IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Issues and Challenges of admissibility of Digital Evidence: A study

By

1. Aquib Husain

Research scholar, Faculty of Law, Jamia Millia Islamia

2. Dr. Eakramuddin

Associate professor, Faculty of Law, Jamia Millia Islamia

ABSTRACT

Today we are not only living in the shade of technology but under the shadow of technology. Authors in this research paper have endeavored to analyse electronic evidence and the laws governing its admissibility in the courts of law. This article deals with the definition of electronic evidence and the evolution of the laws governing evidence through time. It emphasizes the reliability of electronic records in judicial proceedings and the conditions that make them admissible as evidence in court. The author has tried to show the judicial evolution that has occurred regarding the obligatory nature of sections dealing with the authenticity and thereby admissibility and relevance of electronic evidences. Along-with that this article will also be enumerating the roadblocks that are still faced by the investigative authorities when following the rules provided by the legislations. The author has also, in his humble opinion, provided certain suggestions to better dealing with a sensitive form of evidence and improve the current scenario.

INTRODUCTION

Computers were first introduced in India in 1969 and since then our country has never looked back. The 21st Century has brought with it thrilling metamorphoses and developments in technology in the world and India is no exception to this change. Currently nearly every household has a digital device be it computers or laptops or smart phones even the rural area has not been left out of the digitisation effect. In the age of the cyber-world, computer applications have become a trend, and technological advancements have accelerated. With an

increased reliance on digitalisation every field of life has been affected the good, the bad and the ugly side of life. New avenues have not only opened for the betterment of our lives but also for criminals to expand their "portfolios". But as is wont to happen no work can be done without leaving traces. Just like in real life, criminals tend to leave evidences in the digital world as well.

In light of the above-mentioned situation, the Information Technology Act of 2000, which is based on the Model Law on Electronic Commerce of the United Nations Commissions on International Trade (UNCITRAL), changes were made to make digital evidence admissible. Amendments were also made to the Indian Evidence Act of 1872, the Indian Penal Code of 1860, and the Banker's Book Evidence Act of 1891. These revisions establish the legal framework for transactions that take place in the digital realm. In this article, the examination of electronic evidence is scrutinised in relation to other statutory rules concerning the admissibility of electronic evidence.

DEFINITION OF DIGITAL EVIDENCE

Section 3 of the Evidence Act defines "document" as follows:

> **"***Documentmeans any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter*."[1]

This Section also defines Evidence as:

(1) *"all statements which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry; such statements are called oral evidence*
(2) *all documents* ***including electronic records*** *produced for the inspection of the Court."*

Section 2(t) of the IT Act defines the term "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*;"[2]

Electronic evidence means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data.[3]

DIGITAL EVIDENCE UNDER INDIAN LAWS

THE INFORMATION TECHNOLOGY ACT, 2000

As per **Section 2(1)(o)** data represents information, facts, knowledge, concepts, theories etc that are prepared and processed in computer or similar devices that exist in any form. **Section 2(1)(r)** states that electronic form means any information generated, sent or received or stored in any storage device such as a micro film, computer memory etc. **Section 2(1)(t)** talks about electronic record and has been mentioned above. Lastly

[1]The Indian Evidence Act, 1872, (Act 1 of 1872), s. 3
[2] The Information Technology Act, 2000 (Act 21 of 2000), s. 2(t).
[3]https://www.lawinsider.com/dictionary/electronic-evidence (Last Visited on January 12, 2023)

Section 2(1)(v) states that information also includes *data, message, codes, computer programmes, software, databases, micro films and computer-generated microfiche* among other things like sounds, texts images etc.

All of these sections together give a comprehensive idea of what has been considered to be electronic record.

Section 4 Legal recognition of electronic records

Where it is specified by law that any form of information has to be written or typewritten or printed, then irrespective of any other law in place, such requirement has to be presumed to have been satisfied if the following requirements are fulfilled –

a) The information has been provided/produced/made available in electronic form and
b) Such information is accessible to such extent that it can be referred to later.

The second requirement was laid down with the purpose that electronic data being intangible and transient in nature, it would be beneficial to mandate its availability for future reference.

Section 6 of the IT Act provides for the use of electronic records and electronic signatures in Government and its agencies. It states that any electronic record required to be used as per the rules prescribed by the Government or its agencies for specific purposes such as filing of forms, grant of permits etc. shall be considered satisfied.[4] If such record is considered appropriate as per the Government's prescription it is needless to say that they are considered as admissible evidence in a court of law

Section 79A Provides for the appointment of an Examiner of Electronic Evidence whose opinion is to be considered as relevant as per **Section 45A of the IEA.** As per the Explanation to this section of the IT Act[5], evidence when in electronic form is considered as any information of corroborative, confirmative, or other such probative value that is stored, transmitted, etc in electronic form. Examples of such form of information are computer evidence, digital audio, messaging histories, browser histories, secured electronic signatures data bases, contents of computer memory, computer backup, secured electronic records, emails, call records, etc. All this and many more forms of electronic and digital evidences are thus given admissibility by the Courts during civil and criminal trials.

INDIAN EVIDENCE ACT, 1872

The Indian Evidence Act, 1872, hereinafter referred to as the IEA defines evidence as

(a) witness testimony, which includes oral testimony, and
(b) documented evidence, which includes electronic records prepared for the court's scrutiny. [6]

The phrase "all documents produced for the inspection of the Court" was replaced by "all documents including electronic records produced for the inspection of the Court" in **Section 3** of the IEA by the IT Act,

[4] The Information Technology Act, 2000 (Act 21 of 2000), s. 6.
[5]The Information Technology Act, 2000 (Act 21 of 2000), s. 79A.
[6]Ibid.

2000. Electronic evidence is now referred to as "content of documents or electronic records" rather than "paper content".[7]

When it comes to oral evidence of electronic records, **Section 22A** of the IEA states that oral evidence of the contents of the electronic records will not be considered relevant unless one produces proof of genuineness of the electronic record produced as evidence. Other than the contents of the electronic record, all facts can be proved by oral evidence.[8] Sections 59 and 60 of the Evidence Act while dealing with oral evidence form the basis of the hearsay rule. They state that testimony that is not given by someone with direct and personal knowledge cannot be relied upon. This rule also applies to documents, as the contents of a document cannot be disclosed orally. Oral evidence cannot be used to verify or compare the accuracy of a document's content in the absence of the document. Either primary or secondary evidence must be shown to prove the contents of a document.[9] Taking into account the definition of documents given in IEA, the conditions of Section 60 can be said to be applicable to electronic records as well.

While the document itself is primary evidence[10], it was recognised that there would be times when primary evidence would be unavailable. Witness statements and copies of the document can be used to support the claims. Section 65 of the Evidence Act allows "secondary evidence" to be used in place of primary evidence. There are however, certain circumstances when it will be allowed:

- Is misplaced or ruined.
- Cannot be readily transferred, i.e. produced before courts physically.
- Is a state-issued public document.
- When the law allows it, certified copies can be used to verify it; and it is a compilation of multiple papers.[11]
- Alternatively, the prejudiced party or any of its representatives have proven it.

Section 65: Cases in Which Secondary Evidence Relating to Documents May Be Given

Secondary evidence can be used to support a wide range of documents. This section enumerates the conditions under which secondary evidences are admissible as well the form in which they are to be considered admissible. Situations where the original documents appear to be with the opposite party, or its existence has been admitted by the opposite party, or when the original document is or a nature was to not be easily movable. One such example is that of cell phone records. These are stored on massive servers; it is difficult to move and produce them in court. As a result, under sections 63 and 65, secondary evidence of such recordings should be permitted.

This section also details the form in which secondary evidences are to be produced in order to be considered admissible.

Section 65A: Special Provisions as to Evidence Relating to Electronic Record

[7]The Indian Evidence Act, 1872, (Act 1 of 1872), ss. 65A, 65B

[8]The Indian Evidence Act, 1872 (Act 1 of 1872), s. 59

[9]Anvar v. Basheer and the New (Old) Law of Electronic Evidence - The Centre for Internet and Society, *available at:* https://cis-india.org/internet-governance/blog/anvar-v-basheer-new-old-law-of-electronic-evidence (last visited on January 2, 2022).

[10] The Indian Evidence Act, 1872, (Act 1 of 1872) s. 62.

[11] Stephen Mason, Philip Argy, *et.al.*, *Electronic Evidence* (Lexis Nexis, 3rd Edn., 2012).

Even thought Section 65 deals with the various conditions where secondary evidence can be provided and it can be no doubt interpreted to include electronic evidence, due to the volatile and ambiguous nature of such evidence a need was felt to better clarify the admissibility of electronic records as evidence. As per Section 65A, procedures given under **Section 65B** are to be followed when contents of electronic records are to be proved.[12]

Section 65B: Admissibility of Electronic Records

Section 65B deals with electronic devices, process of recording electronic evidences and the requisite conditions while recording such evidences. Sub-Section 1 of Section 65B defines the computer output. Electronic devices with the capacity to store, process, transmit and produce data or information such as computers, audio-video recorders, pen drives, even parts that compose a computer are considered as electronic evidence and are frequently referred to as "computer output."

Documents such as these will be mandatorily made admissible as evidence. No proof or production of original evidence will be needed if the owner of the device or person responsible for handling such device and recording such evidence provides a certificate under Section 65B(4) of the Indian Evidence Act, 1872. The certificate however, should contain the following:

1. During the recording of evidence whether the computer was in working condition or not
2. Whether it was lawfully used by the owner/operator
3. A description of the regular use of computers.
4. Description of feeding information in any other device in the ordinary course of action
5. Whether the computer was in working condition during the entire period in which information is processed or created or transferred and if so its description
6. Description of all the devices, if and when multiple computers or devices were used to create or process the information in question and considering such group of devices as one single device.[13]

Section 65B (4) specially deals with the fact that a certificate purporting to the following would be considered as evidence admissible in the court of law:

(a) The electronic evidence and the information contained within are identified and the manner of its production is described;

(b) If any devices are involved in the production of such electronic evidence, then appropriate particulars are to be provided to show that the electronic record was produced by a computer;

(c) Matters to which the conditions mentioned in sub-section (2) relate are to be dealt with in the certificate, and 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) must put his/her signature on the document.

[12] Kuberan and Sneha Mahawar, *All you need to know about Section 65 of the Indian Evidence Act, 1872*, available at:https://blog.ipleaders.in/all-you-need-to-know-about-section-65-of-the-indian-evidence-act-1872/#:~:text=Section%2065A%20of%20Indian%20Evidence%20Act%2C%201872,-Section%2065A%20and&text=the%20Main%20objective%20of%20Sections,procedure%20given%20under%20Section%2065B. (Last Visited on January 11, 2023)

[13] Ibid.

It is not binding upon the judge to consider a relevant and admissible fact as being proven. A judge must first fully examine the fact in order to conclude its veracity. This is the general rule. Exceptions to this rule can be found in certain amended provisions of the Evidence Act as well as the IT Act where various presumptions regarding the proof of electronic evidences have been provided. **Section 85B** of the Evidence Act states that a record will be considered a secure electronic record until its verification, if security procedures have been applied to such record at a specific time. Without any contrary proof, the court must presume that such a secure electronic record has not been tampered with since obtaining secure status. Secure digital signatures have been dealt with in**spection 15 of the IT Act**. The rationale behind affixing a secure electronic signature by the subscriber is to show his intent to sign or approve the electronic record. **Section 85C** of the Evidence Act presumes that any information listed in the certificate is correct.

RELEVANCY AND ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIA

As has been mentioned above unlike physical evidence electronic evidence does not have a single storage point. It is not only confined to computers but also to a plethora of other devices, thus making its location a challenge all on its own. A major question that has arisen is why the evidence on an electronic device cannot be produced in printed format on a paper. Three possible reasons have been provided by researchers:

1. Electronic documents are accompanied by extra information that is no visible on the face of the document. A simple example could be that the contents of the document in a printed form to be the information but unless mentioned one cannot find out as to when the document was made or transferred to the source from which it has been printed. And even then, the contents of the documents tweaked to change the date mentioned. Such information is known as metadata. Metadata is defined as information that describes other information in order to help you understand or use it.[14]
2. Electronic records like physical documents must conform to the "Best Evidence Rule." If electronic records are being used to as evidence, then it must be proved that the electronic documents are relevant, authentic, and reliable. It also must not violate the rule against hearsay in order to be deemed admissible. Not only will converting electronic into a physical form create doubts as to the authenticity of the source from where it was taken but also as to the authenticity of the contents itself as its is possible to alter, intentionally or unintentionally, the contents of the document when converting it from one form to another – so much so that the court might be convinced to not accept the contents to be admissible.
3. Another reason put forth is that in the digital era, where most of the evidence generated is electronic, it is time that litigators, and courts assimilate the use of electronic evidence into their trials in their original forms.

India is a common law country where the adversarial form of legal system is followed. The prosecution and defence put their arguments in front of a judge who acts as an unbiased referee to ensure the fair justice is done

[14] https://www.oxfordlearnersdictionaries.com/definition/english/metadata#:~:text=%2F%CB%88met%C9%99d%C3%A6t%C9%99%2F,you%20understand%20or%20use%20it (Visited on January 14, 2023)

to both the aggrieved as well as the accused simultaneously guaranteeing that proper legal procedures are followed. The adversarial system assumes that the best way to get to the truth of a matter is through a competitive process to determine the facts and application of the law accurately.[15]

In this form of legal system production of evidence before the judge becomes a crucial aspect for the court to reach a conclusion. However, in order to be admissible as evidence certain requirements need to be fulfilled. For evidence to be admissible it must be relevant, material, and competent. Electronic evidences are no exception to this rule. Electronic evidence has emerged as one of the fundamental bases for litigation. Judges are often confronted with the question of interpreting rules on admissibility of electronic evidence while determining the fate of the defendant or accused. The various forms of electronic evidence such as data from websites, communications on social media, emails, instant messages, computer generated documents etc. create unique problems and challenges for proper authentication.[16]

As has been mentioned before as per Indian laws, electronic evidence comes within the purview of documents[17] and is treated as a type of secondary evidence. In order to be admissible certain conditions however, need to be followed.[18] Further amendments were made to the Indian Evidence Act, 1872 regarding the conditions of authenticity, reliability, and admissibility of electronic evidence.[19] These amendments were brought about by way of Section 92 of the IT Act, 2000. Section 3 of the Evidence Act was amended to include electronic records as a part of "documents" to be termed as documentary evidence. Similarly, 'electronic records' was also inserted in Section 59 of Indian Evidence Act to include electronic evidence as a part of 'contents of documents." The rules of admissibility for electronic evidence were introduced through Section 65-A and 65-B of the Evidence Act.

It is pertinent to note that the words "document or content of documents" in Section 61- 65 of the Indian Evidence Act were neither amended to "electronic records" nor were these words added. It can be interpreted to mean that these Sections are not meant to be referred to or made applicable when dealing with electronic records.[20]

The objective behind adding special provisions of the IEA for admissibility of electronic evidence is that electronic records are highly technical and need specialised interpreters to read the "language." Such evidence cannot be produced easily in the court of law due to the difficulty in carrying the computers or their servers. Section 65-B of the Evidence Act lays down the rules relating to admissibility of electronic evidence as secondary evidence in the form of computer output comprising of print out or data copied on electronic / magnetic media.

[15] https://www.unodc.org/e4j/en/organized-crime/module-9/key-issues/adversarial-vs-inquisitorial-legal-systems.html (Visited on January 14, 2023)

[16] Archana Sarma, Computer forensics in criminal investigation and admissibility electronic evidence in India, *available at* *https://shodhganga.inflibnet.ac.in/bitstream/10603/351813/8/chapter-3.pdf* (Visited on January 14, 2023)

[17] The Indian Evidence Act, 1872, (Act 1 of 1872), s. 3

[18] The Indian Evidence Act, 1872, (Act 1 of 1872), ss. 63 and 65

[19] The Indian Evidence Act, 1872, (Act 1 of 1872), ss. 65A and 65B

[20] Shobha Gupta, Why is Admissibility and Authenticity of Electronic Records Necessary?, *available at* https://theleaflet.in/why-is-admissibility-and-authenticity-of-electronic-evidence-complicated/ (Visited on January 16 2023)

The first part of Section 65B lays down that any electronic record stored in any form in any device shall be deemed to be a document as per Section 3 of IEA provided certain conditions are fulfilled:

1. The computer where the electronic records are stored should be in regular use.
2. The activity must have been carried out by someone having lawful authority
3. The activity should be done during the period when the computer was in regular use
4. The information should have been entered in the course of day-to-day activities.
5. The computer should have been operating properly during the period in question.

In such case no further proof or production of the original is required.

This section also describes what constitutes a single computer:

1. Multiple computers combined together and operating over that period
2. Different computers operating in succession over that period
3. Different combinations of computers operating in succession over that period

The provisions recognise the evidentiary value of any information printed on paper or stored in a compact disc, or similar device subject to the fulfilment of the Sub-section (4) of section 65B of the Evidence Act which provides additional non-technical qualifying conditions to establish the authenticity of electronic evidence. This provision requires that a certificate shall be produced by a senior person having responsibility of the computer which has created and stored the electronic record. The certificate must uniquely identify the original electronic record, describe the manner of its creation, describe the device that created it, and certify compliance with the technological conditions of sub-section (2) of section 65B.[21]

It has been laid down by the Apex Court that Section 65B is a special provision and is different from Sections 63 and 65 when dealing with secondary evidence.[22] It is a challenge to produce a certificate under Section 65B where the device in which the evidence is stored in in the possession of adverse party. The widespread use of portable devices like mobile, tablets, etc. has created even more diverse challenges for the courts while deciding on the issues of authentication of digital information.

It is of paramount importance that the court assure that the evidence produced before the court of law would form a strong foundation when reaching a decision. Admissibility is a fundamental rule of evidence. It is a set of tests carried out by the court to assess the evidence produced before it. This process may become very difficult if the evidence is not handled properly by the law enforcement agencies. It is specially challenging when the law enforcement authorities are scrambling to keep up with the advancements made in the technical field. Constant updates in their training, keeping track of new and improved systems in nearly every day basis, upgrading devices that were already expensive with even more expensive and complicated devices all contribute towards the strain put on the authorities to keep up.

[21]Supra. Note 17

[22]Anvar P.V v. P.K Basheer, (2014) 10 SCC 473

Due to its intangible nature some evidences are compromised beyond salvation because of which cases sometimes are left unheard in courts.[23] It is essential to ensure that evidence stored or generated in a computer is collected, preserved, maintained, and transmitted in accordance with legal requirements. The processes and rules provided must strictly be followed in order to maintain the admissibility of the evidence collected.

CHALLENGES REGARDING ADMISSIBILITY

There is no argument when it comes to the increased demand of the use of digital evidence in both public and private sectors. This has led to digital evidence being admissible in the courts of law as well. With that has risen the need to maintain strict protocols while handling said electronic evidences in order to enable the courts to reach a decision. There are however, roadblocks that the courts will inevitably face due to the vulnerability of electronic evidences.

Digital evidence specially when in large quantities present a challenge for forensic analysts. A hard drive may contain a mix of important and irrelevant information accumulated over a period. It takes time and effort to extract only the relevant information, arrange them and translate them so they can be interpreted.

Partial View of Information

When a computer receives an instruction through human intervention to perform a task such as sending an email, the resulting activities generate data remnants that give only a partial view of what occurred. Only certain results of the activity such as the e-mail message and server logs remain to give us a partial view of what occurred. Furthermore, using a forensic tool to recover a deleted file from storage media involves several layers of abstraction from magnetic fields on the disk to the letters and numbers that we see on the screen. Hence, the actual data is never visible, but only a representation of the same can be seen.[24]

Difficulty in Pin-pointing the Original Creator

There are times when it becomes difficult to attribute the computer activity to one specific person. Analysts can at most find the point of origin of the information i.e the device in which it was originally created, stored, or sent not as to the individual who did this. Even though there are date and time stamps that may be of some help still they are weak evidences as without supportive or corroborative evidence a particular individual cannot be picked out of the other users.

Easily Manipulated or Altered

It is very easy to manipulate electronic records and is thus pose a challenge for the investigative authorities. In the right hands and with the correct knowledge, electronic records and their devices can be altered, deleted, manipulated, copied, distorted, deleted information can be recovered, and even destroyed.

[23] Samuel Noris, Digital Evidence and Computer Crime, 3rd Ed. *Available at,* https://textbooks.elsevier.com/manualsprotectedtextbooks/9780123742681/Instructor_Manual.pdf(Visited on January 16, 2023)

[24] Archana Sarma, Computer forensics in criminal investigation and admissibility electronic evidence in India, *available at* https://shodhganga.inflibnet.ac.in/bitstream/10603/351813/8/chapter-3.pdf (Visited on January 17 2023)

Unreliable Sources

Electronic evidence gathered from the internet specially from social media sources where people are free to post whatever they want however they want subject to minimal restrictions cannot be considered reliable. Not only this but it has also become easy to fake information in order to lead investigators on a wild goose chase. Using VPNS, faking one's information online - instances such as these many a times lead to creating a doubt as to the exact target of the crime.

Susceptibility to Hacking

In case there are multiple devices interconnected, not only does hacking into one make the other susceptible to being hacked but it also makes it difficult to figure out the point of origin of the hack and the perpetrator behind it.

Rigorous Process for the Authorities

Constantly developing and improving technology has instilled a need for constant vigilance by the investigative authorities in order to keep track. This, however, is a rigorous and arduous process that is difficult to keep up with. Technology and its approach towards it, is changing faster than the authorities can learn about them or prepare for them. New codes, new machines, latest sources, registered as well as unregistered applications and unrestrained access to them have created hurdles for the authorities. The time required for them to update their data and websites, to learn the newest system and to get sanctions for the latest upgradation of devices not only acts as a roadblock but also puts a blemish on their competency.

JUDICIAL APPROACH

One of the first cases to address the matter of admissibility of Electronic Evidence was **State (NCT of Delhi) v. Navjot Sandhu**[25] where the Apex Court held that even if a Certificate under Section 65B of the IEA is not filed it does not mean that secondary evidence cannot be given. It held that law permits such evidence to be given in circumstances mentioned in Section 63 and 65 of the IEA. The court relied on the law under Section 63 stating that secondary evidences include copies made by mechanical processes which ensure the accuracy of the contents. It also compared the rule laid down in Section 65 enabling the production of secondary evidence if the "*original was of such a nature as to not be easily movable"* to the fact that certain electronic records are stored in huge servers that cannot be easily moved. The court made a liberal interpretation of the rule of admissibility for electronic evidence as secondary evidence.

This decision was overruled by a three-judge bench in **Anvar P.V. *v.* P.K. Basheer and Others**[26]whereby it was held by the Apex Court that according to Section 65B of the IEA without compliance no computer output will be admissible. Contradicting Justice Sandhu the Court made the observation that his stance on law of

[25](2005) 11 SCC 600
[26](2014) 10 SCC 473

admissibility of electronic evidence regarding electronic record is liable to be overruled as it does not lay down the correct position of law.

In 2015[27] again the question of admissibility of electronic evidence was dealt with by the Supreme Court of India. The court held that computer – generated electronic records are admissible in a trial if they are proved in the manner specified in Section 65B of the IEA. The court held that "*Electronic documents strictu sensu are admitted as material evidence. With the amendment to the Indian Evidence Act, 2000, Sections 65A and 65B were introduced into Chapter V relating to documentary evidence. Section 65A provides that contents of electronic records may be admitted as evidence if the criteria provided in Section 65B is complied with*."[28]

In **Vikram Singh and Anr. *v.* State of Punjab and Anr.**[29], the Supreme Court held that Certificate under Section 65B is a condition precedent to the admissibility of evidence by way of electronic record, thereby upholding the judgment in *Anvar P.V.* case.

In 2018 a Division Bench of the Supreme Court in **Shafhi Mohammad *v.* The State of Himachal Pradesh**[30] held that requirement of certificate under Section 65B (4) is procedural and can be relaxed in the interest of justice provided a party is not in possession of the device.

Anvar P.V. and *Shahfi Mohammad* cases created contradictory views upon the same subject. In the year 2019, a two-Judge Bench of the apex court referred the matter to a three-judge bench for clarification on the point. In **Arjun Panditrao Khotkar *v.* Kailash Kushanrao Gorantyal and Ors,**[31]the Supreme Court had to interpret Section 65B(4) for determining the mandatory requirement of production of certificate under Section 65B(4) as well as its compliance when it is not possible to get such certificate from the competent authority. Justice Nariman noted that Section 65B (1) separates 'original' electronic records from secondary copies. He states that original electronic records are those that are found in the computer or device where it was first stored whereas secondary copies are those made from said primary electronic records. Original records can be identified directly as evidence if the owner of the device provides enough information to establish that the device where the information is first stored is owned/operated by him. If the electronic record is first stored in a device which forms a part of a "computer network" or "computer system" and it is not possible to bring such a network/system physically to the Court, then secondary copies can be produced along with the certificate stipulated by Section 65B(4).[32] The Court upheld *Anvar's*decision while overruling *Tomaso Bruno's* case and thereby put the controversy to rest once and for all.

CONCLUSION

Finally it is true that India has stepped into a new era the digital era and it has brought with it many changes into our everyday lives. Law has always been a bridge between society and order and thus has had to change with changing times. Many changes have been made to various laws in India in order to adapt to the introduction of electronic technology. However, such changes have not been without their challenges past,

[27] *Tomaso Bruno and Anr. v. State of Uttar Pradesh* (2015) 7 SCC 178
[28] Ibid. Para. 25
[29] (2017) 8 SCC 518
[30] (2018) 2 SCC 801.
[31] 2020 SCC OnLine SC 571
[32] Bharat Vasani & Varun Kumar, Supreme Court on the Admissibility of Electronic Evidence under Section 65B of the Evidence Act *available at* https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/ (Visited on January 18 2023)

present, and future. As is wont to happen no change happens easily there are always past laws to be considered that make perfect sense to many, there are present problems that need to be addressed to create a better future and there is the possibility of today's development being used for tomorrow's crime – bringing to mind the very concept of the ever-entwined yin and yang.New laws may have contributed greatly towards improving the legal approach towards electronic evidence and their reliability, but our system still has a long way to go as there are still many hurdles that need to be crossed by not only the law makers but also those authorities who are responsible for implementing, maintaining, and executing said laws. For now, strict adherence to the existing laws and following the interpretations given by India's Apex Court may be the only way to go.

It would be viable to look into other ways to better the system such as adopting e-governance to the maximum possible extant, holding regular workshops for investigative authorities, holding such workshops in batches so as to minimise the lack of officers in the stations, developing ways to produce devices with the latest upgrades at reasonable rates, increasing awareness among the public, generating employment for those who are well-versed with such technology, holding conventions to create awareness and encourage the youth to strive for a better India and many other ways to refine the current legal position.

International Research Journal
IJNRD
Research Through Innovation