'IS THIS EVEN ADMISSIBLE'? A COMPARATIVE ANALYSIS OF THE LEGAL SYSTEMS OF INDIA AND USA ON THE ADMISSIBILITY OF ELECTRONIC EVIDENCE

SAMRIDHI KAPOOR AND ADITI SHEKHAR

INTRODUCTION

It is undeniable that the evolution of technology has led to the generation of tremendous amounts of electronic data in our daily lives. From the era of floppy disks and CDs to phones and smartwatches, a technological revolution can be witnessed in the past few decades.The advancement of technology has contributed to a more digitalized world and accorded significance to the field of e-commerce, a relatively newer field vis-a-vis traditional business. Electronic devices can incorporate crucial data and be used as electronic evidence to facilitatecivil and criminal matters. With the evolution of this fast-pacing technology, there is a pressing need to bring about substantial changes in legal systems where the traditional rules are primarily based on documentary evidence.Given that the nature of electronic evidence is different compared to its counterpart, it can be irrefragably inferred that the regulations pertaining to admissibility, weightage, and relevance ought to be different. Several legal systems like India and USA are still unveiling laws on electronic evidence and lackfocus on its implementation to the fullest. However, there has been a substantial improvement from the last century due to the surge in precedents and legal statutes based on electronic evidence. The aim of this paper is not to highlight the importance of electronic evidence but instead focus on the laws related to them. It seeks to make a comparative analysis by drawing a contrast between the laws of India and USA on electronic evidence by addressing elements such as admissibility and reliability using statutes, precedents, and other secondary sources. Lastly, the authors aim to suggest possible solutions to address the discrepancies in the legal systems of both countries on this particular subject matter.

INDIAN LAW ON ELECTRONIC EVIDENCE; IT Act 2000 and Indian Evidence Act 1872

"*In our technological age, nothing more primitive can be conceived of than denying discoveries, and nothing cruder can retard forensic efficiency than swearing by traditional oral evidence only thereby discouraging the liberal use of scientific aids to prove guilt.*"[1]

The term 'Electronic evidence' was introduced primarily because of three statutes; the Information Technology Act 2000 ("IT Act"), Indian Evidence Act 1872 ("IEA"),and Indian Penal Code of 1860. This paper seeks to analyze Indian law by mainly focusing on the first two statutes. The IT Act is essentially construed upon the 'United Nations Commission on International Trade Law Model Law' on Electronic Commerce.It refers to the same data, record, or image under Section 2(1)(t) of the Act.[2]

A literal interpretation of Section 3 of the IEA of 'evidence' is now inclusive of oral,documentary,and digital evidence produced in legal proceedings. Section 3, which earlier stated, "*All documents produced for the inspection of the Court"*has now been modified to "*All documents, including electronic records for the inspection of the Court*" by Section 92 of the IT Act. This documentary hearsay rulehas also been altered to include electronic records as well, bythe introduction of two additional evidentiary provisions in the Evidence Act,for the admissibility of electronic data, which are section 65A and section 65B.[3]

Moreover, barring Section 3, Section 61 to 65 of the IEA, the 'document or its contents' are not replaced by electronic evidence (s). There is a specific omission of "Electronic records" in light of Section 61 to 65, which expresses the coherent and clearintent of the Parliament to not encompass the applicability of these sections with respect to the overriding provision of Section 65B.[4] The phrase, 'Notwithstanding anything contained in this Act' can be referred to as a non-obstante clause which reinforces that the Parliament had envisioned the specialprocedure for the admissibility of electronic data under these two sections.[5] Despite what is mentioned in these non- obstante provisions, these clauses following it will be fully operational and shall not obstruct the implementation of these non-obstante clauses.[6]

[1]Som Prakash v State of Delhi AIR 1974 Cri. LJ 784 MANU/SC/0213/1974
[2]Vivek Dubey, *Admissibility of Electronic Evidence: An Indian Perspective* 4 FRACIJ 58, 58-63(2017)
[3]*Id.*
[4]*Id.*
[5]*Supra note 2*
[6]Chandavarkar Sita Ratna Rao v Ashalata S. Guram (1986) 3SCR866

AN ANALYTICAL EXAMINATION OF SECTION 65A AND 65B VIS-À-VIS SECTION 61 TO 65 OF THE INDIAN EVIDENCE ACT

The main aim to create a special provision is to exclusively dealwith the admissibility of the electronic record, owing to the technical nature of electronic evidence,which should be admitted in a specific manner. Similar to the functions of Section 61 for documentary evidence, the underlying difference is that Section 65A and 65B tend to create a special procedure for the electronic record, in addition to the oral and documentary evidence, which obeys the hearsay rule. Apart from this, it manages to cover the legitimacy and sanctity of the retrieved electronic evidence, which makes it stand out from the provisions on documentary evidence. This principle was reiterated in State v. Mohammed Afzad where "Computer-generated electronic records shall be considered to be admissible if it can beproved inthe light of Section 65B of the IEA".[7]Thereby, it similarly allows the admissibility of secondary copy comprising of a duplicate copy or electronic data, in general.

Deriving its principle from *lex specialis derogat legi generali*, the Court in Anvar v Basheer, the landmark judgement held that Section 65B was a special provision, inserted through an amendment by the IT Act and will thus, prevail the general law regarding its counterpart; documentary evidence.[8] The fundamental framework for the admissibility of the electronic evidence in India was laid out in this case in this landmark judgement. "A revolution can be witnessed by the manner in which evidence is now produced in a trial, civil or criminal. Prior to 2000, it is a known fact that electronic data was treated under the ambit of a document itself, and secondary evidence of these electronic 'documents' was presented through 'printed reproductions,' the authenticity of which is essentially certified by a signatory of competence. This entire procedure is straightforward and fulfills the requirements mandated by sections 63 and 65 of the IEA."[9]

[7]State v Mohd. Afzal and Ors [MANU/DE/1026/2003]
[8]*Id.*
[9]Anvar P.V. v P.K. Basheer AIR 2015 SC 180 [MANU/SC/0834/2014}

Section 65B (2) lists out the circumstances upon which the replica of the original electronic record can be used[10] for the sake of convenience.[11]It lists the necessary technological conditions for the abovementioned objective:

i. The information was construed by a computer used regularly to store, process,or extract information by the person having lawful authority over it.
ii. Information contained in the electronic record must have been regularly fed into the computer in the ordinary course of the said activities.
iii. The computer was functioning properly throughout the material part of the said period.
iv. The duplicated copy should be a derivation of the original electronic record.

Section 65B (3) elaborates explicitly upon what constitutes as a single computer. Considering technological advancement, a single computer may also involve a combination of computers functioningcollectively over a particular period or any other manner involvingsuccessive operation over that period.[12]Section 65B (4) additionally lists out non-technical and legitimate criteria to establish the integrity of digital evidence. If the certificate comprises of the unique identification of the original record, a statement about the means of its production describing particular details about the device and is signed by the person (in their official capacity)with respect to the functioning of the device-in-question then the certificate shall bedeemed to be adequate for the matter to be stated to the best of the knowledge by the citizen who is in management of "relevant activities."[13]It is crucial to discuss the provisionto ensure that the admissibility of electronic evidence must comply and cumulatively satisfy the criteria under Section 65B (2) of the IEA.

THE LATENT YET UNHEEDED AMENDMENTS OF ELECTRONIC EVIDENCE

A strict implementation of the verdict in Anvar's case could be distinctly noticed in Sanjaysinh v Dattatray Phalke.Regarding the admissibility of a transcription of a recorded conversation,it was held that there could be no authenticity for this translation without a proper source.[14] In another

[10]The Indian Evidence Act 1870, Section 65B
[11]*Id.*
[12]*Id.*
[13]Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors [Civil Appeal No. 20825 of 2017]
[14]Sanjaysinh Ramrao Chavan v Dattatray Gulabrao Phalke [MANU/SC/0040/2015]

ruling, Jagdeo Singh v The State dealt with the admissibility of an intercepted telephone call on a CD which was without the mandated certificate under 65B Evidence Act.[15]"The Evidence Act does not permit proof of an electronic record by oral evidence if requirements under Section 65B of the Evidence Act are not complied with, as the law now stands in India."[16]The Delhi High Court stated that this secondary electronic evidence is thus, disallowed and cannot be looked into for any purpose whatsoever.[17]However, we shall further see how only an insignificant number of proceedings have judiciously followed the guidelines mentioned in the landmark case.

The chief problem lies in the fact that this special procedure under section 65A and 65B for the admissibility of electronic evidence are barely used. The lower tier courts in India are immenselyincompetent and technologically backward. Though the above cases are perfect examples of the Indian judiciary following protocol,India's judicial system isdecrepit and poorly funded to advance technology.[18]Mostly, the trial judges have overlooked the new provisions and resorted to the conventional provisions on documentary evidence. In the NCT of Delhi v Navjot Sandhu, the Court held, "As per Section 23, secondary evidence means copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy. Section 65 enables the secondary evidence of the contents of a document to be specified if printouts taken from the computers and certified by a responsible officer can be led into evidence through a witness who can identify the signatures of the certifying officer or speak to the facts based on his personal knowledge".[19]The Trial Court bypassed the procedures concerning interception of telephone calls and wiretaps in several ways. Without the proper authority, the Supreme Court also interfered to verify the secondary evidence and did not compare the duplicate CDRs to the original record. It further accepted hearsay evidence, which is precisely the kind of circumstances, the special provision purports to avoid by virtue of Section 65B, which requires an unbiased certification under subsection 4.There have been several counterclaims where the special procedure has been largely ignored, Navjot Sandhu's case being an example. Parties have themselves disputed the authenticity and authorization of the printed transcriptions of CDRS.[20]

[15]Jagdeo Singh v The State and Ors. MANU/DE/0376/2015
[16]Lorraine v Markel American Insurance Company 241 FRD 534
[17]*Id.*
[18]*Supra note 2*
[19]State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600
[20]Amar Singh v Union of India (2011) 7 SCC 69

Blatant violation can be seen in Ratan Tata v Union of India[21]where a CD comprising of interceptedcalls was produced during the trial without ensuingthe method under Section 65B. Similarly, the prerequisite of a certificate has been held to be voluntary if the electronic evidence produced by the party is not in possession of this deviceand subsequently, the regular provisions can be invoked.[22]The special procedure was made voluntary by the Courts in the 'interest of justice'. In addition to this blasphemy, non-filing of the certificate was deemed not to be 'incurable irregularity' and could be 'simply'remediedlater during the trial as well.[23] The Orissa High Court hadstated that it is not a necessary requirement for the prosecution to fulfill all the given criterion when it came to the filing of the certificate under Section 65B of IEA before making a Voice Examination Report and transcript of the CD admissible[24]. The sole purpose of referring to several judgements is because it can easily be inferred that the Courts continue to use the conventional approach instead of following the specialized procedure laid out post amendment. These rulings are a reminder that there is a lack of enforceability of the new provisions, and consistency needs to be maintained. The paper in the latter half shall further analyze thisirregularity and elaborate on how judges end up using their discretion to decide the admissibility of electronic evidence on an individual basis.

THE ROAD AHEAD

Despite the new provisions, India has a pressing need to formulate a uniform mechanism for keeping a check on the veracity of electronic evidence. Appositeinstructions should be framed with respect to the provisions of the IT Act (using Section 67C), formulate guidelines on imprinting and implementing policies for the retention of data throughout the trialsin order to preserve this digital data to avoid malpractice or tampering. Another possible way to go about admissibility is by framing strict rules for safeguarding, repossession, and production of records after the Chief Justice's Conference of 2016. It is paramount for the Indian Courts to follow the guidelines laid out in Anvar's case, adopt a consistent approach, and implement safeguards to proof the law on the admissibility of electronic evidence fully.

US LAWS ON ELECTRONIC EVIDENCE; A glimpse into the Federal Rules of Evidence

[21]Ratan Tata v Union of India Writ Petition (Civil) 398 of 2010
[22]Shafhi Mohammad v The State of Himachal Pradesh (2018) 2 SCC 801
[23]Paras Jain v State of Rajasthan (2015) SCC OnLine 8331
[24]Pravata Kumar Tripathy v Union of India 2014 SCC OnLine 407

In the era of social media and smartphones, the bar for admissibility of electronic evidence should be set, keeping in mind the misuse of such technology for the fabrication of evidence as well as the overarching growth of technology itself. The reliance placed on the different evidence depends on a case-to-case basis. Federal Rules of Evidence[25] govern the laws around the admissibility of electronic evidence similarly as it deals with the documents. Though established at a federal level,these rules have been adopted by most of the different states in US as their backbone for the law of evidence. For any electronic evidence to be admissible under these rules, it must be authentic, relevant, should not be classified as hearsay, and depending on the type of evidence that is being produced, an original writing rule might be attached to it. Lorraine v Markel American Insurance Co.[26] has proved to be a landmark judgement discussing the subject matter of admissibility of electronically stored information and address the issues arising from it.Subsequently, it resolves the problem by referring to four fundamental conditions that must be addressed for the admissibility of electronic evidence. A combined analysis of the Federal Rules of Evidence with this landmark judgement provides the essential requirements that parties must follow for the permissibility of electronic evidence.

Lorraine v Markel establishes that to make evidence admissible, it must first be established that the evidence in question is relevant, as "relevancy is not an inherent characteristic of any item of evidence."[27] Federal Rules of Evidence 401and 402 have been ascertained as the primary rules used to analyze the relevancy of any evidence. Rule 401[28] states that any evidence would be considered relevant if it affects the probability of any fact in question. Rule 402[29] allows all relevant evidence (as per 401) to be admissible in court if not expressly forbidden by the statutes mentioned in the provision. Rule 403[30] also provides an essential requirement for relevant evidence that may not be admitted owing to prejudice or misleading the jury and other factors like wasting the time of the court etc.

[25]FED. R. EVID.
[26]*Lorraine* 241 F.R.D.
[27]*Id.*
[28]FED. R. EVID. 401.
[29]FED. R. EVID. 402.
[30]FED. R. EVID. 403.

The second condition to be examined is the 'authentication' of evidence examined under Federal Rule of Evidence 901[31]. This rule clearly states that authentic evidence would be identified when it is used to support a finding that the item in question is exactly what it seems to be. The rules also provide an elaborate list of different methods through which the evidence introduced can be authenticated. This highlights that the evidence being presented must exactly be what it seems to be. One of the most common examples supporting this would be under the 'witness with personal knowledge' where hypothetically speaking,'I wrote these emails' would be enough to authenticate the emails in question. However, the witness authenticating evidence under this rule must provide 'factual specificity'. In United States v Catabaran[32] and United States v Linn[33] it can be ascertained as two concrete examples of witnesses with personal knowledge. In both cases, electronic evidence in the form of computerized ledgers and computer records, respectively, were procured before the witnesses in their ordinary course of business. United States v Blackwell[34] would also be an example of the same because the location of the weapon-in-question was determined by a photograph of the same, which was consequently affirmed by the detective who searched the location itself. Expert opinion under Rule 901 (b)(3) can also be attained to prove the authenticity of the evidencein question. Authentication of evidence is decided "on a case-to-case basis upon standards that may vary from jurisdiction to jurisdiction and even from jurist to jurist"[35]. Rule 901(b)(4) highlights that evidence may be authenticated under this section highlighting the appearance or characteristics of the evidence in question. Many electronic forms of evidence like email and other records are often authenticated under this rule. In United States v Siddiqui[36], an email was authenticated through the circumstantial evidence provided in the email itself, which displayed the defendant's work address, nickname, and so on. Similarly, in Dickens v State[37]it was demonstrated that "a recipient or non-recipient with that communication was sent may authenticate"[38] such electronic evidence. At the same time, courts determine the probative value of each authentic evidence on a case-to-case basis.

[31]FED. R. EVID. 901.
[32]United States v Catabaran 836 F.2d 453 (9th Cir. 1988)
[33]United States v Linn 880 F.2d 209 (9th Cir. 1989)
[34]United States v Blackwell 694 F.2d 1325, 1330 (D.C. Cir. 1982)
[35]Sheldon M. Finkeltein & Evelyn R. Storch, *Admissibility of Electronically Stored Information: It's Still the Same Old Story,* 23 J. Am. Acad. Matrim. Law. 45, 47-48 (2010).
[36]United States v Siddiqui 235 F.3d 1318 (11th Cir. 2000)
[37]Dickens v State 927 A.2d 32 (Md. Ct. Spec. App. 2007)
[38] Jonathan D. Friedan & Leigh M. Murray, The Admissibility of Electronic Evidence Under Federal Rules of Evidence, 17 Rich. J. L.& Tech. 5, 19 (2011).

This landmark judgement has highlighted this need for greater examination of authenticity as this simple requirement is also not fulfilled very often under this rule. Thus, no fixed approach that can be taken to authenticate all the electronic evidence present.

The third hurdle that must be crossed for the relevant and authentic evidence to be admissible is for the evidence not to be classified as hearsay. Federal Rules of Evidence 801[39] and 802[40] examine the same, whereby conditions are laid out for any evidence to be construed as hearsay or not. Hearsay would constitute, "an expressly assertive written or spoken utterance or non-verbal conduct expressly intended to be an assertion"[41]. The question regarding electronic evidence that arises is whether electronic evidence could be used to give out statements. It is observed that many of the statements made by computers shall not constitute hearsay considered as the statement cannot be made by machine but a declarant.[42] The exceptions to hearsay are further mentioned in Federal Rules of Evidence 803[43]. These include many categories such as present sense impression, excited utterance, public records, etc. However, with respect to electronic evidence, one of the most prominent exceptions used is business records formulated as a regular conducted activity. Many business records are demonstrated to be in the ordinary cause of business to make them admissible as an exception to hearsay. However, Monotype Corp. v International Typeface Corporation[44] depicts how hearsay can be construed through an email sent that was not recognized to be in an ordinary course of business. State of New York v Microsoft[45] also further displays a similar example where emails sent by an employee were held to be non-admissible because there was no evidence as to whether the employer required such emails in the course of business. Thus, the crucial verdict in Lorainealso elaborates on the original writing rules depicted under Federal Rules of Evidence 1001-1008. This rule elucidates that in case of evidence presented in the form of a written statement, recording, or in the form of a photograph, the Court would require the party presenting such evidence to furbish an original or a duplicate original to prove the contents of such evidence. This rule is implied to include all

[39]FED. R. EVID. 801.
[40]FED. R. EVID. 802.
[41]*Lorraine* 241 F.R.D.
[42]Mark L. Krotoski, *Effectively Using Electronic Evidence Before and at Trial*,59 U. S. Attorney's Bulletin. 52, 63 (2011).
[43]FED. R. EVID. 803.
[44]Monotype Corp. v International Typeface Corporation43 F.3d 443, 450 (9th Cir. 1994).
[45]New York v Microsoft Corp. No. CIV A. 98-1233 (CKK), 2002 WL 649951 (D.D.C. Apr. 12, 2002).

evidence that is 'electronically stored or generated'. Federal Rules of Evidence 1004[46] display an exception to the best evidence rulewhere if the original evidence has been destroyed and not in bad faith, the witness may be allowed to testify as to what that evidence contained. Hypothetically, this can be displayed through an example, where a letter compiled on a laptop is destroyed because the house caught fire (herebydestroying the laptop). In such a case, the witness would not have an original, but he would still be allowed to testify as to the contents of the letter if he had read/written it.

"Application of the Federal Rules to electronic evidence is still, to some degree speculative."[47]With the evolution of the new forms of technology, there needs to be an evolution in the interpretation of judges of the federal rules for the admissibility of electronic evidence. However, there remains an issue of distrust concerning the internet and other types of electronic evidence. "What now seems to be a healthy skepticism towards email and internet may become a broader distrust on the part of courts."[48]The more technology is getting advanced, the more difficult it isto ascertain authenticity because an analysis is drawn out between the source of the evidence generated and its authenticity. The fabrication of electronic evidence hits right at the core of the probative value that should be assigned to it. Therefore, while ascertaining authenticity, it is imperative for the courts to examine the electronic evidence being introduced carefully. The issues arising with authentication of electronic evidence demonstrate that to make certain evidence admissible, the Courts should recognize the creative interpretations made to the law for this admissibility of evidence. Yet, at the same time, there must be an extensive and detailed examination by the Court owing to the very nature of electronic evidence, as it can be fabricated easily. Moreover, there should be more clarity as to the nature of hearsay that can be constituted as'electronic evidence'. "Comparison of electronic evidence with its most similar non-electronic analogue will enable a proponent to draw upon the court's familiarity with traditional evidentiary principles to provide comfort in the trustworthiness of electronic evidence."[49] Although such comparison seems like the way to opt for, there should be a broader discussion on the various types of electronic evidence that cannot be proved authentic or admissible. The law of evidence in the United States of America provides a clear path for any

[46] FED. R. EVID. 1004.
[47]Leah V. Romano, *VI. Electronic Evidence and the Federal Rules*, 38 Loy. L.A.L. Rev. 1745, 1801(2005).
[48]*Id.*
[49]*Supra note* 38 at 39.

lawyer to discern the admissibility of electronic evidence yet highlights the need for expansion of laws to include electronic evidence.

THE COMPARATIVE STUDY OF THE LEGAL SYSTEMS

A combined reading of the Indian Evidence Act and the IT Act provides the basic law regarding the admissibility and introduction of electronic evidence in a court of law. In the United States of America, Federal Rules of Evidence provide the same. To get digital evidence admitted in the court of law in US, a fixed procedure has to be followed by examining relevancy, authenticity, the rule of hearsay, and the best evidence rule. The Indian courts do not have a similar procedure for the same. Despite the procedure laid down, admissibility of digital evidence is examined on a case-to-case basis, and the judges must exercise their discretion while ascertaining the same. For the better functioning of the law discussing digital evidence, the Indian Courts need to employ the procedure laid down, while the US Courts need to provide clarity and specificity to the laws regarding electronic evidence.

While doing a comparative analysis, Anvar does for India what Lorraine did for US federal courts[50]. Though the law may be substantially different, a point of commonality would be that both countries must adopt an unwavering and absolute approach towards the admissibility of electronic evidence. "While Indian courts have developed case law regarding reliance on electronic evidence and have all the necessitated amendments to incorporate the provisions on the appreciation of digital evidence."[51], US is yet to develop a fully established law on electronic evidence apart from the Federal Rules of Evidence. The criterion for documentary evidence also applies to computer-generated evidence, unlike the IT Act of 2000, which primarily focuses on electronic devices. The Federal Rules of Evidence deal with authentication without quite distinguishing between computer-generated evidence and other forms of documentary evidence.[52] Thus, the rules for electronic evidence in USA are based on the mere extension of the rules for documentary evidence instead of formulating specific regulations on digital devices. With the fast-paced advancement of technology, the paucity of regulations based on electronic evidence and its strict implementation continue to exist.

[50] *Supra note* 2
[51] Shweta & Tauseef Ahmad, *Relevancy and Admissibility of Digital Evidence: A Comparative Study*, 2 IJLMH 1, 15 (2019)
[52] *Id.*

In addition, manipulation of electronic devices and their fabrication persist and have been overlooked by the Courts. This results inquestioning the very sanctity of electronic evidence before the Courts in the first place. This also leads to the fact that though it makes criminal prosecution easier like, in Ajmal Kasab's case where they built a strong case by merely producing transcripts of internet transactions. However, this could also take an opposite turn since it helps them prepare a defense simply by using highly advanced technology to produce primary evidence, in the form of electronic evidence, some of which may not even exist.[53] Without addressing this major issue on authenticity, the Courts shall face a difficult time determining the veracity and, thus its admissibility in a case, whether it be USA or India.

CONCLUSION

Advancement in technology has demanded an evolution in the law dealing with aspects of it. Both India and the USA have formulated basic laws regarding the admissibility of electronic evidence to keep up with such an evolution. India has interpreted and analyzed the same under Section 65A and 65B of the Indian Evidence Act along with the IT Act. The US courts have interpreted the admissibility under Federal Rules of Evidence and expanded upon the traditional laws of admissibility. The law of evidence in America provides a higher threshold regarding admissibility and admittance of digital evidence. Yet, the Indian law regarding this has been established specifically for this reason, although it has not been used effectively. However, through an analysis of both the systems of law presented, a need for further evolution is clearly displayed. The analysis demonstrates the need for a uniform system in both countries regarding the admissibility of such evidence as going forward, it would be more than required. The issues regarding suspicion and fabrication of electronic evidence have gripped both the law systems, thereby displaying the need for a higher threshold for ascertaining its admissibility. There is a long way to go for both systems to inculcate the law regarding the admissibility of digital evidence fully.

[53] *Id.*