Christ University Law Journal
2021, Vol. 10, No.1, 73-96
ISSN 2278-4332 | https://doi.org/10.12728/culj.18.4

The Dichotomy of the 65B Certificate: Analysing Trends with Regard to the Authentication of Electronic Evidence in India

Bhavyakirti Singh* and Aditya Bamb†

Abstract

It is a known fact as to how intricately interwoven electronic forms of communication and electronic media are in all aspects of life in the 21st century, including governance, crime and justice. This is widely recognised, and our reliance on technology is only bound to increase. Yet, development in legal literature does not occur synchronously. Where the pace of technology increases with time, legal developments that should ideally be concomitant, fall behind and often cause confusion, not only among the parties to the dispute in question, but also to lower Courts that seek to apply such principles in the future. One such nobly motivated legislative development is the 65B Certificate, the legal position with regard to which has seen multiple alternating views on the question of its mandatory nature with the latest developments delivered by the Supreme Court in the judgments of *Shafhi Muhammad* (2018) and *Arjun Khotkar* (2020). This paper discusses the changes that regulations dealing with the authentication of electronic evidence have undergone, post the introduction of the Section, analyses probable causes of the same and concludes with the contention that the current position of law may be inadequate.

* National Law University, Jodhpur, India; singh.bhavyakirti@gmail.com
† National Law University, Jodhpur, India; bambaditya@gmail.com

Keywords: Admissibility, Authenticity, E-Commerce, Indian Evidence Act, 1872, Information Technology Act, 2000

1. Introduction

This paper seeks to address the gap created by the progressive growth in technology and the struggle faced by the Courts while evaluating the credibility of evidence presented in complex forms, which may not be ordinarily interpreted. The first part of the paper elaborates upon the interpretation of electronic evidence as contemplated by the Information Technology Act, 2000 [IT Act, 2000] read with the Indian Evidence Act, 1872 [Evidence Act, 1872]. Subsequently, it analyses the circumstances which led to the introduction of Section 65B of the Act and its legal context. The paper then thoroughly examines the scope of the provision and the requisite procedure of authentication to obtain the certificate. It then engages in a case-law analysis relating to the admissibility of electronic evidence under Section 65B of the Act which reveals a conflict in position with regard to the requirement of a certificate. The paper then critically analyses the Supreme Court's judgments in the *Shafhi Muhammad* and *Arjun Khotkar* cases.[1] Finally, the paper recommends certain changes to the existing position of law with respect to the admissibility of electronic evidence in consonance with changes in technology, as well as with the practicalities of the Indian Courtroom.

2. Electronic Evidence in India

In principle, electronic evidence means "information of probative value that is stored or transmitted in binary form"[2] or "information

[1] Shafhi Muhammad v. State of Himachal Pradesh, AIR 2018 SC 714; Arjun Panditrao Khotkar v. Kailash Kushanrao & Ors. [Civil Appeal Nos. 20825-26 of 2017, decided on 14/07.2020].

[2] Scientific Working Groups on Digital Evidence and Imaging Technology, Best practices for digital evidence laboratory programs glossary; *See* Carrie Morgan Whitcomb, *An Historical Perspective of Digital Evidence: A Forensic Scientist's View*, 1(1) INTERNATIONAL JOURNAL OF DIGITAL EVIDENCE,

stored or transmitted in binary form that may be relied on in Court."[3] However, it must be noted that while such a general definition may be useful for educational purposes, it fails to clarify and pinpoint as to the exact constitution of electronic evidence. For the purposes of clarity and precision, the authors first discuss the interplay of provisions under the IT Act, 2000 and the Evidence Act, 1872.

Section 2(1)(t) of the IT Act, 2000 defines 'electronic record' as "data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche".[4] Further, Section 2(1)(r) of the IT Act, 2000 interprets 'electronic form' as any "information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device".[5] Simply put, an electronic record requires information to be stored, received or sent in an electronic form.[6] However, any electronic record cannot be admitted into a Court of law merely on the basis of its electronic form. Section 4 of the IT Act, 2000 provides legal recognition to such electronic record on the cumulative satisfaction of two conditions:

i. That it is rendered or made available in an electronic form, and,

ii. That it is accessible so as to be usable for a subsequent reference.[7]

---

https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[3] International Organization on Computer Evidence, G8; BUKHARD SCHAFER & STEPHEN MASON, THE CHARACTERISTICS OF ELECTRONIC EVIDENCE, in MASON S. & SENG D. (EDS.), ELECTRONIC EVIDENCE 18-35 (2017) [*hereinafter* "SCHAFER AND MASON"].

[4] § 2(1)(t), Information Technology Act, No. 21, Acts of Parliament, 2000 (India).

[5] § 2(1)(r), Information Technology Act, No. 21, Acts of Parliament, 2000 (India).

[6] Arvind M. Bhandarwar, *Electronic Record, Its Proof and Certificate under Section 65B of Indian Evidence Act* [*hereinafter* "Bhandarwar], http://mja.gov.in/Site/Upload/GR/%20ELectronic%20Record.pdf.

[7] § 4, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).

Consequently, the question arises as to whether on the satisfaction of these two conditions, the electronic evidence in question becomes relevant and a judge is duty-bound to appreciate it. As shall be observed later, the nature of electronic evidence is such that mere compliance with the two-fold test under Section 4 of the IT Act, 2000 does not make it relevant from an evidentiary perspective. The rules of relevance and admissibility are determined by the Act. Therefore, this brings us to Sections 65A and 65B of the Evidence Act, 1872, which aid in determining the relevance of electronic evidence in India.

3. Legislative History of Section 65B

In 1965, Gordon E. Moore, the Intel co-founder, made an interesting observation with regard to the growth of transistors on integrated circuits.[8] He asserted that technological growth is not linear but exponential.[9] He did not realize that this simple observation would turn into a law governing the growth of technology, economy and social change for more than half a century subsequently.[10] However, constant change is a consequence of exponential growth.[11] Therefore, due to the exponential growth in usage and development of technology, coupled with the advent of the internet, it becomes necessary to deal with the issue of electronic evidence and make changes to the legal regime that had existed prior to such changes. It is fairly obvious that for the drafters of the Evidence Act, 1872, the innovations of technology and computers, emails or communication through social media platforms were unfathomable. Therefore, the initial framework of the Act reflected a traditional approach to documentary evidence in the form of paper records.

---

[8] Gordon E. Moore, *Cramming More Components onto Integrated Circuit*s, http://www.monolithic3d.com/uploads/6/0/5/5/6055488/gordon_moore_1965_article.pdf.

[9] *Id.*

[10] Max Roser and Hannah Ritchie, *Technological Progress,* https://ourworldindata.org/technological-progress.

[11] DANIEL W. GRAHAM, HERACLITUS, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY, (Edward N. Zalta ed., Fall 2019 ed.), https://plato.stanford.edu/archives/fall2019/entries/heraclitus/.

However, this does not imply that after the proliferation of the computer and other technological equipments,[12] the functioning of the Courts came to a standstill with respect to matters concerning electronic evidence. On the contrary, in 1996, an amendment was made to the Companies Act, 1956,[13] which dealt with the admissibility of certain types of electronic evidence. Further, there are several instances where the Courts have admitted electronic evidence,[14] most popularly in the *RK Malkani* case.[15] In essence, the Courts treated electronic evidence as secondary evidence under Section 63 of the Evidence Act, 1872. It would be presented in the form of transcripts or a printed reproduction and certified by a competent signatory to verify authenticity.[16] Subsequently, the signatory would identify their signature in Court and could be cross-examined.[17] The entire process was drawn out and could be easily exploited due to the absence of sufficient safeguards for checking the authenticity of the digital evidence. Nevertheless, the Courts were obligated to apply the traditional framework to these cases which generated inconsistencies and uncertainty due to the analogous approach.[18] This brought about an increased reliance upon judicial discretion by the judges who were unsure as to the extent to which the traditional approach could cover such cases, thereby leading to

---

[12] *See,* World Without Borders: *E-mail and Cyberchat are Revolutionizing the Way We Live*, The Week, at 12 (1999).

[13] § 610 A, Companies Act, No. 18, Acts of Parliament, 2013 (India).

[14] Yusufalli Esmail Nagree v. State of Maharashtra, AIR 1968 SC 147; Yahoo! Inc v. Akash Arora, 78 (1999) DLT 285; Aradhya Sethia, *Rethinking Admissibility of Electronic Evidence,* 24(3) INT'L J. L. & INFO. TECH. 229 (2016) [*hereinafter* "Sethia"].

[15] RK Malkani v State of Maharashtra, AIR 1973 SC 15.

[16] Tejas Karia, Akhil Anand & Bahaar Dhawan, *The Supreme Court of India re-defines admissibility of electronic evidence in India*, 12 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE L. REV. 33-37. *See also,* Bhairav Acharya, *Anvar v. Basheer and the New (Old) Law of Electronic Evidence,* https://cis-india.org/internet-governance/blog/anvar-v-basheer-new-old-law-of-electronic-evidence.

[17] *Id.*

[18] SCHAFER & MASON, *supra* note 3.

contradictions and confusion. The fundamental rules governing the law of evidence appeared to be at risk.

These factors prompted the need for a change in the framework, which could adequately address contemporary needs in the form of electronic transactions. Thus, this translated into legislative action in the form of an amendment to the Evidence Act, 1872 by virtue of the IT Act, 2000 coming into force.[19] The amendment was based on the guidelines given by the United Nations Commission on International Trade Law [UNCITRAL], which recognized the growing complications that every nation faced with respect to the admissibility of digital evidence.[20] The amendment modified the interpretation clause, i.e., Section 3 of the Evidence Act, 1872, to include electronic evidence within the ambit of documentary evidence.[21] Further, it facilitated the introduction of Section 65A and Section 65B as special provisions to govern the admissibility of electronic evidence, the importance of which has not been overlooked by Courts in India.[22]

4. Section 65B: Scope and Certification

Trustworthiness is built on the foundation of two qualitative dimensions, namely, reliability and authenticity.[23] The authenticity of a digital document is a test checking whether the document is, in fact, what it claims to be.[24] A third parameter of integrity indicates

---

[19] Entry 9, Schedule II, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).

[20] UNCITRAL Model Law on Electronic Commerce, UNGA Res 51/162, 16 December, 1996, www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

[21] § 3(2), Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[22] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178; State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600; Mohd. Ajmal Mohammad Amir Kasab v. State of Maharashtra, (2012) 9 SCC 1.

[23] STEPHEN MASON AND ALLISON STANFIELD, AUTHENTICATING ELECTRONIC EVIDENCE 193–260 (2017) [*hereinafter* "MASON AND STANFIELD"].

[24] HEATHER MACNEIL, TRUSTING RECORDS: LEGAL, HISTORICAL AND DIPLOMATIC PERSPECTIVES (2000); LIVIA IACOVINO, RECORDKEEPING,

the soundness of the data in terms of its completeness and the extent of damage caused to it, if any.[25] Further, this test is a pre-condition to the goal of admissibility.[26] The differences between a physical document and a digital document confers a special status on the admissibility of electronic evidence as 'digital data is inherently malleable or mutable.'[27] This implies that it may be highly exposed to alteration, corruption, and/or damage which poses an appreciable risk to the admissibility of such data. Section 65B, along with Section 65A, was introduced as a safeguard to effectively counter the above-mentioned issues and to come to grips with the change in technology. The *raison d'être* of Section 65A seems to be to merely refer to Section 65B.[28] The scope of the Section extends to criminal as well as civil proceedings, thus displaying the need for extensive analysis to understand its implications in the Indian context.

Section 65B, through sub-Section (1), begins with a non-obstante clause,[29] implying that the provision is applicable, irrespective of a contrary provision within the Act and will have an overriding effect in case of a conflict.[30] It states that any information contained in an electronic record that is transferred to paper or generated through a computer output in the form of CDs, USBs, etc. shall be admissible in a Court of law if it satisfies the conditions stipulated by Section 65B as regards the information and the computer output. It can be observed that sub-Section (1) has two functions. Firstly, it operates

---

ETHICS AND LAW 41 (2006), as cited in MASON AND STANFIELD, *supra* note 23.

[25] MASON AND STANFIELD, *supra* note 23.

[26] Daniel K B Seng, *Computer output as evidence*, SING JLS 161–3; MASON AND STANFIELD, *supra* note 23.

[27] Steven W. Teppler, *Testable Reliability: A Modernized Approach to ESI Admissibility*, 12 AVE MARIA L. REV. 213, 217, https://avemarialaw-law-review.avemarialaw.edu/Content/articles/v12i2.Teppler.pdf.

[28] § 65A, Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[29] § 65B (1), Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[30] Great Western Rly. Co. v. Swindon & Cheltenham Extension Rly. Co., (1884) 9 AC 787, 808; Pannalal Bansilal Patil v. State of Andhra Pradesh, AIR 1996 SC 1023.

as a deeming provision which treats information contained in an electronic record as a document for the purpose of interpretation.[31] Secondly, it functions like an enabling provision creating an exception to the 'best evidence' rule,[32] thereby, allowing the admissibility of secondary documents even in the presence of original evidence.[33] As mentioned earlier, there are certain riders that must be satisfied in order to make the electronic evidence admissible under sub-section (1). Section 65B, through sub-section (2) explicitly lays down certain qualifications to ensure that the output is accurate and that computers are used lawfully, in accordance with the daily activities of business or otherwise.[34] The conditions are mandatory and must be read in conjunction to ensure the accuracy and reliability of data. However, we are yet to see whether these conditions do, in fact, guarantee the authenticity, reliability and integrity of the data. Further, it is pertinent to note that the sub-section does not explicitly prohibit the alteration of data, although it may be inferred from the purpose of the provision. Furthermore, Section 65B(2) must be read with Section 65B(3) which interprets the nature of computer used with respect to the number of computers used to process or store data.[35]

Section 65B(4) has been the most controversial when it comes to academic as well as legal discussions about the admissibility of electronic evidence. Section 65B(4) mandates the production of a certificate in order to provide a statement with respect to the electronic evidence.[36] The certificate may/shall contain information with respect to the (a) identification of electronic record and the manner in which it was produced. Further, information related to

---

[31] § 65B (1), Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[32] HALSBURY'S LAWS OF ENGLAND, VOLUME 17 138 (4th ed.); RATANLAL AND DHIRAJLAL, LAW OF EVIDENCE, (23rd Ed); Bank of India v. Ahbhoy Mohammed, 2008 SCC OnLine Bom 91; Ashwini Vaidialingam, *Authenticating Electronic Evidence: Sec. 65B, Indian Evidence Act* 1872, 8 NUJS L. REV. 43 (2015) [*hereinafter*, "Vaidiyalingam"].

[33] § 65B (1), Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[34] § 65B (2), Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[35] § 65B (3), Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[36] § 65B (4), Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

the (b) specifications or characteristics of the device used for the production of the electronic record to show that it was produced by a computer. Additionally, the above-mentioned information disclosed in the certificate should be (c) signed by a person in a 'responsible official position in relation to the operation of the relevant device or the management of the relevant activities' to the best of his knowledge or belief. It can be observed that Section 65B(4), via a certificate, operates as one of the ways to satisfy the conditions of Section 65B(2). However, the point of contention is with respect to whether a certificate is a mandatory requirement for the admissibility of electronic evidence. Further, there is debate as to the sufficiency or ability of a certificate to ensure reliability of data.[37] Additionally, the language of Section 65B(4) indicates that the conditions (a), (b), and (c) are mandatory and must be cumulatively satisfied in order for the certificate to be valid.[38] The requirement under (c) of sub-section (4) is unclear with respect to who can be a signatory and give a statement in relation to the certificate. The ambiguous wording of the Section has long confused the various stakeholders involved and has been the subject of fierce debate.

It could be said that Section 65B is archaic in nature due to its overwhelming resemblance to Section 5 of the Civil Evidence Act, which came into effect in the year 1968 in the United Kingdom.[39] In fact, the requirements under sub-section (2) of Section 65B are strikingly similar to Section 5(2) of the Civil Evidence Act, 1968. Further, the requirement of a certificate and the conditions stipulated under sub-section (4) mirror those given under the UK legislation. The perplexity of these observations is heightened when it is noted that the Civil Evidence Act had been repealed in the year 1995 which is five years prior to the induction of Section 65B into the Indian legal system. This paper advocates a purposive approach, acknowledging the context in which the provision was implemented as well as the objective that it seeks to attain.

---

[37] Sethia, *supra* note 14.

[38] On the contrary, *See* Jagdeo Singh v. State, MANU/DE/0376/2015, 2015 CRI L.J. 3976 S.C.; Anvar PV v PK Basheer, (2014) 10 SCC 473.

[39] Civil Evidence Act, Chapter 64, § 5, Acts of Parliament, (UK)(1872).PO

4.1 Process of Certification

Regardless of whether the requirement of a certificate is mandatory or not, it is important to determine the stage at which the certificate is to be produced or who is qualified to be a signatory. With respect to the author of the certificate, the third condition encapsulated under (c) of sub-Section (4) of Section 65B is relevant and lays down the onus on the party, for presenting the electronic evidence. According to the provision, as mentioned above, the signatory to the certificate must be 'occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities.' Additionally, the person must have adequate knowledge with respect to the functioning of the device.[40] The mandatory requirement of this provision can affect the interests of an innocent party, wherein the person occupying the responsible position refuses to be a signatory to the certificate, as the evidence might be detrimental to his interests. In such a situation, it becomes impossible for the party to produce a certificate. On the other hand, the provision was implemented with a view to prevent the alteration of data and ensure its accuracy, integrity and reliability.

Another important aspect of Section 65B is with respect to the time at which the certificate is to be obtained by the party seeking to admit the electronic evidence concerned. It must be noted that the entirety of Section 65B, including sub-section (4), does not, explicitly or implicitly, mention the time at which the certificate is to be obtained. The Supreme Court in the *Anvar case*¸ declared that the certificate is to be obtained at the time of producing the document.[41] Therefore, even valid and authentic electronic evidence produced prior to obtaining a certificate was held to be inadmissible. Nevertheless, the position of law with this respect is still unclear due to conflicting High Court judgments which came subsequent to *Anvar*.[42]

---

[40] Jagdeo Singh v. State, 2015 CRI L.J. 3976.

[41] Anvar PV v. PK Basheer, (2014) 10 SCC 473.

[42] Ankur Chawla v. Central Bureau of Investigation, MANU/DE/2923/2014; SK Saini v CBI, MANU/DE/2441/2015, Sethia, *supra* note 14, in favour of the position in *Anvar*. Kundan Singh v. State,

5. Section 65B and the Courts

The Supreme Court first discussed 65B certificates in a landmark judgment in the *Parliament Attack* or *Navjot Sandhu* case;[43] specifically in the context of call record printouts. The Court, with regard to the admissibility and reliability of such duplicate evidence, decreed that the non-filing of a 65B certificate would not lead to a conclusion of non-admissibility of secondary evidence. In such a situation, circumstances mentioned in other applicable provisions must be considered. Section 63 of the Indian Evidence Act, 1872 sets out 'Secondary Evidence' to mean and include copies of the original, through a mechanical process that ensures accuracy and Section 65 of the same enables such evidence to be adduced in the absence of the original. Further, with regard to the cross-examination of witnesses for this evidence, the Court relied on a House of Lords case,[44] to reject an argument for the production of a technical witness acquainted with the functioning of computers. It was held that:

> printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service providing Company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak about the facts based on his personal knowledge.[45]

Thus, the Court here allowed officials of the concerned companies to depose to the fact that the secondary evidence in the form of call record printouts was obtained from their computer records,[46] justifying the same by commenting on the 'fair' familiarity of the witnesses with the computer system and output. The Court placed an additional burden on the prosecution to call a technical expert

---

2015 SCC OnLine Del 13647, Paras Jain v. State of Rajasthan, MANU/RH/1150/2015, state a contrary position.

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

[44] R v. Shepard, 1993 AC 380 (U.K.).

[45] ¶ 15, State of NCT of Delhi v. Navjot Sandhu, (2005) 11 SCC 600.

[46] US, Rule 1001(3), U.S. Federal Rules of Evidence (1972).

directly in the know of things, in case a specific suggestion regarding, say, fabrication of the said evidence was brought up.

Navjot Sandhu was followed by *Anvar P.V. v. P.K. Basheer (Anvar)*,[47] which overruled the former. The Court in this case, has clearly stated that the Act has not permitted proof of an electronic or digital record through oral evidence and testimony if the requirements under Section 65B have not been complied with. The genuineness of the record would only come into question post compliance with and due production of the record as per 65B, for which one could resort to Section 45A, i.e., opinion of examiner of electronic evidence.

The Court also prescribes the provisions of the IT Act, 2000, Section 65A, Section 59 and Section 65A as a complete code in itself with regard to evidence relating to electronic records. Reversing the understanding of the same in *Navjot Sandhu*, the Court held that the general law as under Section 63 and 65 would have to yield to this special law, and thus have no application in cases of secondary evidence which are in the form of an electronic record. The same would be 'wholly governed' by Sections 65A and 65B. To summarise:

> An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.[48]

The Court has also drawn a distinction between the production of primary and secondary electronic evidence. Where primary evidence is adduced, for example, CDs that have been duly seized by the police or any other authorised agency, the same may be produced and played before the Court to verify the veracity. On the other hand, where they have been transferred from other instruments into a computer, thus going through multiple stages of

---

[47] Anvar PV v. PK Basheer, (2014) 10 SCC 473.

[48] ¶ 22, Anvar PV v. PK Basheer, (2014) 10 SCC 473.

transfer, and CDs have been made therefrom, they may not be produced in front of the Court without due certification. Though the principle here is appropriate, the Court may have used an inadequate or perhaps even inappropriate example to elucidate upon the same. Data storage records would only be primary evidence where the recording has been made on a device which directly stored the information, such as CD, hard drive etc. The Court concludes by reiterating that "if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act, 1872, the same is admissible in evidence, without compliance of the conditions in Section 65B of the Evidence Act, 1872."[49] Another instance where the Court does lightly misinterpret the provision is in its mention of conditions under Section 65B(4). Where the Section specifically mentions that 'any' of the conditions may be met, the judgment has overlooked the term and erringly presented the conditions as 'and' conditions. This is significant as the Court has gone on to further discuss that such safeguards have been taken to ensure that the two hallmarks of electronic evidence, i.e., source and authenticity remain intact and unperturbed. Yet, in the case *Sonu* v. *State of Haryana*,[50] the Court proceeded to avoid the application of decision of the court in *Anvar* by misinterpreting a contention with regard to the inadmissibility of electronic evidence in the absence of a 65B Certificate. The argument in itself was dismissed in view of the Court's application of procedural estoppel, stating that this objection should have been taken only at the trial stage and the same may not be contended at an appellate stage in view of the non-existence of a circumstance of inherent inadmissibility of said electronic evidence. In a situation to the contrary, non-objection at during trial would not lead to rejection of the contention at an appellate level. The Court relied on cases discussing irregularities in the mode of proof, concluding that the same may not be discussed during the final appeal hearings.[51] Thus, where the Court avoided the question of whether or not a 65B certificate is mandatory for admissibility of

[49] ¶ 24, Anvar PV v. PK Basheer, (2014) 10 SCC 473.
[50] Sonu Amar v. State of Haryana, MANU/SCOR/14605/2013.
[51] Gopal Das v. Sri Thakurji, AIR 1943 PC 83.

electronic evidence in Court, it allowed presentation of the same in this case against a procedural misstep on part of the appellants.

6. Shafhi Mohammad and Section 65B

One of the latest cases that falls into disrepute for a faulty interpretation of precedent, as well as a flawed application of principles under Section 65B is *Shafhi Muhammad v. State of Himachal Pradesh*.[52] While answering questions with regard to admissibility of videography of the scene of the crime or scene of recovery during investigation, the Court relaxed the mandate of certification as established by the Court in the case of *Anvar*.

Referring to multiple decisions of the Court,[53] it was concluded that the threshold of the admissibility of electronic evidence could not be ruled out on technicalities if the same is relevant, though the reliability may be subsequently determined on the basis of facts and circumstances. [54] In contrast, electronic and digital evidence would be admissible regardless of whether certification has been provided in cases where the person producing such evidence is not in a position to furnish the certificate owing to non-possession of the device. Sections 65A and 65B were held to be mere procedural additions provided as clarifications, thus starkly differing from the opinion of the Court in *Anvar* which had held these provisions to be a complete code on the subject.

This judgment may be appreciated for its implicit impact on the admissibility of illegally obtained evidence. The Court reasoned that it would be wrong to deny a party the benefits of accurate technology in cases where such evidence may be relevant on the grounds of non-production of the certificate. There may be situations where the electronic evidence is being provided by a person who is not in control of the said device and is thus not in a position to

---

[52] Shafhi Muhammad v. State of Himachal Pradesh, AIR 2018 SC 714.

[53] Ram Singh and Ors. v. Col. Ram Singh, 1985 (Supp.) SCC 611; Tukaram S. Dighole v. Manikrao Shivaji Kokate, (2010) 4 SCC 178; R v. Maqsud Ali (1965) 2 All ER 464 and R v. Robson, (1972) 2 All ER 699.

[54] ¶ 6, Shafhi Muhammad v. State of Himachal Pradesh, AIR 2018 SC 714.

produce such certificate owing to lack of fulfilment of conditions under Section 65B(4). To prevent such relevant material from being kept out of consideration, the evidence may be considered admissible by not completely excluding the application of Sections 63 and 65 in situations where a certificate cannot be secured. This interpretation resolves the problems with regard to admissibility of illegally obtained evidence in Court and brings it at par with non-electronic evidence, thus excluding the application of the *fruit of the poisonous tree* doctrine across all forms of evidence in the country as it ought to be.

But the Court further went on to expand the scope of Section 65B by stating that the requirement of the certificate is merely procedural and may be relaxed wherever interest of justice so requires,[55] exposing the process of the Court to possible abuse on account of instances of false and fabricated evidence.[56] As compared to physical evidence such as handwriting, it would be tougher in manifolds for a Court to check the veracity of electronic evidence. A certification would be helpful in attesting to the fact that the evidence is unaltered and unerring before it is admitted bearing in mind the various stages of transfer it undergoes before being presented before the Court in form of evidence. Furthermore, with all due respect, the Apex Court of the country, instead of clarifying the position of law ensuring certainty and uniformity, relied on the phrase 'wherever interest of justice so requires' casting a doubt on the applicability of Section 65B as a whole. The Court did not lay down any specific guidelines elucidating the situations in which a certificate could be done away with. The authors of this paper understand that each case is accompanied with a unique set of facts and circumstances, however, using an abstract phrase without stipulating specific guidelines does not seem like a practical solution. In effect, this shifts the duty of clarifying, whether a certificate is required or not, on the sub-ordinate courts without the presence of effective guidelines on the interpretation of Section 65B.

---

[55] ¶ 15, Shafhi Muhammad v. State of Himachal Pradesh, AIR 2018 SC 714.
[56] *See,* Jatinder Pal Singh v. Krishan Kishore Bajaj, MANU/PH/2422/2018.

7. Arjun Khotkar and Section 65B Today

The debate and confusion regarding the nuances of application of Section 65B prompted the Supreme Court to refer this question to a larger bench in view of the increasing dependence upon electronic evidence during investigations.[57] Herein, the Supreme Court explicitly reinstated the validity of *Anvar* findings, declaring *Shafhi* as *per incuriam*. The Court sought to secure a clear delineation between the provisions under Sections 65A and 65B, as opposed to the rest of Chapter V, which had been held to be inapplicable in concluding the admissibility of electronic evidence. The Bench emphasized upon the mandatory character of the certificate, which, though is unnecessary in case of the availability of the original document or device, is a pre-requisite for admissibility where one cannot produce the same. In rejecting the premise of *Shafhi* with regard to incapability of production where one is not in possession of a device, the Court clarified that a relevant application may be made before a Judge to direct production of the certificate or device from another concerned person, emerging from the general power of a magistrate to issue summons.

Additionally, the Court also made general directions to intermediaries, including cellular companies and internet service providers under Section 39 of the Evidence Act, 1872 and Section 67C of the IT Act, 2000, to retain relevant records for a certain period where associated Call Detail Records or devices are seized during investigation. Further recommendations were also made to frame rules under Section 67C for data retention by intermediary companies. While this may be appreciated as an obvious and correct identification of relevant provisions and case law by the Court, it once again falls short of clarifying uncertain nuances in the determination of admissibility that arose in cases such as *Sonu*, thereby opening to interpretation issues such as the non-application at the 'appropriate' stage and its implications on the trial process.

---

[57] Arjun Panditrao Khotkar v. Kailash Kushanrao & Ors. [Civil Appeal Nos. 20825-26 of 2017, decided on 14/07.2020].

Further, its direct and emphatic overruling of *Shafhi* also raises certain questions – would information stored on devices that are irretrievable, for instance, destroyed, lost or where the applicant is unaware of the location, be inadmissible? This would especially be the case where the lock-in period of the information with the intermediary has elapsed. What would be the consequences where the applicant can produce copies of the relevant document without certification in absence of the original device?

8. Looking Ahead

An implicit recognition of the lacuna in the *Arjun Khotkar* judgment is sufficiently clear through the recommendations for formation of rules with no judicial direction in the fashion of *Vishakha v. State of Rajasthan (Vishakha)*[58]. For instance, the judgment in *Visakha* contained specific and elaborate guidelines formulated for the prevention of sexual harassment of women in workplaces. In fact, it is viewed as a milestone in feminist jurisprudence which eventually to the enactment of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. However, while the Court in *Arjun Khotkar* recognized the need for judicial guidance, it failed to elaborate upon such guidelines which, in our view, are necessary for the purposive interpretation of Section 65B. Additionally, although there was a discussion on the modern trends in the treatment of electronic evidence in relation to foreign jurisdictions, the Court did not make any effort to apply or deliberate upon the impact of these observations specifically in the Indian context. In the interim, the authors of this paper have recommended certain changes to the existing position of law in consonance with the objective of the provision in addition to the context in which it was implemented.

It must be noted that the *Shafhi case* referred to the *Anvar* judgment and then stated a position of law that is contradictory and irreconcilable with the one stated in *Anvar* without overruling the same. Additionally, the promulgation of *Arjun Khotkar* law leads to an absurd result which is irrational and does not fall in line with the

[58] Vishaka & Ors.v.Stte of Rajasthan & Ors. (1997) 6 SCC 241.

aim of Section 65B. To summarize, in accordance with the position after *Shafhi*, the Courts can make an exception to the requirement of a certificate in any case which requires their intervention in the 'interest of justice'. However, in a case where the certificate is deemed to be required, the position in *Anvar* would have to be followed and therefore, a party would have to satisfy all requirements under Section 65B(4), where the certificate has to be obtained at the time of producing the document.[59] Further, Section 65B(4) becomes the only way to satisfy the requirements under Section 65B(2). The difference in the standard of admissibility in the two situations is of pertinence. On the one hand, if a certificate is not required, a party escapes the onerous requirements of Section 65B(4) and has a considerably lower threshold for admissibility. Conversely, if a certificate is required, a party faces the burdensome task of mandatorily complying with all the requirements under Section 65B(4) resulting in a much higher threshold for admissibility. This is even more baffling when it is noted that the emergence of this disparity would come down to judicial discretion. Naturally, a balance must be sought between the two situations without relying on vague exceptions which lead to the exacerbation of existing problems associated with the admissibility of electronic evidence.

Yet, the position after *Arjun Khotkar* is linear for situations discussed by the Court. Where the original device is produced, a certificate is not required. However, where the original device cannot be produced before the Court, a certificate must mandatorily be filed for the admissibility of relevant evidence at the earliest stage of trial, so as not to cause prejudice to the accused. In consequence, a post-dated certificate would not be valid. The inadequacy of the judgment to answer all necessary questions, as well as of the archaic Section 65B itself, so as not to leave uncertainties, has been recognised in a separate opinion by Ramasubramanian J., who draws parallels with the evolving jurisprudence in other common law countries, and encourages an approach cognisant of modern technology. Thus, the authors of this paper have made certain suggestions to modify the prevailing position of law to appropriately balance the disparities

[59] *Id.*

and absurdities created by the interpretation of existing case laws on the subject.

9. Reforming the law

Due to the increasing relevance of electronic evidence in the legal scenario and the rise of e-commerce, it is necessary to have a suitable provision addressing all the concerns mentioned above. There has to be a balance between the availability and admissibility of electronic evidence and its susceptibility to manipulation due to its inherently malleable nature.

Section 65B was introduced via an amendment to the IT Act, 2000, to deal with electronic evidence. The circumstances in which it was enacted in addition to the language of the Section which uses the phrase 'special provisions' can only indicate that the provisions were meant to be exhaustive and an exclusive application of the provisions was intended. An absence of a Statement of Object or policy discussions precludes a comprehensive analysis of the aim. However, the inherent and patent differences between electronic evidence and traditional evidence calls for differential treatment.[60] Therefore, the first recommendation is to treat Sections 65A, 65B read with Section 59 as a special code meant to exclusively deal with electronic evidence, which has, fortunately been accepted in *Arjun Khotkar*.

Due to the exponential growth of technology, it is clear that subordinate Courts, which handle majority of such matters in India, would not be equipped with the latest technology or the know-how required to deal with such matters. Therefore, Section 65B(4) mandated a certification process which made an enquiry as to the nature of the technology used and the manner in which it was produced. It addresses important questions relating to the integrity of the data as well as the consistency with which information was recorded by the system. The certificate is the least a party can obtain to produce electronic evidence which can warrant authenticity and reliability. Additional methods to prove authenticity may be

[60] ¶ 15, Anvar PV v. PK Basheer (2014) 10 SCC 473.

required in certain cases and will be discussed later. However, a certificate under Section 65B(4) must be mandatory for the production of electronic evidence because it provides a foundation on the basis of which the evidence can be evaluated. Further, it promotes certainty and uniformity without excessively relying on judicial discretion. Hence, the second recommendation is to make the certificate a mandatory requirement for the admissibility of electronic evidence under Section 65B.

In the *Shafhi case*, the Court recognized that there are situations when the requirements under sub-section (4) of Section 65B cannot be satisfied resulting in inadmissibility of electronic evidence due to lack of a certificate. This observation was nullified in *Arjun Khotkar*. Further, this paper recognizes the high threshold that is set by sub-section (4) in terms of the time at which it must be obtained, and the position of the person qualified to be the author of the certificate. In lieu of the above observations coupled with the earlier recommendation of making the certificate mandatory, a relaxation of the conditions set under sub-section (4) seems appropriate. Therefore, it is recommended that firstly, the contemporaneous certificate requirement mandating its production during evidence is not required and must be waived. Secondly, an exception must be created to the rule requiring mandatory certification to accommodate illegally obtained evidence. In situations where the person is not in operation of the device; an exception must be created. However, the ambit of this exception must not be wide enough to encourage false evidence.[61] Therefore, it should be restricted to accommodate illegally obtained evidence.

Further, even though the requirement of a 65B certificate as a rule may be justified, it would still not hold true or adequate as conclusive proof in every circumstance. With the advancement of technology and its multifaceted features, authentication through a certificate may fall short of the aim of its institution and inclusion

---

[61] *See,* Ayush Mishra, *The Conundrum of Certification of the Electronic Evidence,* BLOG OF THE CENTRE FOR CRIMINAL LAW STUDIES, NLU JODHPUR, https://criminallawstudiesnluj.wordpress.com/2019/09/10/the-conundrum-of-certification-of-the-electronic-evidence/#_ftn1.

within the rules of evidence. Apart from the obvious legislative introductions within the content of the certificate to make it more all-encompassing (e.g., addendums to ensure non-presentation of false and fabricated evidence, tampering with the evidence during the investigation process etc.),[62] it would also be fruitful to make provisions for the Court to be able to procure additional evidence. Authentication methods such as expert evidence should be encouraged. The Evidence Act, 1872 has provided for an Examiner of Electronic Evidence,[63] but frequent solicitation of opinion from independent authenticators and private experts may also be promoted so that evidence can be verified. A thorough corroboration of the evidence is also necessary as the general scepticism with regard to the use of digital evidence flows from the ease of the possibility of its manipulation. It would thus also be helpful if the certificate provided for something akin to an audit trail.[64]

The U.S. Federal Rules of Evidence also allowS for authentication through public records and metadata, apart from oral testimony which has also been provided in the Indian Evidence Act, 1872.[65] Comparison with other authenticated evidence, similar to the functioning of Section 73 can also be functional.[66] Even circumstantial evidence, which is one of the most frequently used rules of digital authentication, especially for social media authorship authentication in the US, may be taken into consideration. Detailed guidelines for the same may be developed on the basis of case law.[67]

---

[62] DAC Janet Williams QPM, *The U.K. ACPO (Association of Chief Police Officers) Good Practice Guide for Digital Evidence*, Version 5, ASSOCIATION OF CHIEF POLICE OFFICERS, (October, 2011), https://www.digital-detective.net/digital-forensics documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

[63] § 45A Indian Evidence Act, No. 1, Acts of Parliament, 1872 (India).

[64] ACPO Guidelines, *supra* note 59, § 2.1.3.

[65] Vaidialingam, *supra* note 32; Federal Rules of Evidence, Rules 901, 902 (U.S.)(2015).

[66] United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

[67] HON. PAUL W. GRIMM, GREGORY P. JOSEPH, ESQ., DANIEL J. CAPRA, BEST PRACTICES FOR AUTHENTICATING DIGITAL EVIDENCE 9 (2016) [*hereinafter* "GRIMM ET. AL."].

There may be an extensive amount of information that has not been elaborated upon adequately through the details mentioned on the certificate. In these cases, expert evidence and opinion that provides essential information may be more valuable before a Court. The general practice of relying upon provisions such as Sections 22A and 45A of the Act independent of the certificate would also be helpful while dealing with cases that fall within the exceptions Section 65B. This may also be beneficial in anticipation of better methods of authentication,[68] where oral testimony of experts can build upon the basic information provided through the certificate in cases where the certificate has been furnished.

In addition, it is also suggested that certain general standard exceptions to the rule of authentication of digital evidence, or self-authenticating digital documents be culled out.[69] Some obvious inclusions would be official government websites and documents uploaded thereon. Public documents filed on record have a certain presumptive value of genuineness, [70] and it would not be a far stretch to ascribe such presumptive value to, say, forms filled online or authenticated documents uploaded on official websites and presented before the Court as printouts or otherwise.[71] We may apply the same principle for other online resources such as official websites of newspapers, magazines, periodicals, other journals etc., businesses with certain financial or other records on websites, results of examinations (Universities or other Educational Institutions/All India Examinations), diagnostic centres or laboratories that make results available online etc. Since the information disseminated

---

[68] Vaidiyalingam, *supra* note 32, at 65.

[69] Federal Rules of Evidence, 2015, Rule 902 (U.S.); GRIMM ET. AL., *supra* note 64.

[70] *See*, Williams v. Long, 585 F. Supp. 2d 679; Arvind M. Bhandarwar, *Electronic Record, Its Proof and Certificate Under Section 65B of Indian Evidence Act*, http://mja.gov.in/Site/Upload/GR/%20ELectronic%20Record.pdf.

[71] Neeraj Aarora, *Every Computer Output does not Require a 65B Certificate – IEA, 1872,* CYBERPUNDIT BLOG, (Feb 28, 2017), https:// cyberpandit.org/?article_post=every-computer-output-does-not-require-65b-certificate-iea-1872.

therein flows mostly from the administrator of the said website, third-party tampering is less likely. In any case, self-authenticity is also bound to be a rebuttable presumption. This would also serve another purpose, i.e., to reduce the effort or cost that may have to be ascribed to authentication. Therefore, self-authentication offers a suitable solution to the onerous burden imposed by the certificate and is especially useful in the cases mentioned above.

10. Conclusion

In a world which is increasingly dependent on evolving forms of technology to facilitate communication, business, travel, etc. it is critical for the legal system to grow and adapt to the changes around. Further, the exponential growth of technology makes it progressively exigent to constantly reform the law and bring it in line with evolutionary technological innovations which could not be contemplated at the time of making the law. Therefore, in this technologically driven world, the rules governing electronic evidence assumes immense importance particularly due to the distinct nature of electronic evidence which makes it vulnerable to manipulation, alteration, damage, etcetera.

Section 65B, formulated on the basis of UNCITRAL guidelines, was introduced to the Evidence Act, 1872 to govern the admissibility of electronic evidence in India. Though ambiguously worded and astonishingly similar to the provisions of a repealed Act in the UK, i.e. the Civil Evidence Act, 1968, the purpose of the provision must not be ignored. A separate provision in the form of Section 65B was crafted predominantly to check the manipulation of electronic evidence and consequently determine its admissibility. In the absence of the satisfaction of conditions under sub-section (2) and the certificate requirement under sub-section (4) of Section 65B, there exists no uniform alternative method to check the authenticity of electronic evidence in India. The *Shafhi* interpretation of Section 65A and Section 65B as mere procedural provisions by the Supreme Court proved inconsistent with the purpose of these provisions. A more detailed and fruitful analysis of the chronology of admissibility, relevance and certification of electronic evidence in

consonance with Section 136 of the Act has been carried out in *Arjun Khotkar*, though it is not without its own shortcomings.

This paper sought to make certain recommendations to alleviate this uncertainty and strike a fair balance between accommodating electronic evidence within the Courtroom and excluding it due to its vulnerability to manipulation. The authors argued that the requirement of a certificate under Section 65B(4) must be the rule with specific exceptions created to accommodate illegally obtained evidence, self-authenticating evidence, etc. The procedural requirements under Section 65B ensure a minimum level of authenticity which could be corroborated with additional evidence to establish greater reliability if deemed necessary by the circumstances of the case. However, as things stand, in a developing country rapidly moving towards digitalization, an incomplete interpretation and an application of Section 65B replete with lacunae can lead to adverse consequences for the justice system in India.