AUTHENTICATING ELECTRONIC EVIDENCE: §65B, INDIAN EVIDENCE ACT, 1872

Ashwini Vaidialingam[*]

§§65A and 65B of the Evidence Act, 1872 were introduced in 2000 with the aim to lay down admissibility standards for electronic evidence in courts. However, this attempt at standardization has not seen much success and there has been significant divergence in practice in courts across India. Recently the Supreme Court in P.V. Anvar v. *P.K. Basheer attempted to address this problem by explaining and laying down the requirements under §65B.*

This paper argues that while the Supreme Court in Anvar may have been well-intended, it has misstated the position of law. First, the provision has been read in a manner that contravenes principles of statutory interpretation. Second, the Supreme Court has improperly restricted the possible methods of authentication to only 'certificates' under §65B(4). At the same time, there are problems with how §65B, as originally drafted, attempts to offset questions of accuracy and reliability. Accordingly, this paper, on an examination of practices followed by other common law countries, recommends the adoption of an entirely different model of authenticating electronic evidence.

I. INTRODUCTION

It is trite knowledge that world's transactions are increasingly electronic in nature. One inevitable outcome of this proliferation is that courts have been compelled to take cognizance of electronic evidence, from CCTV footage to emails, making their contributions are crucial. However, despite their evidentiary relevance, electronic records suffer from problems that their physical counterparts do not. Electronic data is easy to create, copy, alter, destroy, and transfer from one medium to another. In short, by their very nature, electronic records can be easily manipulated. Consequently, their accuracy and reliability is frequently suspect. This creates a conflict between the relevancy

[*] 5th year student, B.A., LL.B. (Hons.) National Law School of India University, Bangalore. I would like to express my sincere gratitude to Ms. Mannat Sabhikhi, Ms. Ritika Sinha, Ms. Deekshitha Ganesan and Mr. Abhinav Sekhri for their advice and encouragement

and admissibility of electronic evidence, something that has been recognized by jurisdictions across the world.[1]

In 2000, §65B was inserted into the Indian Evidence Act, 1872 ('Evidence Act') [2] in an attempt to modernize Indian evidentiary practices and help our courts deal with the advances in technology. The provision deems computer output such as printouts, CDs, data on hard disks etc. to be 'documents' under the Evidence Act, thus making them admissible in court.[3] It simultaneously seeks to ensure the reliability and accuracy of such evidence by demanding that certain conditions listed under §65B (2) be met.[4]

Despite the good intentions behind this amendment, the provision has been controversial.[5] This is primarily because High Courts in their treatment of electronic evidence under §65B have been inconsistent and arbitrary. Due to different courts demanding different methods for the fulfillment of the conditions laid down in §65B(2), there has been tremendous lack of uniformity. This variation in practice not only inconveniencies litigants, it also creates possibilities for the derailment of justice.

Recently, the Supreme Court sought to put to rest all these controversies in *Anvar P.V.* v. *P.K. Basheer* (*'Anvar'*).[6] To create uniformity in practice, the Court interpreted §65B as mandating one specific authentication method: a certificate as described under §65B(4) as a necessary precondition for admissibility of electronic evidence.[7] This paper seeks to examine the position of law on electronic evidence in light of this decision.

---

1 For example, South Africa, USA, Ireland, Singapore etc. *See generally* Murdoch Watney, *Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position*, 1 Int'l JL & IT. (2009); J.S. Givens, *The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards*, Cumberland Law Rev. 95 (2003-04); Law Reform Commission, Ireland, *Documentary and Electronic Evidence*, LRC CP 57 – 2009, 2009; Technology Law Development Group: Singapore University of Law, *Computer Output as Evidence*, September, 2003, available at https://www.agc.gov.sg/DATA/0/Docs/PublicationFiles/Sep_03_ComputerOutput.pdf (Last visited on February 8, 2016).

2 Information Technology Act, 2000, Schedule II, Entry 9.

3 *See generally* Indian Evidence Act, 1872, §65B.

4 *Id*.

5 *See* Apar Gupta, *How to rely upon an email in court*, December 14, 2011, available at http://www.iltb.net/2011/12/how-to-rely-upon-an-email-in-court/ (Last visited on January 20, 2016); Bhairav Acharya, *Anvar* v. *Basheer and the New (Old) Law of Electronic Evidence*, September 25, 2014, available at http://cis-india.org/internet-governance/blog/anvar-v-basheer-new-old-law-of-electronic-evidence (Last visited on January 20, 2016); Aradhya Sethia, *Where do we stand on 'secondary electronic evidence'?*, October 16, 2014, available at http://spicyip.com/2014/10/guest-post-where-do-we-stand-on-secondary-electronic-evidence.html (Last visited on January 20, 2016).

6 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

7 *Id*.

Part II of this paper discusses the position of law that prevailed prior to Anvar. This is done by first examining §65B and the way in which it fits within the framework of the Evidence Act. I then examine the way in which courts before Anvar understood and enforced the conditions for admissibility under §65B. In Part III, I provide a detailed analysis to the decision in Anvar, arguing that the approach taken by the Supreme Court is contrary to established principles of statutory interpretation. Not only has the Court misread many parts of the provision, but it has also willfully read in new requirements to suit its needs. Of the many conclusions the Supreme Court arrives at through this approach, the specific conclusion regarding the method of authenticating the electronic evidence is the focus of Part IV. Given the language of §65B, it is important to determine whether the approach that regards the availability of a 'certificate' (or the lack thereof) in respect of a particular piece of electronic evidence, as the necessary precondition and the sole ground for determination of its admissibility, is correct or not. On a reading of the Evidence Act and decided cases, I argue that this limitation that Anvar imposes is incorrect. Finally, in Part V, I examine contemporary practices in other jurisdictions. Based on their experiences, I propose the adoption of a different model for authenticating electronic evidence.

II. UNDERSTANDING §65B: PRE-ANVAR

A. OVERVIEW OF §65B

The Information Technology Act, 2000 was enacted with a view to regulate e-commerce transactions.[8] In furtherance of this, amendments to Chapter V of the Evidence Act dealing with documentary evidence were introduced. §§ 65A and 65B were introduced as special law regulating the admissibility of electronic evidence, which was rapidly making its presence felt in Indian courts.[9]

The only perceivable purpose of §65A is to refer to §65B, which then elaborately describes the method of authenticating electronic evidence.[10] Thus, the crux of the debate on electronic evidence lies squarely in the domain of §65B.[11] Sub-section (1) of the provision opens with a declaration that any

[8] This can be inferred from the Preamble to the IT Act, 2000, which reads: "An Act to provide legal recognition for transactions carried out by means of electronic date interchange and other means of electronic communication, commonly referred to as electronic commerce…" The 2008 amendments to the Act, however, expanded the scope of the statute significantly.

[9] Information Technology Act, 2000, Schedule II, Entry 9.

[10] It is interesting to note that §65A states: "Special provisions as to evidence relating to electronic record- The contents of electronic records may be proved in accordance with the provisions of § 65B." (emphasis added). This could arguably be interpreted as permitting the proving of the contents of electronic records in any other manner, including under §§ 61-65.

[11] Indian Evidence Act, 1872 §65B (It states:
"65B. Admissibility of electronic records.-

(1) Notwithstanding anything contained in this Act, 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 (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:—

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,—

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

information contained in electronic records that is transferred on to any media such as a CD or a USB device (referred to as 'computer output') will be admissible in court as evidence of the electronic record.[12] That is, parties are not obligated to produce the original record, which may be present on a desktop computer or a remote server, and which is difficult (if not impossible) to bring to court.[13] This enabling provision creates an exception to the common law evidentiary principle that where an original document is available, no secondary document may be produced.[14]

This leeway that §65B(1) grants is subject to one caveat of certain conditions listed in §65B(2)[15] relating to the information and computer in question being satisfied. These conditions seek to ensure that output was generated and the computer was used lawfully in the ordinary course of business. Specifically, they require the following: *first*, the computer must have produced the output in a period when it was regularly used to store/process information for activities regularly carried out by a person in lawful control over it.[16] *Second*, during that period of time, said information must have been regularly fed into the system in the ordinary course of said activities.[17] *Third*, the computer should have been operating properly, if it was not working, then it must have been such as to not affect the electronic record or the accuracy of the information contained in it.[18] Finally, the information in the electronic record must be a copy of, or derived from, the information that was fed into the computer in the ordinary course of the activities.[19]

These four conditions are accompanied by the use of 'and' as a conjunction, indicating that all the conditions must necessarily be complied with. These conditions are crucial to §65B, introduced to counter the problems of accuracy and reliability that beleaguer electronic evidence.[20]

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.").

12 Indian Evidence Act, 1872, §65B(1).

13 This can be compared to §65(d), Indian Evidence Act, 1872, which allows secondary evidence where "the original is of such a nature as not to be easily movable".

14 This is also known as the 'best evidence' rule. *See* Halsbury's Laws of England, Vol. 17, ¶138 (4th ed., 1973); Ratanlal and Dhirajlal, Law of Evidence (23rd ed., 2014); *Bank of India* v. *Alibhoy Mohammed*, 2008 SCC OnLine Bom 91 : AIR 2008 Bom 81; *Bimla Rohal* v. *Usha*, (2002) 2 Shim LC 341 (In our Evidence Act, this principle is codified in §64 and §65 for physical documents).

15 Indian Evidence Act, 1872, §65B(2).

16 *Id*., §65B(2)(a).

17 *Id*., §65B(2)(b).

18 *Id*., §65B(2)(c).

19 *Id*., §65B(2)(d).

20 *See infra* Part IV (A) for more discussion on the nature of §65B(2).

The other key sub-section is §65B(4),[21] which speaks of a 'certificate' in relation to the electronic record. The provision makes a certificate containing information under clauses (a), (b), or (c) of sub-section (4), evidence of the matter that it states. For example, if a certificate for a CD is issued under clause (a), it will identify the CD as containing the statement sought to be introduced in court and describe the manner in which it was produced (whether through a computer or a laptop, what was the software used etc.). This identification and description need not be corroborated by further proof, if a person "occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities"[22] signs the certificate, the details are assumed to be true. This is equally applicable to clauses (b) and (c) of sub-section (4). The question whether this 'certificate' is mandatory or not and whether it is the only way one may satisfy the conditions under §65B (2) has long been the bone of contention.[23] This is addressed in greater detail in Parts III and IV of this paper.

The remaining sub-sections of §65B (3) and (5) are largely technical in nature, relating to the nature of the computer and methods of supplying and producing information.[24] They have, thus far, remained controversy-free.

When one breaks §§ 65A and 65B down in this manner, it becomes apparent that the two provisions mirror §§ 61-65 of the Evidence Act. The language in §65A echoes that of §61. The electronic record in its original form (on the computer/remote server) is equivalent to primary evidence, as defined by §62. If this original record and not the computer output is produced, it is possible to circumvent the conditions stipulated in §65B(2). This is similar to §64 which declares the "existence, condition, or contents"[25] of physical documents proved, when they are produced in its original form. Finally, the computer output referred to in §65B(1) can be compared to secondary evidence under §63(2) or (3),[26] depending on the process by which it was created. Just as §65B(2) conditions need to be satisfied for computer output, secondary evidence is permissible only if it falls under §65.[27]

The fact that such extensive comparison to the original provisions in Chapter V of the Evidence Act is possible raises two questions. *First*, whether there is a requirement of §§ 65A and 65B. *Second*, whether the purview of §§ 61 to 65 is broad enough and equally capable of dealing with electronic evidence.

---

21 Indian Evidence Act, 1872, §65B(4).

22 *Id*., §65B(4). *See* Part IV (B) for more discussion on who this person "occupying a responsible official position…" can be.

23 *See infra* Part II (B), III & IV.

24 Indian Evidence Act, 1872 §§65B(3) & (5).

25 *Id*., §65.

26 *Id*., §63.

27 *Id*., §65.

The answer to the former appears to be in the affirmative. With respect to the second question, while it is true that §§ 61 to 65 of the Evidence Act are broad enough to cover electronic evidence themselves, such an approach would have led to electronic evidence being treated the same way as physical evidence. This would not have taken into account their particular unreliability. Not only does electronic evidence carry with it the usual problems of deliberate or accidental human error that traditional evidence does, it poses additional problems such as hardware failure, software glitches, and the comparative ease of tampering and manipulation.[28] These problems are beyond the comprehension of traditional evidence law. It is in recognition of this that several countries have introduced special laws to deal with electronic evidence.[29] In the words of one preamble, the purpose of these special laws is to "facilitat[e] and regulat[e]…electronic communications and transactions" while simultaneously "prevent[ing] abuse of information systems".[30]

In India, the introduction of §§ 65A and 65B, with their elaborate conditions and safeguards was the corresponding attempt to solve these unique problems. The provisions were meant to provide guidance and lay down standardized procedure for trial courts to follow, so that they could deal with the new challenges thrown up by technological advances. However, as the next section demonstrates, the divergent attitudes taken by trial courts towards electronic evidence, has frustrated both these aspirations.

B. JUDICIAL HISTORY

The test for admissibility under § 65B was considered for the first time in 2003 in *State* v. *Mohd. Afzal* ('*Mohd. Afzal*'),[31] also known as the Parliament Attack case. The Division Bench of the Delhi High Court was called upon to determine whether the call records in evidence had been admitted in accordance with §65B. The appellant-accused contended that certain call records were inadmissible as the prosecution had not submitted the §65B(4) certificate, which they argued was the only permissible way of satisfying §65B.[32] The prosecution rebutted this on the grounds that the conditions under §65B(2) had been met through the testimony of the relevant prosecution witnesses. This argument of the prosecution found favour with the Delhi High Court. On an examination of the provisions under § 65B, the Court noted that, "compliance with Sub-sections (1) and (2) of § 65B is enough to make admissible and prove electronic records".[33] They agreed with the prosecution that the certificate

---

28 *Supra* note 1; J. Hofman, *Electronic Evidence in Criminal Cases*, 19(3) SACJ 257, 258 (2006).
29 *See infra* Part V.
30 South Africa Electronic Communications and Transactions Act, 2002, Preamble.
31 State v. Mohd. Afzal, (2003) 107 DLT 385.
32 *Id*., ¶266.
33 *Id*., ¶276.

under §65B(4) was merely an "alternative mode of proof".[34] Comparing computer output under §65B to secondary evidence under §65(d), the court held that the oral evidence was equally sufficient; the lack of certificate was not an automatic bar.[35]

Two years later, this decision was affirmed in appeal by the Supreme Court in *State (NCT of Delhi)* v. *Navjot Sandhu* ('Afsan Guru').[36] The Court examined and accepted as sufficient the oral testimony provided by the prosecution witnesses.[37] It unequivocally held that even if the requirements under §65B(4) were not satisfied, evidence could be produced under §§ 63 and 65 of the Evidence Act.[38] In the words of P. Venkatrama Reddi, J:

> "Irrespective of the compliance with the requirements of § 65-B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely, §§ 63 and 65. It may be that the certificate containing the details in sub-section (4) of § 65-B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely, §§63 and 65."[39]

This decision led to a general relaxation of standards for electronic evidence. High Courts around the country approved other authentication methods as replacements for certificates, most notably, oral evidence. This has been done through the testimony of persons who created the computer output,[40]

---

[34] *Id*. That the §65B(4) certificate was an 'alternative method' was approved by the Delhi High Court in Rakesh Kumar v. State, (2009) 163 DLT 658. This in turn has been used as authority to waive certification. *See* Vijay v. State (Govt. of NCT of Delhi), 2014 SCC OnLine Del 4585 : (2014) 4 JCC 2494; Om Prakash v. State, (2014) 143 DRJ 349; Sun Pharmaceuticals Industries Ltd. v. Mukesh Kumar P., 2013 SCC OnLine Del 2713.

[35] *Id*. (The Court states:

"The normal rule of leading documentary evidence is the production and proof of the original document itself. Secondary evidence of the contents of a document can also be led under § 65 of the Evidence Act. Under sub-clause (d) of § 65, secondary evidence of the contents of a document can be led when the original is of such a nature as not to be easily movable. Computerised operating systems and support systems in industry cannot be moved to the court. The information is stored in these computers on magnetic tapes (hard disc). Electronic record produced there from has to be taken in the form of a print out.")

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

[37] *Id*.

[38] *Id*., ¶150.

[39] *Id*.

[40] A.M. Perumal v. Star Tours and Travels (India) Ltd., 2010 Cri LJ 3732; Devender Kumar Yadav v. State (NCT of Delhi), 2012 SCC OnLine Del 3771; Vijay v. State (Govt. of NCT of Delhi), 2014 SCC OnLine Del 4585 : (2014) 4 JCC 2494; Om Prakash v. State, (2014) 143 DRJ 349; Sun Pharmaceuticals Industries Ltd. v. Mukesh Kumar P., 2013 SCC OnLine Del 2713; Achchey Lal Yadav v. State, 2014 SCC OnLine Del 4539; Gajraj v. State, ILR (2009) Supp

persons qualified to testify as to the signature of the certifying officer, or the particularly low threshold of persons capable of "speak[ing] of the facts based on [their] personal knowledge."[41]

At the same time, many courts have also ignored both Mohd. Afzal and Afsan Guru, instead choosing to continue to demand a certificate for authentication.[42] In other cases, where neither certificates nor oral evidence were deemed adequate authenticators for uniquely complex technology, courts have called for technical data such as 'bit image copy' and hash codes.[43] In one exceptional case, the court simply did away with the authentication requirement on the basis that the other party had consented to placing certain computer files on record.[44]

On an overall analysis of the cases dealing with § 65B, it is clear that admission of evidence depends entirely on judicial discretion. Courts choose to follow whatever local requirements they believe is most appropriate for a case. An opportunity was presented to the Supreme Court nine years after Afsan Guru, in Anvar, to revisit the test for admissibility under § 65B, and conclusively lay down a standard, solving this uniformity problem.

III. ANVAR: REINTERPRETING §65B

The question of law under §65B in Anvar arose in connection with an election petition under §100(1)(b) of the Representation of People's Act, 1951. P.V. Basheer, the respondent, had been elected to the Kerala Legislative Assembly in 2011. The petitioner, P.K. Anvar, challenged the election on the grounds that the election propaganda used in the form of songs, speeches, and announcements had been defamatory. He argued that this amounted to a 'corrupt practice', and prayed for the setting aside of the election. In response, the Respondent challenged the admissibility of CDs containing said propaganda on the grounds that the requirements under §65B were not satisfied.[45] Specifically, the certificate discussed by §65B(4) was missing. The Kerala High Court, concurring with the Respondent that the requirements under §65B had not been

(2) Del 477; Babu Ram Aggarwal v. Krishan Kumar Bhatnagar, 2013 SCC OnLine Del 324 : (2013) 2 AD Del 441; Brij Kishore v. State, 2010 SCC OnLine Del 1892 : ILR (2010) Supp (1) Del 279; Mohd. Wasim v. State, 2012 SCC OnLine Del 5378 : (2012) 7 AD Del 599; Parminder Kaur v. State, 2014 SCC OnLine Del 3918; Shubha v. State of Karnataka, Criminal Appeals Nos. 722, 757 and 856 of 2010 (Kar) (Unreported); Devesh Kumar v. State, ILR (2010) 2 Del 798.

41 Societe Des Products Nestle SA v. Essar Industries, (2006) 33 PTC 469 (Del).

42 Pradeep Kumar v. State of Bihar, 2014 SCC OnLine Pat 483; Aniruddha Bahal v. CBI, (2014) 210 DLT 292.

43 Chetan Gupta v. CIT, ITA Nos. 1891, 1892 & 1893/Del/2012 (Del) (Unreported).

44 Mohd. Tahir Mohmed Arif Bakaswala v. State of Gujarat, 2010 SCC Online Guj 4829.

45 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

met, dismissed the election petition.[46] In appeal against this decision, the petitioner approached the Supreme Court.

The Supreme Court commenced its analysis by taking note of §59,[47] which prohibits the use of oral evidence to prove the contents of documents, and §65A, which states that the only way to adduce evidence of electronic records is through §65B.[48] On this basis, it excludes the applicability of all provisions of the Evidence Act, except §65B.[49]

This pure statutory interpretation is followed by an examination of its own previous decision in Afsan Guru.[50] The Supreme Court disagrees with Afsan Guru's dictum that §§ 61-65 of the Evidence Act can be applied where the conditions stipulated in §65B were not satisfied. It holds that while §§ 61-65 deal with general documentary evidence, §65B only refers to one special subset – electronic records. Therefore, applying the principle of g*eneralia specialibus non derogant*,[51] the Supreme Court holds that electronic evidence can be adduced solely under §65B. This conclusion is buttressed by the observation that §65B begins with a *non-obstante* clause.[52] The Supreme Court's interpretation of §65B consequently becomes critical.

In its analysis of the provision, the Supreme Court's focus is almost exclusively on sub-sections (2) and (4) of §65. It comes to three significant conclusions: *first*, all the conditions under sub-section (2) are mandatory. This understanding appears to be in consonance with the language used in sub-sections (1) and (2) of §65B, as noted earlier in this paper.[53]

The *second* conclusion of the Supreme Court relates to its interpretation of §65B(4). In addition to the four conditions under §65B(2), the Court paraphrases §65B(4) to arrive at five conditions that it states must be satisfied

---

46 *Id*.

47 Indian Evidence Act, 1872, §59 (It must be noted that this is an inaccurate reference to §59. §59 is inapplicable in light of §22A of the Indian Evidence Act, 1872, which is a special provision introduced at the same time as §65B. Applying the principle of *generalia specialibus non derogant*, §22A prevails. However, it must be noted that the effect is largely the same: §22A also bars the use of oral evidence. This is subject to the crucial exception of 'genuineness of the electronic record' however. *See infra* Part IV(A) for greater discussion on the use of oral evidence).

48 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶13.

49 *Id*. (The Supreme Court holds: "Any documentary evidence by way of an electronic record under the Evidence Act, in view of §§ 59 and 65A, can be proved only in accordance with the procedure prescribed under §65B." (emphasis added)).

50 *Id*., ¶22.

51 *See* Blacks' Law Dictionary (9th ed., 2009) (This latin maxim translates literally as general things do not detract from specific things. It enshrines the principle that a special law, or a law enacted to cover specific situations, will always prevail over a more generally applicable law).

52 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶13. This has been noted once prior to Anvar. *See* Abdul Rahaman Kunji v. State of W.B., 2014 SCC OnLine Cal 18816.

53 *See supra* Part II (A).

before a statement under §65B can be made.[54] The first of these relates to the method of authentication. The court states that under §65B(4), a certificate 'must' be produced.[55] The obvious corollary is that in the absence of a certificate, the electronic record will be inadmissible under §65B. This particular reading of the Evidence Act and the consequences flowing from it are analysed in greater detail in Part IV of this paper.

The remaining four conditions laid down by the court concern the contents of the certificate.[56] While these appear to be derived from the language of §65B(4), the interpretation adopted by the court is very curious. *First*, the Supreme Court ignores words that introduce elements of voluntariness and alternativeness in the provision.[57] For instance, §65B(4) states that a certificate must do "any of the following things," before listing out its clauses (a), (b), and (c).[58] This indicates that even if one of the three clauses are satisfied by the certificate, it would pass muster. The Supreme Court, in interpreting this, understands clauses (a), (b), and (c) §65B(4) as being individual *compulsory* aspects of the certificate.[59] Similarly, §65B(4)(c) permits the certificate to deal with any of the matters to which the conditions mentioned in sub-section (2) relate".[60] The Supreme Court reads it to mean that *all* of the conditions mentioned in sub-section (2) *must* be specified in the certificate.[61] The replacement of 'any' with 'all' is not explained in any manner.

Secondly, the Supreme Court reads in words where none exist. For example, the Court states that all the 'applicable' conditions of §65B(2) must be specified in the certificate.[62] No such language of 'applicability' exists in the section. Alarmingly, the addition of such a word creates a dichotomy between sub-section (2) and sub-section (4). Sub-section (2) makes 'all' the conditions mandatory, without regard to their "applicability." Given this, it is

---

54 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶14 (The Supreme Court states:
"Under § 65B(4) of the Evidence Act, if it is desired to give a statement in any proceedings pertaining to an electronic record, it is permissible provided the following conditions are satisfied:
(a) There must be a certificate which identifies the electronic record containing the statement;
(b) The certificate must describe the manner in which the electronic record was produced;
(c) The certificate must furnish the particulars of the device involved in the production of that record;
(d) The certificate must deal with the applicable conditions mentioned under § 65B(2) of the Evidence Act; and
(e) The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device.").

55 *Id*., ¶14(*a*).

56 *Id*., ¶14(*b*)-(*e*).

57 *Id*., ¶14.

58 Indian Evidence Act, 1872, §65B (4).

59 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶14 (*a*)-(*c*).

60 Indian Evidence Act, 1872, §65B (4)(c).

61 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶14(*d*).

62 *Id*., ¶14(*d*).

unclear how an element of "applicability" can be introduced into sub-section (4) by judicial interpretation.

Finally, the Supreme Court engages in selective paraphrasing, ignoring many parts of the sub-section. For instance, clause (b) of §65B(4) not only requires the certificate to give details of the particulars of a device involved in the production of the electronic record, it also requires these details to show that the electronic record was produced by a computer.[63] The Supreme Court overlooks this aspect. Similarly, the person required to sign the certificate must be in an official position either in relation to the 'operation' or in the 'management' of the device, as is appropriate. However, the Supreme Court refers merely to 'operation'.[64] While the nature of the consequences that will flow from this are uncertain, this indicates a substantial degree of negligence on the part of the Supreme Court.

Therefore, it is clear that that the interpretation of § 65B(4) in Anvar does not conform to the language of the provision, which both unambiguously and repeatedly adopts a policy of flexibility. Such an approach is in complete contravention of the literal rule of statutory interpretation.[65] What is truly unfortunate is that no part of the Supreme Court's decision acknowledges or attempts to explain the deviations made.[66]

The *third* conclusion the Supreme Court arrives at, in its interpretation of §65B, is that there is a requirement of contemporaneity in the production of the certificate. It is worth extracting the same here: "Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of § 65B obtained at the time of taking the document" (emphasis added)[67]

This dicta is to be read alongside a reference made to Afsan Guru. The Supreme Court in Anvar specifically notes that in Afsan Guru, a 'responsible officer' had certified the electronic records in question "at the time of

---

63 *Id*., ¶14 (*c*).

64 *Id*., ¶14 (*e*).

65 G.P. Singh, Principles Of Statutory Interpretation (2004); P. St. J. Langan, Maxwell On The Interpretation Of Statutes (12th ed., 1969).

66 Given the nature of §65B and the specific reasons for its introduction, legislative intent could very likely have been to make the certificate and all of the details mentioned in the provision mandatory. Poor drafting, which affects all provisions introduced through the Information Technology Act, 2000, is more likely to be the culprit. On this basis, it may have been possible to make an appeal to either the Golden Rule or the Mischief Rule in statutory interpretation to justify a deviation from the literal rule. In all fairness, the lack of extrinsic sources (statement of objects and reasons, standing committee reports etc.) on §65B means that the Supreme Court did not have any guidance on the matter. This argument merely goes to the glibness with which the Supreme Court deviates from the literal interpretation, without even making an attempt at an explanation.

67 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶22.

production itself".[68] That contemporaneous authentication is met with implicit approval in Anvar.

This contemporaneity requirement is one of the reasons the electronic evidence in Anvar was finally held to be inadmissible. The Supreme Court held that since a certificate was not produced at the same time the computer output was generated, it could not be admitted at all.[69] What this means is that if a party omits to get a certificate at the time of, say, generating CD or printout, the evidence becomes inadmissible. This requirement imposes exceptional burdens on parties who may not always be in a position to obtain such a certificate at the time of generating the evidence, such as whistleblowers.[70] Further, the conclusion that the Supreme Court has arrived at on this point exaggerates the usefulness of the certificate. Unlike safeguards employed in the case of physical evidence, which prevent tampering or ensure an unbroken chain of custody, it is merely a certification that the evidence was generated in a particular manner. Therefore, the level of authenticity it is bestowing on the evidence is in any case minimal.

Finally, it must be noted that the contemporaneity requirement is unquestionably extra-statutory. §65B makes no mention of any time period within which the certificate must be produced, let alone that the certificate must be taken at the same time as the document. The effects of this holding are already being felt. The Delhi High Court in *Ankur Chawla* v. *CBI*[71] recently applied the contemporaneity requirement to declare evidence inadmissible, stating that since time had elapsed, there was "no point in now permitting the prosecution to place the…certificate on record."[72]

IV. ANVAR: LIMITING METHODS OF AUTHENTICATING ELECTRONIC EVIDENCE

A. §65B(4) CERTIFICATE: IS IT REALLY MANDATORY?

One of the conclusions in Anvar, noted in the previous section, was that the court's reading of §65B had created a limitation on the methods of authentication, namely, that only a certificate under §65B(4) can be used to

[68] *Id*., ¶21.
[69] *Id*., ¶23.
[70] *See infra* Part IV (B).
[71] Ankur Chawla v. CBI, 2014 SCC OnLine Del 6461.
[72] *Id*. *But see* Paras Jain v. State of Rajasthan, 2015 SCC OnLine Raj 8331 (The Rajasthan HC had the opportunity to consider a situation where the prosecution had not produced the certificate at the time of filing the charge-sheet; they had produced it during the course of the trial. The court dismissed a challenge against this delayed filing by the accused on the grounds that in Anvar "the question of stage at which such electronic record is to be produced was not before the Hon'ble Court". Such creative reading of Anvar enabled the prosecution to bring on record crucial electronic evidence).

satisfy the conditions under §65B(2). Therefore, if a litigant wishes to use any alternative method to satisfy the conditions under §65B(2), it is now no longer possible. This rule has already seen application: the Delhi High Court in the recent decision of *Jagdeo Singh* v. *State*[73] held that oral evidence regarding electronic evidence was insufficient.[74] In the absence of a certificate satisfying the Anvar conditions, the evidence was held to be inadmissible.[75]

This is not a conclusion supported by the language of the provision. On the contrary, on a plain and literal reading, §65B(4) merely states that a duly signed certificate containing some matter compliant with (a), (b), or (c), 'shall be evidence' of that matter. Nowhere does the provision state that a certificate 'shall be submitted' if electronic evidence is to be admitted, or that 'all' other authentication methods are barred. In the absence of any such bar, the conclusion drawn by the Supreme Court is incorrect. This is supported by §§65B(1) and (2), which deem computer output of electronic records as documents subject to the fulfillment of certain conditions. The mode of fulfilling the conditions is not specified.

Given that §65B does not mandate the submission of a certificate, one question logically follows: what other authentication methods for electronic records are legally permissible under the Evidence Act?

The answer to this question lies in the kind of evidence that is permitted under the Evidence Act. As per §3, broadly two kinds of evidence are permitted, documentary evidence and oral evidence.[76] Either of these two kinds of evidence may, theoretically, be sources of information regarding the accuracy and reliability of an electronic record.

The former - documentary evidence - would relate to certificates, affidavits, reports, official documents, and the like. I have previously established that §65B(4) does not make a certificate either mandatory or an exclusive method of authentication.[77] In the absence of such language, the logical conclusion would be that there is no express bar on other kinds of documentary evidence. Therefore, it should be possible to use other documentary evidence, other than a certificate under §65B(4), to admit electronic records.

---

[73] Jagdeo Singh v. State, 2015 SCC OnLine Del 7229, ¶¶68-79 (Interestingly, the Delhi HC held: "Since PW-17 can speak only about the computer which he was using and what he was listening to on it are copies made of the originals, no part of § 65-B EA can be said to have been complied with, much less substantially complied with" (emphasis added). Applying Anvar, the oral evidence as a method of authentication ought to have been *ab initio* insufficient, regardless of whether the conditions of §65B(2) were satisfied or not. That is, the discussion of substantial compliance is unnecessary in the absence of a certificate).

[74] *Id*.

[75] *Id*.

[76] Indian Evidence Act, 1872, §3.

[77] *See supra* Part III.

The question of whether oral evidence can be used to satisfy §65B(2) conditions is trickier since §22A of the Evidence Act expressly bars the use of oral evidence.[78] However, it makes a crucial distinction. While oral evidence cannot be adduced to prove the contents of the document, it can be adduced if it goes towards the 'genuineness' of the record.[79] Therefore, when it is suspected that a document is manufactured, or is not what it claims to be, oral evidence can be adduced to determine whether the record is genuine.

This 'genuineness' is precisely what the four conditions under §65B(2), as discussed above, seek to ensure. To illustrate, as per §65B(2)(c), a person seeking to introduce as evidence computer output generated at a particular time, must ensure "that throughout the material part of the said period, the computer was operating properly".[80] If the computer alleged to have produced the record was not operating properly at the relevant time,[81] it is highly probable that the document was not generated accurately. Similarly, if the information contained in the computer output was not of the kind "regularly fed into the computer in the ordinary course of the said activities",[82] it would obviously raise red flags. Such information will have to be scrutinized to see if it was manufactured specifically for the purpose of the trial or not. Thus, genuineness is clearly a concern that §65B(2) addresses. Consequently, there is no reason why the four conditions it stipulates cannot be met through oral evidence as per §22A of the Evidence Act.

Anvar considers and rejects this line of argument, stating that "only if the electronic record is duly produced in terms of § 65B of the Evidence Act, the question would arise as to the genuineness thereof…"[83]

It is clear from the above statement that the Supreme Court believes that the question of genuineness can never be answered at the stage of admissibility. On the contrary, the Supreme Court indicates that this is always a post-admission question. Such an understanding of evidence law is incorrect for two reasons.

First, this argument is inconsonant with the language of §65B, as noted above. It is also inconsistent with the policy behind it. As the Supreme Court itself acknowledges, the purpose behind §65B, which specifically relates to admissibility, is to guarantee 'source and authenticity' of documents.[84] This is unquestionably a question relating to the genuineness of the document.

---

78 Indian Evidence Act, 1872, §22.
79 *Id*.
80 *Id*., §65B(2)(c).
81 *Id*.
82 *Id*., §65B(2)(b).
83 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶16.
84 *Id*., ¶15.

Therefore, there is clear contradiction in the court's reasoning behind dismissing oral evidence.

Second, the declaration by the Supreme Court that reliability or genuineness "go to the weight of evidence and not to admissibility" is not accurate.[85] If one examines the Evidence Act, it is clear that it does not split the process of adducing evidence into the stages of relevance, admissibility and weight. In fact, it is completely silent on how evidence is to be weighed. The only reference to the stages of relevance and admissibility is under §136, which states that if the judge thinks a fact is relevant, he 'shall' admit it.[86] Therefore, far from recognizing them as different evidentiary stages, the Evidence Act conflates relevancy with admissibility.

However, despite this lack of statutory support, there is significant Supreme Court jurisprudence that has explained what is to be considered at the stage of admissibility.[87] Starting with *R.M. Malkani* v. *State of Maharashtra*,[88] a line of Supreme Court cases concerning the evidentiary value of tape-recorded conversations, have held that reliability of the evidence must be established before it is admitted.[89] That is, even if the information is relevant, it will not be admitted if it is not reliable. The reason for this has consistently been that new technology, like tape-records, can easily be tampered with or manipulated. Given these identical concerns, there is no reason why this ratio cannot be extended to electronic evidence as well; in fact, the same logic applies seamlessly.[90] Ironically, the Supreme Court in Anvar itself emphasized the importance of authenticity of electronic evidence for these very reasons.[91]

Therefore, contrary to the reasoning provided by the Supreme Court, genuineness is indeed a concern under §65B, and is a crucial part of the evidentiary stage of admissibility. Consequently, it should permissible under the Evidence Act for a party to adduce oral evidence to satisfy the conditions of

---

85 *See id*., ¶18 (The Supreme Court does not cite authority for this proposition of law. Instead, it points vaguely to the American Federal Rules of Evidence to support its point that reliability is considered only at the stage of weight).

86 Indian Evidence Act, 1872, §136.

87 *See* Ram Bihari Yadav v. State of Bihar, (1998) 4 SCC 517 : 1998 Cri LJ 2515, 2517; Sarkar's Law of Evidence 86, 88 (S. Sarkar and V. Manohar, 15th ed., 1999) (It is interesting to note that this jurisprudence had been brought to the notice of the court of first instance i.e. the Kerala High Court. It is however unclear what the argument advanced by counsel was. Anvar P.V. v. P.K. Basheer, (2012) 247 KLR 933, ¶¶68-69).

88 R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471, ¶23.

89 *See* Yusufalli Esmail Nagree v. State of Maharashtra, AIR 1968 SC 147, ¶6; Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdass Mehra, (1976) 2 SCC 17, ¶¶18-22 : AIR 1975 SC 1788; Tukaram S. Dighole v. Manikrao Shivaji Kokate, (2010) 4 SCC 329, ¶¶23-27.

R. v. Maqsud Ali, (1966) 1 QB 688 : (1965) 3 WLR 229 : (1965) 2 All ER 464 (CCA); But *see* S. Pratap Singh v. State of Punjab, AIR 1964 SC 72 : (1964) 4 SCR 733, ¶16.

90 But *see* Law Commission of India, *Review of the Indian Evidence Act, 1872*, Report No. 185, Part II, 19, 2003.

91 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶15.

§65B(2) and the certificate should not the only possible authentication method envisaged.

B. DIFFICULTIES AND DICHOTOMIES

Post-Anvar, the above discussion on whether the Evidence Act makes other methods of authentication possible or not, is irrelevant. The law as it stands today admits electronic records into evidence only if a certificate is produced.[92] This leads to curious difficulties in the application of the law.

First, Indian courts are frequently faced with situations where evidence has been improperly or illegally obtained especially by whistleblowers, investigative agencies conducting surreptitious/unapproved searches, approvers seeking favour with authorities etc. Such evidence is allowed because Indian evidence law famously does not follow the 'fruit of the poisoned tree' doctrine; instead we have adopted the position that the method by which the evidence is obtained is irrelevant.[93] The problem that is likely to arise in such cases is that certification by a "person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities"[94] will be practically impossible. For example, data that is stolen is unlikely to get certification. An owner of a computer (the person in the 'responsible official position' over the computer) is hardly likely to aid a thief by signing a certificate authenticating the information contained therein. Therefore, the reading of § 65B in Anvar will lead to a dichotomous situation: while illegally obtained evidence will be admissible in the case of non-electronic evidence (where no such certification by the owner is required), it may be inadmissible in the case of electronic evidence.

Second, certificate-based authentication method is also particularly susceptible to fraud/manipulation. It is not based on objective, ascertainable facts as metadata is. It also does not have the three-fold safeguards of oath, cross-examination and observation of demeanour that is guaranteed in the case of oral evidence. On the contrary, the certificate is a mere statement on the record that is submitted by the same party desirous of getting the evidence admitted. Consequently, apart from the fear of falling afoul of the law of perjury, there is nothing preventing parties from submitting fraudulent/manufactured certificates.[95] Therefore, Anvar fails in its attempt at setting a higher threshold of authenticity/genuineness of electronic records.

---

92 The Supreme Court's order in Anvar has binding force of law. *See* Article 142, Constitution of India, 1950.

93 *See* Law Commission of India, *Evidence obtained illegally or improperly: Proposed Section 166A, Indian Evidence Act, 1872*, Report No. 94, 1983; *Yusufalli Esmail Nagree* v. *State of Maharashtra*, AIR 1968 SC 147; *R.M. Malkani* v. *State of Maharashtra*, (1973) 1 SCC 471.

94 Indian Evidence Act, 1872, §65B(2)(a).

95 *See* Indian Penal Code, 1860, §§191-200.

Apart from potential misconduct by parties, the reliability of the certificate is also undercut by the fact that it does not verify against tampering or other improper procedures affecting its accuracy. If the conditions under §65B(2) are examined, it is clear that it is limited to determining who has control over the computer in question and the regularity with which the information has been fed into the computer.[96] It does not guard against tampering/alteration of the information. Therefore, even if the lawful owner of a computer, in the regular course of business, deliberately alters evidence, the conditions of §65B would be satisfied.

This cumulatively results in a very low reliability threshold for the certificate. Anvar's insistence on this authentication method is very likely to cause an increase in the amount of false and/or frivolous evidence that parties introduce into the record. This will not only prolong the trial, increasing systemic delays, it will also undercut the truth-seeking process.

The following section of the paper, looking at the experiences of other common law jurisdictions, proposes a new authentication model for electronic evidence. It advances solutions to these two specific problems.

V. REWORKING §65B: EXPANDING AUTHENTICATION METHODS

There are two primary ways in which common law jurisdictions differ in their approach to the admissibility of electronic evidence. *First*, they either make a special law for electronic evidence, or they treat electronic evidence on par with traditional kinds of evidence. For instance, Canada[97] and South Africa[98] have both enacted special statutes to deal with electronic evidence. On the other hand, the US[99] and the UK[100] both address it under their main evidence statutes.

The *second* way in which countries differ relates to the way they deal with methods of authentication – whether they prescribe specific methods, or they leave the question of method open, vesting in courts the discretion to determine reliability. The former practice can be seen in Canada[101] and the Australian federal unit of South Australia[102]; the US[103] and South Africa are

---

96 *See* Indian Evidence Act, 1872, §65B(2).

97 *See generally* Uniform Electronic Evidence Act, 1998 (Canada).

98 *See generally* South Africa Electronic Communications and Transactions Act, 2002 (South Africa).

99 *See generally* Federal Rules of Evidence, 2015 (U.S.).

100 *See generally* Civil Evidence Act, 1995 (U.K.); Criminal Justice Act, 1988 (U.K.).

101 Uniform Electronic Evidence Act, 1998, §§3-7 (Canada).

102 South Australian Evidence Act, 1929, §59B (South Australia).

103 Federal Rules of Evidence, 2015, §§901, 902 (U.S.).

examples of the latter.[104] A third approach is also possible - authenticity is only considered at the stage of weighing evidence. This approach is most clearly articulated by the UK.[105]

India, by enacting the Information Technology Act, 2000 and introducing §§ 65A and 65B into the Evidence Act, clearly opted for the special law approach. The second diverging practice i.e. the issue of method of authentication is the more contentious issue in India.

Post-Anvar, as the law stands, India falls within the first of the three categories by prescribing a specific, limited, authentication method. As demonstrated, this is a highly flawed approach. However, what must be noted that is that these flaws are ones relating exclusively to the approach the Supreme Court has taken to interpretation; the outcome of this judicial rewriting of §65B must be judged separately.

If Anvar is viewed from this outcome-based or end-based perspective, it is apparent that there are two immediate benefits of making a certificate mandatory under §65B. *One,* a bare-minimum guarantee of reliability, and *two*, uniformity in practice across the country. Whereas the first takes one (small) step towards preventing the repetition of Afsan Guru-esque tragedies,[106] the second guards against poor exercise of discretion by judges, which needless to say is endemic in India. These benefits of a specific authentication method, limiting the scope of judicial discretion, cannot be understated, particularly in light of the discussion in Part II (B) of this paper. At the same time, this has to be counterbalanced by the problem of the certificate only creating a low reliability threshold that were identified in Part IV (B) of this paper, namely, the problem of illegally obtained evidence, the certificate's poor guarantee of authenticity, and the lack of guarantee against tampering/alteration.

It is proposed that this balance be achieved through a hybrid authentication model, inspired by the erstwhile-UK,[107] South Australian,[108] and

---

[104] South Africa Electronic Communications and Transactions Act, 2002, §15 (South Africa).

[105] *See generally* Civil Evidence Act, 1995 (U.K.); Criminal Justice Act, 1988 (U.K.); *See* UK Law Commission, *The Hearsay Rule in Civil Proceedings*, Report No. 216, 1993; UK Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics,* Report No 245, 1997; Law Reform Commission, Ireland, *supra* note 1, ¶¶5.74–5.86; Technology Law Development Group, Singapore, *supra* note 1, ¶¶2.25-2.43.

[106] *See* Acharya, *supra* note 5.

[107] Civil Evidence Act, 1968, §5 (U.K.).

[108] South Australian Evidence Act, 1929, §59B (It states:
(2) The court must be satisfied—
(a) that the computer is correctly programmed and regularly used to produce output of the same kind as that tendered in evidence pursuant to this section; and
(b) that the data from which the output is produced by the computer is systematically prepared upon the basis of information that would normally be acceptable in a court

American[109] models. Before elaborating on the nature of the changes that can be introduced, the three specified models can be broadly outlined as follows.

The first of these is the UK model under §5 of the Civil Evidence Act, 1968.[110] This provision is identical to §65B, both in language and in structure.[111] It declares, for instance, that a certificate fulfilling four specified conditions, and signed by a person 'occupying a responsible position' may be evidence of the matters stated therein. These four conditions, laid down in §5(2), are identical to those specified in §65B(2).

The second, the South Australian model, can be called an expanded or improved version of the 1968 UK model. §59B stipulates three conditions in addition to the four standards mentioned in §5(2). *One*, the computer should not have been altered such that it affected the accuracy of the output.[112]

---

of law as evidence of the statements or representations contained in or constituted by the output; and

(c) that, in the case of the output tendered in evidence, there is, upon the evidence before the court, no reasonable cause to suspect any departure from the system, or any error in the preparation of the data; and

(d) that the computer has not, during a period extending from the time of the introduction of the data to that of the production of the output, been subject to a malfunction that might reasonably be expected to affect the accuracy of the output; and

(e) that during that period there have been no alterations to the mechanism or processes of the computer that might reasonably be expected adversely to affect the accuracy of the output; and

(f) that records have been kept by a responsible person in charge of the computer of alterations to the mechanism and processes of the computer during that period; and

(g) that there is no reasonable cause to believe that the accuracy or validity of the output has been adversely affected by the use of any improper process or procedure or by inadequate safeguards in the use of the computer.

(3) …

(4) A certificate under the hand of a person having prescribed qualifications in computer system analysis and operation or a person responsible for the management or operation of the computer system as to all or any of the matters referred to in subsection (2) or (3) of this section shall, subject to subsection (6) of this section, be accepted in any legal proceedings, in the absence of contrary evidence, as proof of the matters certified.

(5) An apparently genuine document purporting to be a record kept in accordance with subsection (2) of this section, or purporting to be a certificate under subsection (4) of this section shall, in any legal proceedings, be accepted as such in the absence of contrary evidence.

(6) The court may, if it thinks fit, require that oral evidence be given of any matters comprised in a certificate under this section, or that a person by whom such a certificate has been given attend for examination or cross-examination upon any of the matters comprised in the certificate).

[109] Federal Rules of Evidence, 2015; Lorraine v. Markel American Insurance Co., 241 FRD 534, §§901, 902.

[110] Civil Evidence Act, 1968, §5 (U.K.).

[111] §65B appears to have been copied almost to the word from §5 of the Civil Evidence Act, 1968. It is interesting (and appalling) to note that this happened in 2000, about 5 years after the UK repealed the 1968 Act and replaced it with the UK Civil Evidence Act, 1995.

[112] South Australian Evidence Act, 1929, §59B(2)(e).

Two, records of all alterations should have been kept by a responsible person,[113] and *three*, that there be no reasonable cause to believe that the accuracy of the information was affected by improper use or inadequate safeguards.[114] These three conditions cumulatively guard against tampering/alteration of the electronic record, which §5 of the UK Civil Evidence Act, 1968 does not. §59B also departs in other important ways. For instance, it permits the leading of oral evidence, if the court thinks it necessary.[115] It also allows the certificate to be challenged by other records that may have been maintained in relation to the computer in question, as long as these other documents themselves comply with the conditions contained in the provision.[116]

The American federal law on electronic evidence is the third and final model. §§ 901 and 902 of the Federal Rules of Evidence, 2015 lay down out a non-exhaustive list of accepted authentication methods.[117] These range from oral evidence to expert testimony to proof by public reports. In 2007, in *Lorraine* v. *Markel American Insurance Co.,*[118] the Chief Magistrate Judge of the District of Maryland extended the applicability of these provisions to electronic evidence. This landmark decision is widely regarded as an essential primer on, and as explaining the position of law in the US on, the admissibility of electronic evidence.[119] This has led to the creation of a flexible, inclusive framework whereby electronic evidence can be made admissible by way of multiple means; parties and courts are not constrained by any one method of authentication. This ensures that "room for growth and development in this area"[120] is guaranteed. A combination of the best of these three models can help us resolve the problems identified with § 65B.

To begin with, I propose that the certificate based authentication system be maintained, as in the erstwhile-UK model, and as it continues to be in South Australia. However, this must be significantly modified. *First*, additional conditions must be added to §65B(2), which take into account tampering

[113] *Id*., §59B(2)(f).
[114] *Id*., §59B(2)(g).
[115] *Id*., §59B(6).
[116] *Id*., §59B (5).
[117] Federal Rules of Evidence, 2015, §§901, 902.
[118] Lorraine v. Markel American Insurance Co., 241 FRD 534.
[119] J.D. Frieden and L.M. Murray, *The Admissibility of Electronic Evidence under the Federal Rules of Evidence*, XVII (2) Rich. J.L. & Tech. 5 (2011); M. Gifford, *Admitting Electronic Evidence in Federal Court: I've Got All This Electronic Data – Now What Do I Do With It?*, 2 ABA J. 8 (2008); Rashbaum *et al*, *Admissibility of Non-US Electronic Evidence*, XVIII (3) Rich. J.L. & Tech. 9 (2012); Lexis Nexis, *Lorraine* v. *Markel: Electronic Evidence 101*, 2007, available at https://www.lexisnexis.com/applieddiscovery/LawLibrary/whitePapers/ADI_WP_LorrainevMarkel.pdf (Last visited on January 30, 2016).
[120] Federal Rules of Evidence, 2015, *Advisory Committee's note* to Rule 901(b).

or deliberate alteration of electronic evidence. This will make the certificate more comprehensive in its coverage.[121]

Second, a specific exception needs to be carved out for illegally obtained evidence, exempting such evidence from a certificate requirement. This will help resolve the previously noted dichotomy between traditional and electronic evidence.[122]

Third, and most importantly, the language should be altered to make the certificate mandatory, and not optional, as it is in its current form. There are several reasons for this. *First*, the § 65B(4) certificate (modified as above) presents to the court the minimum necessary information regarding electronic records. Technical questions such as how the computer output was generated, the regularity with which information was fed into the system, whether the computer had ever had technical failures etc. are difficult for the court to comprehend without assistance. The certificate will act as a starting point for any inquiry into the authenticity/genuineness of the evidence. *Second*, it guarantees a certain degree of uniformity in practice across the country. It will also help courts ask the right questions regarding the nature of the electronic record, which they otherwise might not. *Third*, in the absence of a mandatory certificate, one might be faced with situations where courts accept electronic evidence without any authentication method whatsoever i.e. without any guarantee of authenticity/genuineness. If the certificate is made mandatory, an aggrieved party will be in a better position to challenge admission of the electronic record.

Yet, while the certificate creates a minimum information and authenticity threshold, it will obviously not be sufficient in all situations. As observed previously, the certificate is a neither foolproof nor a very strong guarantor of authenticity/genuineness. Therefore, in addition, § 65B should be amended to specifically empower courts to demand, and parties to submit if they so choose, additional authentication. Admittedly, with such a grant of judicial discretion comes the fear of judicial overreach. However, this can be easily curbed: additional authentication can be demanded only where there is reason to believe or reasonable grounds for suspicion that the any of the conditions/requirements of § 65B are not satisfied.

Such a model, mirroring the non-exhaustive, broad set of authentication methods prescribed by Rules 901 and 902 of the American Federal Rules of Evidence, 2015[123] would allow for authentication methods such as metadata,

---

[121] *See* South Australian Evidence Act, 1929, §59B(2)(g) (This emulates the South Australian provision, strengthening the safeguards provided for in §65B(2) by protecting against improper processes or procedures in the production of the output).

[122] *See supra* Part IV (B).

[123] Federal Rules of Evidence, 2015, Rules 901, 902.

authentication through public records, oral testimony, specimen comparison etc. There are several benefits to increasing the number of authentication methods for electronic evidence in this manner. *First*, and most importantly, they will help corroborate the evidence, and may often reveal important information that certificates do not.[124] *Second*, advances in technology are bound to lead to better authentication methods in the near future. In those circumstances, restricting authentication to a primitive certification method such as the §65B(4) certificate will be both regressive and counterproductive. It will prevent the necessary growth and development of Indian evidence law. *Finally*, by allowing multiple methods of authentication that corroborate the §65B certificate, the electronic evidence sought to be admitted will be forced to meet a higher reliability threshold. This will go a long way in improving the truth-seeking function of courts.

At the moment, if Anvar is followed, none of these benefits will accrue. Admittedly, these other authentication methods are not barred by §65B in its current form. However, these methods will necessarily have to be in addition to the §65B(4) certificate. Litigants will only view this as an additional unnecessary burden and are unlikely to take it upon themselves. Therefore, these additional authentication methods will in practical terms be redundant. Further, in any event, if the position of law laid down in Anvar is allowed to stand, these additional methods will not prevent the admission of the evidence; they will only go towards weight.[125] Consequently, even if a court today doubts the reliability of a piece of evidence, as long as the certificate is produced, it will be forced to place it on record.

The proposed model resolves these problems by empowering courts to demand additional authentication. By doing so, it will help courts exclude *prima facie* unreliable evidence from the record. This empowering of courts is particularly important in the case of improperly or illegally obtained evidence, for which this proposed model carves out an exception. Given the particular unreliability of such kind of evidence, it will be helpful to have a combination of reliable authentication methods, such as, oral evidence in combination with metadata.

VI. CONCLUSION

The Supreme Court's decision in Anvar evokes mixed feelings. On the one hand, it blatantly disregards principles of statutory interpretation, ignoring and wilfully reading in statutory requirements as it sees fit. From a practical viewpoint, by laying down mandatory form and content requirements,

[124] *See* M. Gifford, *supra* note 119; J. Isaza, *Metadata in Court: What RIM, Legal and IT Need to Know*, 2010, available at http://www.armaedfoundation.org/pdfs/Isaza_Metadata_Final.pdf (Last visited on February 8, 2016).

[125] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶16-17.

it creates unnecessary rigidity in §65B. Yet, when viewed from a policy perspective, it has yielded benefits. It has granted the dual advantages of uniformity and certainty in evidentiary practices. This can be seen in the way lower court around the country have dealt with electronic evidence since September 2014,[126] with the singular exception of *Tomaso Bruno* v. *State of U.P.*[127] in January 2015.

However, accepting Anvar with both its flaws and its advantages is less than ideal. If we are to truly embrace the modernization of evidence law, we cannot accept the low reliability threshold that Anvar sets, nor can we restrain our future selves from capitalizing on inevitable technological advances. Therefore, it is essential that the methods of authenticating electronic evidence should not be restricted in the way Anvar desires. The model that this paper proposes, which necessitates certificates (subject to the exception of illegally obtained evidence) but permits additional authentication methods, is one definite way out of the difficulties Anvar will eventually lead us into.

[126] Manoj Kumar S. v. State of Karnataka, Criminal Appeal No. 1419 of 2012, decided on 30-6-2015 (Kar) (Unreported); Ankur Chawla v. CBI, 2014 SCC OnLine Del 6461; S.K. Saini v. CBI, 2015 SCC OnLine Del 11472; Balasaheb Gurling Todkari v. State of Maharashtra, (2015) 3 Bom CR (Cri) 51; Harish v. State of Delhi, 2015 SCC OnLine Del 10552; Indian Micro Electronics (P) Ltd. v. Chandra Industries, 2015 SCC OnLine Del 10076 : (2015) 6 AD Del 52; Bonanzo Portfolio Ltd. v. State of Assam, (2015) 1 GLT 339; S.M. Katwal v. Virbhadra Singh, 2015 SCC OnLine HP 1155; Hosamanera Prakash v. State of Karnataka, (2015) 2 AIR Kant R 710; Naveen v. State, (2015) 5 Kant LJ 574 (DB); Vikas Verma v. State of Rajasthan, (2015) 2 WLN 494 (Raj).

[127] Tomaso Bruno v. State of U.P., (2015) 7 SCC 178 (4 months after Anvar, the Supreme Court held that in cases involving electronic evidence, secondary evidence may be adduced under §65. Astonishingly, Kurien, J. was also a part of the bench deciding this case, although he did not deliver the opinion of the Supreme Court. P. Banumathi, J. in ¶25 held:

"…Sub-section (1) of § 65B makes admissible as a document, paper printout of electronic records stored in optical or magnetic media produced by a computer, subject to the fulfilment of the conditions specified in sub-section (2) of § 65B. Secondary evidence of contents of document can also be led under § 65 of the Evidence Act" (emphasis added).