics of the system that created it, and verify that it complies with the provisions of section 65B sub-section (2). Section 65A states that the contents of digital archives can be proven in compliance with section 65B's provisions and conditions.

Admissibility of Electronic Evidence &Jurisdictional Developments

Prior the 2000 Amendment

Computers and digital archives were clearly well off in the future when the Indian Evidence Act was written in 1872. As a result, the Act relied solely on the standard definition of photographic evidence, namely, paper documents. Since electronic documents were being more widely used, the standard system built on the presumption of physical records was no longer adequate. Computer-stored content had already made its way into Indian courts even prior to the time when the Information Technology Act of 2000 made any changes to the Evidence Act. And before these changes to the Evidence Act were enacted, most electronic documents were already being admitted in court.[5] The courts, however, muddled the application of the conventional system of proof law in order to test the authenticity of such evidence.[6] Many questions concerning the authenticity of electronic data were much more ambiguous as a result of this. As a result, it became necessary to resolve these issues by regulatory intervention. Recognizing this need that existed in a number of countries, the United Nations Commission on International Trade Law (UNCITRAL) set out a model legislation on the admissibility of electronic documents.[7] The UNCITRAL

[5]Yusufalli Esmail Nagree v State of Maharashtra, AIR 1968 SC 147;Ziyauddin Buhanuddin Bukhari v Brijmohan Ramdas Mehta, AIR 1975 SC 1788; RK Malkani v State of Maharashtra, AIR 1973 SC 157.

[6] In N Sri Rama Reddy v VV Giri, AIR 1971 SC 1162, the court ruled implying the call intercepts as "primary and direct evidence of what has been said in the recording". In *Pratap Singh v State of Punjab*, AIR 1964 SC 72, the court had issued some basic guidelines regarding the admissibility of digital records. Thus, courts used several provisions to admit e-evidence in the absence of specific legislative provisions.

[7]UNGA Res 51/162 (16 December 1996), UNCITRAL Model Law on Electronic Commerce. Last accessed on 10 May 2021 from

Model's lynchpin evidentiary theory is that a data message should not be treated differently from other messages for the purposes of admissibility of evidence.[8] The very fact that information in preserved in the digital format does not preclude it from having legal effect. It would, however, also have to meet the criteria as per section 65B(2) to be admitted before a court of law as evidence.[9]

The UNCITRAL values were widely adopted in India in 2000, thanks to a revision to the Indian Evidence Act of 1872. Electronic evidence was recognized as a form of photographic evidence under the Amendment Act.[10] Around the same time, it established mandatory requirements imposed upon digital evidence to comply with clauses under 65B for their admission before a court of law, which included protection against the high likelihood of digital evidence being tampered or manipulated.[11] Section 65B of Act was added as part of a push for legal amendments, with the aim of attracting e-commerce businesses through technologically adept legislation. Since the Evidence Act applied to both civil as well as criminal trials, the sense in which the amendment was passed is also important. As a result, the admissibility framework that was enacted with the advent of e-commerce still extends to other cases, including criminal trials.

Early 2000s: Continued Denial of the Nature of E-evidence

Section 65B nearly exactly mirrored section 5 of the United Kingdom's Civil Evidence Act of 1968. Since section 5 of the Civil Evidence Act has now been revoked in late-1990s, only a couple of years before section 65B of the Indian Evidence Act was introduced in 2002, the imitation of provisions under section 5 of the CEA is clearly anachronistic.[12] The Supreme Court, apparently perplexed by rapid development in technology-based testimony, further muddled the provisions by issuing an analysis that was without any textual contemplation.[13]

Despite the fact that these requirements are obligatory, the legislation has been interpreted inconsistently. In court cases, the certificate of authentication, for

www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.
[8]Ibid art 9.
[9]Ibid art 5.
[10]Digital evidence were found in the definition of documentary evidence. Indian Evidence Act 1872, s 3(2).
[11]Indian Evidence Act 1872, s 65A, s 65B.

[12]The clauses defer in terms of the type of digital record which is covered. Although the scope of the CEA was “a statement contained in a document produced by a computer”, the scope of section 65B of the Indian Evidence Act is “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”.
[13] The legislation was replaced with the Civil Evidence Act, 1995.

example, is not necessarily filed with the electronic archives. The Supreme Court, for example, held in *State (NCT of Delhi) v. Navjot Sandhu*[14] that the courtwas allowed to accept digital documents in the form of printed papers or optical drives on prima facie basis, i.e. with no due process to ensure their validation and veracity. The evidence and admissibility of cell phone call logs was the subject of this lawsuit. Someonecould claim that the authorized person refused to issue the required certificate under65B(4) and that the protocol laid down under 65B had not been followed, so no emphasis could be put on the cell telephone data. The SC later decided that a cross-examination with an authorized personnel familiar with computers and technology in which the printouts/optical versions could be obtained as needed to establish the veracity of the evidence. Consequently, when the physical copies were presented as proof, they were admitted as duplicate copies of the original evidence rather than as originals.

This pattern of disregarding the special protocol for introducing documents as facts was continued in subsequent proceedings. For example, in *Ratan Tata v. Union of India*[15], an optical disk drive that contained intercepted phone callswere presented in the Supreme Court without observing the protocol set out in section 65B of the Evidence Act. Unfortunately, with a few cases, the lower judiciary is mostly technologically unreliable, and may not understand the authenticity problems or have protections when enabling the entry of electronic proof. The Supreme Court's judgments set a new precedent requiring lower courts to recognize the importance of the special process for electronic proof. The above-mentioned rulings overlooked the fact that the legislature established a special system for using electronic documents as testimony in court specifically because paper versions of the electronic records would be open to fraud and violence. Because the Proof Act makes all types of device outputs admissible as evidence, the courts have ignored and misunderstood the inherent existence of electronic evidence, putting recorded information at risk of misuse. In this regard, the Indian courts have not taken up mason's debate on the subject. As a result, for a long time, courts had not raised concerns about the accuracy of digital data or required the involvement of competent authority to ascertain the authentication of the document, and digital

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

[15]Rata Tata v Union of India & Ors (2011) WP (C) No. 16.

documents filed before courts were assumed to be accurate without being subjects to proper checks and balances.

Anvar P.V. v. P.K. Basheer: A Paradigm Shift

With greater attention to electronic information over time, there has been a shift away from dealing with digital documents as conventional ones. However, it took almost a decade for the Supreme Court to rule definitively that photographic testimony in the form of an electronic archive can only be proven by the protocol outlined under 65B. The apex court, in *Anvar P.V. v P.K. Basheer & Ors.*[16], overturned the judgement in *State (NCT of Delhi) v. Navjot Sandhu* and reinterpreted the implementation of clauses 63, 65, and 65B of the legislation.[17]

In *Anvar P.V. v. P.K. Basheer*, the appellant, Mr. P.K. Anwar, had lost a previous Assembly election and filed an appeal claiming that the incumbent MLA had harmedthe appellant'sreputation and engaged in activities damaging to his image, and that the defamatory material was captured in songs and on optical disk drives. The Supreme Court rejected the argument that courts should consider digital documents as prima facie proof without requiring them to be authenticated. It was decided that every electronic report must be followed by a certificate obtained in accordance with provisions under65B when the event was recorded, in the absence of which, secondary documentation relating to digital records is inadmissible. As a result, strict adherence to section 65B is required for anybody planning to depend on emails, blogs, or some other digital format in a civil or a criminal case. Since electronic records are more vulnerable of tampering and alteration, the Supreme Court has taken this stance to ensure that the authenticity and the integrity of digital proof is protected and ensured.

The Indian courts' progressive and methodical approach to ensuring that the protections for relying on digital information are followed is the product of a proper understanding and knowledge of the existence of electronic documents. It was a watershed moment for India's evidence-gathering methods, as it didn't only preserve time in trials by keeping parties from having to prove digital information by supplementary oral testimony in the form of cross questions, but it also prohibited the use of fudged or corrupted digital evidence.

Evidence Laws in the UK and the USA

[16]Anvar PV v PK Basheer (2014) 10 SCC 473.
[17]Indian Evidence Act 1872, s 63, 65, 65B.

It is important to understand the context in which the provisions under section 65B(2) were introduced. In the early 2000s, e-commerce were making their first mark in the country and that, sometimes, led to trials where the case dependent upon a piece evidence created/stored in the electronic form. Admitting e-evidence arbitrarily as courts did before the judgement in *Anvar v. Basheer*ignored the fact that electronic evidence could be tampered. Section 65B(2), on the other hand, could not contemplate a future of rampant cybercrimes where it may not be feasible for victims of cybercrimes to meet all conditions under section 65B(2). This section investigates laws, processes,and jurisdictional developments related to the admissibility of electronic evidence in the United Kingdom and the United States.

The Case for Special Conditions in the UK

The admissibility of digital records in the United Kingdom used to be based on the implementation of the customary best evidence rule and the hearsay rule prior to law action in 1968. There were also no clear exceptions to the hearsay and best proof rules to maintain the consistent admission of digital evidence. In 1968, Congress intervened in the context of section 5 of the Civil Evidence Act, that deals with the eligibility of computer-generated claims. But several problems with the provision's operation emerged, mostly due to technological difficulties. According to the Law Commission, these admissibility standards not only placed substantial restrictions on the use of electronic information as business evidence, but they were also ineffective in dealing with any of the issues that could occur in the field of electronic records.[18] As a result, it was proposed that no special rules be made for the method of evidence for computerized documents.[19] The Civil Evidence Act, which also omitted special provisions on electronic documents, provided legal guidance to those recommendations.

Similar amendments to the admissibility of electronic proof in criminal trials were enacted in 1997.[20] Despite the fact that the conditions under clause 69 of the Police and Criminal Evidence Act of1984 differed from those under clause 5 of the CEA, they both had special provisions for digital records.[21]Concerning the mandated requirements laid out under clause 69 of the PACE, the Law Commission noted that

[18]Law Commission, The Hearsay Rule in Civil Proceedings (Law Com No. 216, Cm 2321, 1993).
[19]Ibid [5.13] and [5.14].
[20]Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, Cm 3670, 1997).
[21]PACE Act 1984, s 69(1)(a), 69(1)(b).

the progress in digital devices, in regard to network infrastructures, has rendered it incredibly difficult to prove compliance with the inspection and qualification requirements and that the data output receiver is particularly "hard-pressed to demonstrate compliance under sec. 69".[22] The Justice and Criminal Evidence Act, which was enacted in response to these recommendations, recommended against the introduction of certain technology-specific conditions to the admissibility of electronic documents.[23]

Why the US has no Special Rules for Electronic Evidence?

The Federal Rules of Evidence of the United States extend the exact procedures to digital evidence as is for conventional ones.[24] Company reports are the most widely utilized hearsay exemption for the entry of digital evidence in the United States.[25] And if a piece of digital evidence meets the criteria for exemptions, it suffices to satisfy the hearsay portion of the testimony.[26] Validation is a different issue, and in *Lorraine v Market American Insurance Company*[27], the court explicitly stated this distinction when setting out a general basis for electronic record admissibility. The best evidence rule comprises of (i) reliability, (ii) hearsay, and (iii) the best evidence rule. The use of a traditional system, on the other hand, can often lower the threshold for the admission the digital record.

In *State v Armstead*[28], the judgement had noted a difference between machine-produced evidence and human statements. They found, since the system was impartial and captured the event in its entirety, a robot imprint of telecommunications tracks was computer-generated proof and was thus admissible without a hesitation. For an argument to be found hearsay, the court considered it necessary that it be made by a human being.[29] Many computer-generated records are also excluded from the hearsay procedure of admission as a result of this decision. Then the other two standards of admissibility, namely validity and the strongest proof clause, must be met. As a

[22]Law Commission para 13.6.
[23]Justice and Criminal Evidence Act 1999, s 60.
[24] See Orin S Kerr, 'Computer Records and the Federal Rules of Evidence' (2001). Retrieved from http://euro.ecom.cmu.edu/program/law/08-732/evidence/kerrcomputerrecords.pdf. Last accessed 11 May 2021.
[25] "Comment: Evidence – Admissibility of Computer Business Records as Exceptions to the Hearsay Rule" (1970) 48 North Carolina L R 687; Federal Rules of Evidence, r 803(6).
[26]Federal Rules of Evidence, r 901; see 'Computer Data and Reliability: A Call for Authentication of Business Records under the Federal Rules of Evidence' (1986), 80 North Western Univ L R 956.
[27]Lorraine v Market American Insurance Company, 241 FRD 534 (D Md 2007).
[28]State v Armstead, 432 So 2d 837 (La 1983).
[29]Ibid.

result, the traditional system rendered admissibility of some types of electronic proof a little simpler.

The US system's experience suggests that, while time-consuming at times, traditional standards will more or less deal with the admissibility of electronic proof and that a special procedure is not needed. The advantages of this scheme are that, in addition to maintaining adequate inspections, it also ensures stability by not imposing strict mechanical criteria such as registration. The US system has preserved ample tolerance for emerging technology by not imposing any restrictive criteria particular to the admissibility of digital proof. Rather, because the criteria are broad and open-ended for courts to decide on for each individual case/evidence, there could be contradictory results.

The Canadian Framework of System Integrity

The Canadian paradigm relies on the quality and reliability of an electronic database scheme rather than on the veracity and soundness of a single digital evidence.[30] Through this method, the credibility of the device is used to conclude the record's trustworthiness.[31] In this case, clause 6 of the Uniform Electronic Evidence Act allows the bench to determine if a record-keeping method followed a certain "pattern, process, use, or tradition" when recording or maintaining electronic documents. Unlike the approaches used in India, the United Kingdom, and the United States, this approach focuses on whether the record is made by a credible method rather than whether it is a true copy.

Since the risk of fraud and deviation from market procedure occurs more often at the individual document level than at the system level, individual record-based assessment of continuity of validity is necessary in the case of paper documents. Manipulation of computer data, on the other hand, occurs at the machine level instead of at the level of a person's records. A scheme of presumption has been developed in the Canadian context to fulfil the integrity of the system test. The integrity of a systemcould be proved using any of the three presumptions mentioned in the Canadian framework.[32] The assumption of honesty of the digital file system is formed under the first assumption if the information is presented to the extent as long as the system functioned without any problems during

[30] Uniform Electronic Evidence Act 1997, s 4.
[31] See Luciana Duranti, Corinne Rogers and Anthony Sheppard, 'Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later' (2010), 70 Archivaria 95-124.
[32]Uniform Electronic Evidence Act 1997, s 5.

the applicable period, or that the failure to operate properly did not affect the credibility of the digital recording device.[33]

The credibility prerequisite is assumed in the second assumption, which occurs anytime electronic documents are collected or retained by an individual that is not bias to any one party in the trial.[34] Since the other person understands their own record-keeping method more efficientas comparedothers, the reason behind such presumption is that the other person has the potential to exhibit unreliability and refute the presumption. The third presumption applies to documents kept by a third party that is not a party to the case.[35] The trial method is made more effective by these assumptions. It also prohibits activities such as using proof against the individual who has the authority to certify the authentication of the evidence.

This assumption is that the other person has the potential to demonstrate unreliability of the system and possibility to refute the presumption. The third presumption applies to documents kept by a third party that is not a party to the case. The trial method is made more effective by these assumptions. It also prohibits activities such as using proof against the individual who has the authority to grant the certificate on the back of the certificate.

Conclusion

The decision to repeal sections 5 and 69 of the Civil Evidence Act and the Police and Criminal Evidence Act in the United Kingdom represents the fact that making a different collection of requirements regarding the admission of digital proof might not be necessary. The problem about exploitation vulnerability may be addressed by using general technology-neutral concepts, as is seen in the Canadian framework of system-integrity. It is important to note that opposing a different framework for digital proof is not the same as advocating for a reduced admissibility requirement. The goal is rather to make the criteria of admission flexible enough so as to not exclude a vast chunk of digital evidence, and at the same time, strict enough for the evidence to be non-bias and independent of the interest of parties involved.

The Canadian system-integrity approach is not only flexible to allow for the admission of electronic evidence when issuance of a certificate as required under Indian laws may not be possible, it also makes the trial process efficient by presuming the

[33]Ibid, s 5(a).
[34]Ibid, s 5(b).
[35]Ibid, s 5.

integrity of the system in certain cases, such as when it's under the possession of a neutral third party.

The court in the case of *State v. Navjot Sandhu*ruled that certification of the digital evidence, if not feasible, is not mandatory and the evidence could still be admitted before a court of law as evidence as long as it satisfies the criteria under sections 63 and 65.In *Anvar v. Basheer*, the Court ruled saying that digital proof had to be admitted exclusively based on the satisfaction of provisions under 65B of the Evidence Act 1872. As the pretext of the 2002 amendment was the advent of e-commerce, policymakers did not contemplate a surge in cybercrimes where it may be in the adverse interest of the computer owner to grant the certificate if the evidence is to be used against the owner.

As of today, the Indian Evidence Act leaves out on several critical questions regarding the admissibility of electronic evidence when the certification of the same involves a conflict between the party authorized to issue it and the other party. Although similar provisions for certification/issuance of an affidavit exist/existed in other countries, they are either not the only exclusive way for admission of an electronic record (Canada) or have since been repealed such as in the case of UK, South Africa, and the Australian state of South Australia.

The piecemeal legal answers to improvements brought on by the Indian IT revolution can in the long term do more damage than good, as the Indian digital proof evidentiary process shows.Since we are becoming rapidly growing our dependence on IT devices and environment, the truth of legal cases would be influenced by how these developments are incorporated into our legal systems. The way our justice processes deal with digital proof would undoubtedly have an effect on trials and other dispute resolution procedures.There requires a comprehensive overhaul and taking cues from developments in other jurisdictions, a new system should be brought about that is flexible enough to not exclude a considerable amount of electronic evidence from the consideration of the courts, and at the same time, is strict so as to ensure their authenticity. Whether or not such a system incorporates certification, it will definitely not be the exclusive way to admit a piece of electronic evidence.

Bibliography

1. Anvar P.V. v P.K. Basheer (2014) 10 SCC 473
2. Civil Evidence Act 1968 (UK).
3. Civil Evidence Act, 1995 (UK).

4. Computer Data and Reliability: A Call for Authentication of Business Records under the Federal Rules of Evidence' (1986), 80 North Western Univ L R 956.
5. Evidence Admissibility of Computer Business Records as Exceptions to the Hearsay Rule (1970) 48 North Carolina L R 687
6. Federal Rules of Evidence, r 803(6).
7. Federal Rules of Evidence, r 901
8. Indian Evidence Act 1872.
9. Justice and Criminal Evidence Act 1999, s 60.
10. Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, Cm 3670, 1997).
11. Law Commission, The Hearsay Rule in Civil Proceedings (Law Com No. 216, Cm 2321, 1993).
12. Lorraine v Market American Insurance Company, 241 FRD 534 (D Md 2007).
13. Luciana Duranti, Corinne Rogers and Anthony Sheppard, 'Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later' (2010), 70 Archivaria 95-124.
14. N Sri Rama Reddy v VV Giri, AIR 1971 SC 1162.
15. Orin S Kerr, 'Computer Records and the Federal Rules of Evidence' (2001). Retrieved from http://euro.ecom.cmu.edu/program/law/08-732/evidence/kerrcomputerrecords.pdf. Last accessed 11 May 2021.
16. PACE Act 1984, s 69(1)(a), 69(1)(b).
17. Pratap Singh v State of Punjab, AIR 1964 SC 72.
18. Rata Tata v Union of India & Ors (2011) WP (C) No. 16.
19. RK Malkani v State of Maharashtra, AIR 1973 SC 157.
20. State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.
21. State v Armstead, 432 So 2d 837 (La 1983).
22. UNGA Res 51/162 (16 December 1996), UNCITRAL Model Law on Electronic Commerce. Last accessed on 10 May 2021 from www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.
23. Uniform Electronic Evidence Act 1997 (Canada).
24. Yusufalli Esmail Nagree v State of Maharashtra, AIR 1968 SC 147.
25. Ziyauddin Buhanuddin Bukhari v Brijmohan Ramdas Mehta, AIR 1975 SC 1788.