E-EVIDENCING AND ITS ADMISSIBILITY

Written by ***Shashank Mittal***

Senior Legal Counsel, Bharti Airtel Limited, India

INTRODUCTION

Technology has captivated not just India but the whole world in the twenty-first century. The utilization of computers isn't restricted to organizations yet accessible to each person at swipe of a finger. Information Technology has refined each and every human activity. In this time of digital world as the utilization of computers turned out to be better known, there was development in the field of technology. The advancement of Information Technology (IT) brought forth the internet wherein web gives equivalent occasions to all individuals to get to any data, information stockpiling, examine and so on with the utilization of high technology.

This ever-growing reliance on electronic methods for communication, internet commerce, and data storage in computerized structures has unquestionably necessitated a reform in the law governing information technology and the laws governing the admissibility of electronic evidence in all cases in India. The proliferation of computers and the effect of information technologies on society as a whole, as well as the ability to store and collect data in advanced structures, have all necessitated reforms in Indian law to integrate the arrangements on electronic proof evaluation. The Information Technology Act, 2000 and its revision depend on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce. The Information Technology (IT) Act 2000 was amended to consider the admissibility of electronic evidence. Amendments to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 empower the legislative framework to transact in electronic world.

With the amendment in law, Indian courts have established case law on the use of electronic evidence. Judges have also demonstrated an understanding of the inherent "electronic" existence of evidence, which includes knowledge of the admissibility of such proof and the

translation of the law corresponding to how electronic proof can be brought and registered before a court. Digital proof or electronic proof is any probative data stored or communicated in computerized structure that party to a legal dispute may use at court trial. Prior to accepting any evidence, it is indispensable that the assurance of its authenticity, veracity and relevance be discovered by the court and to set up if the fact is hearsay or a duplicate is preferred to the original. Computerized Evidence is "data of probative worth that is stored or communicated in binary structure".

Proof isn't just restricted to that found on electronic devices however may also include proof for computerized gadgets, for example, media transmission or visual device and sound gadgets. The E-Evidence can be found in messages, computerized photos, ATM exchange logs, word processing, archives, text narratives, documents spared from bookkeeping programs, spreadsheets, web program history information databases, contents of computer memory, computer reinforcements, computer printouts, Global Positioning System tracks, Logs from a hotel's electronic entryway locks, digital video or sound records. Electronic Evidence will in general be more voluminous, harder to demolish, handily altered, effortlessly copied, conceivably more expressive and all the more promptly accessible.

MEANING OF ELECTRONIC EVIDENCE

The definition of evidence as given in the Indian Evidence Act, 1872 covers a) the evidence of witness i.e. oral evidence, and b) documentary evidence which includes electronic record produced for the inspection of the court.[i] Section 3 of the Act was amended and the phrase "All documents produced for the inspection of the Court" was substituted by "All documents including electronic records produced for the inspection of the Court".[ii]

Also known as 'electronic evidence', 'digital evidence' or 'computer evidence'. The word digital evidence is especially used where physical-world information is converted to binary numeric form as in digital audio and digital photography. Definitions of digital evidence include 'Information of probative value stored or transmitted in binary form; and 'Information stored or transmitted in binary form that may be relied on in court. Electronic evidence refers to data

(comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.[iii] This definition has three elements:

Firstly, includes all forms of evidence created, manipulated or stored in a product that in the widest meaning, be considered as computer.

Secondly, will include any form of device, whether it is a computer as we presently understand the meaning of a computer; telephone systems, wireless telecommunications systems and networks, such as the Internet; and computer systems that are embedded into a device, such as mobile telephones, smart cards and navigation systems.

Thirdly, restricts the data to information that is relevant to the process by which a dispute, whatever the nature of the disagreement, is decided by an adjudicator, whatever the form and level the adjudication takes. This includes one aspect of admissibility - relevance only - but does not use 'admissibility' in itself as a defining criteria, because some evidence will be admissible but excluded by the adjudicator within the remit of their authority, or inadmissible for reasons that have nothing to do with the nature of the evidence - for instance because of the way it was collected. However, restricts the definition of electronic evidence to those items offered by the parties as part of the fact finding process.[iv]

Electronic Evidence has become a central cornerstone of correspondence, distribution, and reporting as a result of the tremendous increase of e-governance in the public and private sectors, as well as ecommerce operations. Government bodies are opening up to electronic filings to enact different governance measures, as well as annual filings to oversee and monitor sectors. Electronic Evidence/Digital Evidence in different formats is constantly being used in court trials. Judges are often called to comment on the admissibility of electronic proof during the course of a trial, and this decision has a significant effect on the outcome of a civil lawsuit or the conviction or acquittal of the accused. The Court continue to grapple with this new electronic frontier as the unique nature of evidence, as well as the ease with which it can be fabricated or falsified, creates hurdle to admissibility not faced with the other evidences. The

various categories of electronic evidence such as CD, DVD, hard disk/ memory card data, website data, social network communication, email, instant chat messages, SMS/MMS and computer-generated documents poses unique problem and challenges for proper authentication and subject to a different set of views.

CO-RELATION OF THE INFORMATION TECHNOLOGY ACT, 2000 AND THE EVIDENCE ACT, 1872

The concept of "electronic evidence" has been introduced through the Information Technology Act, 2000 ("IT Act") and the related amendments in the Evidence Act, 1872 ("Evidence Act") and the Indian Penal Code, 1860 ("IPC"). The IT Act and its amendment are based on the United Nations Commission on International Trade Law ("UNCITRAL") model Law on Electronic Commerce. According to Section 2(1)(t) of the IT Act, the term "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer-generated micro fiche. Section 4 of the IT Act expressly recognises the validity and use of electronic records in place of ordinary paper-based records.

The Evidence Act was modified by Section 92 of the IT Act, which expanded the definition of "evidence" to include "electronic record," making digital evidence admissible. Sections 63 and 65 of the Evidence Act, which dealt with and provided for the admissibility of electronic evidence prior to its legal acceptance, mostly dealt with and provided for the grounds for admissibility of electronic evidence. Electronic information obtained by different means through applying cyber forensics was called a "fact" under these rules, and written reproductions were considered secondary evidence, requiring authentication of validity by a qualified signatory who was vulnerable to cross-examination relating to the certified paper.

However, the omission of the word, "Electronic Records" in the scheme of Section 61 to 65 of Evidence Act; and the exclusion of electronic record under Section 59 of Evidence Act clearly signifies the clear and explicit legislative intention to not extend the applicability of Sections 59 and 61 to 65 of the Evidence Act to electronic record, in view of overriding provision of

Section 65B of the Evidence Act, which deals exclusively with the admissibility of such electronic record.

ELECTRONIC EVIDENCE – THE INDIAN EVIDENCE ACT, 1872

In Section 59, the terms "Content of papers" have been replaced with "Content of documents or electronic archives," and Sections 65A and 65B have been added to incorporate the admissibility of electronic information. Traditionally, the general law of testimony has been that clear oral evidence, with the exception of records, can be used to prove any facts. The hearsay law states that any oral testimony that is not direct cannot be counted upon until it meets one of the exceptions outlined in sections 59 and 60 of the Evidence Act. In the case of letters, though, the hearsay rule is not as rigid or as clear as it is in the case of oral testimony. Since oral testimony cannot prove the contents of a text, and the document speaks for itself, this is the case. As a result, when a document is missing, oral testimony cannot be provided as to the document's authenticity, and it cannot be linked to the document's contents. This is due to the fact that it will violate the hearsay clause (since the document is absent, the truth or accuracy of the oral evidence cannot be compared to the document). In order to prove the contents of a document, either primary or secondary evidence must be offered.[v]

While the text itself is primary evidence, it was recognized that there would be times when primary evidence would not be available. Thus, under section 63 of the Evidence Act, secondary evidence in the form of authenticated copies of the document, copies produced through electronic processes, and oral accounts by anyone who has seen the document are permissible. Therefore, the provision for allowing secondary evidence in a way dilutes the principles of the hearsay rule and is an attempt to reconcile the difficulties of securing the production of documentary primary evidence where the original is not available. Section 65 of the Evidence Act sets out the situations in which primary evidence of the document need not be produced, and secondary evidence - as listed in section 63 of the Evidence Act - can be offered. This includes situations when the original document

1. Is in hostile possession.

2. Or has been proved by the prejudiced party itself or any of its representatives.
3. Is lost or destroyed.
4. Cannot be easily moved, i.e., physically brought to the court.
5. Is a public document of the state.
6. Can be proved by certified copies when the law narrowly permits; and
7. Is a collection of several documents.

ADMISSIBILITY OF ELECTRONIC RECORDS

The contents of electronic documents can be proven in compliance with Section 65B of the Evidence Act, according to Section 65A of the Evidence Act. As a result, all photographic testimony in the form of an electronic archive can only be proven using the protocol outlined in Section 65B of the Evidence Act. Section 65B of the Evidence Act provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record, whether it be the contents of a document or communication printed on a paper, or stored, recorded, copied in optical or magnetic media produced by a computer, it is deemed to be a document and is admissible in evidence without further proof of the production of the original, subject to satisfaction of the conditions set out in Section 65B(2) - (5) of the Evidence Act.

TECHNICAL AND NON-TECHNICAL ASPECTS

Section 65B of the Evidence Act provides for both technical conditions and non-technical grounds for admissibility of electronic evidence. Sub-section (2) of Section 65B of the Evidence Act lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used. These are:

a) At the time of the creation of the electronic record, the computer that produced it must have been in regular use;

b) The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer;

c) The computer was operating properly; and

d) The duplicate copy must be a reproduction of the original electronic record.

As can be inferred the above conditions relate to veracity of the data. The conditions have a two-fold impact:

i) ensure that there has been no unauthorised use of the data; and
ii) the device was functioning properly, ensuring accuracy and genuineness of the reproduced data.

Sub-section (3) of Section 65B of the Evidence Act is self-explanatory and confirms that if the user has been using a networked device either to store or process information, all the connected devices will be considered to be a single device.

CERTIFICATE OF AUTHENTICITY

Section 65B (4) of the Evidence Act provides for the non-technical conditions being the requirement of a certificate of authenticity. The purpose of the certificate is to satisfy the conditions laid out by the preceding sub-section (2) of Section 65B of the Evidence Act. An individual in a responsible role in relation to the device from which the data was generated must execute/sign the certificate. The certificate must identify the electronic record containing the statement, describe the manner in which it was produced and also give such particulars of any device involved in the production of the electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer. The certificate must also deal with any of the matters to which the conditions for admissibility relate. The entire idea behind the certificate is also to ensure the integrity of the source and authenticity of the data, so that the Court may be able to place reliance on it. This is critical since electronic data is more prone to tampering and alteration.

PRESUMPTIONS UNDER EVIDENCE ACT

In order to allow the use of electronic records, the Evidence Act also allows for such presumptions. The court shall assume that any electronic document purporting to be an arrangement (containing the parties' electronic signatures) was signed by affixing the parties' electronic signatures in accordance with Section 85A of the Evidence Act. In the same way, Section 85B of the Evidence Act allows the Courts to presume that the secure electronic record has not been altered since the specific point of time to which the secured status relates, until proven to the contrary. In addition, Section 85C of the Evidence Act provides for presumption as to the accuracy of information contained in an electronic signature certificate, while Section 81A of the Evidence Act provides for such presumption with respect to Gazettes in electronic forms.

RELEVANCE, GENUINENESS, VERACITY AND RELIABILITY OF ELECTRONIC RECORDS

As the relevance of electronic documents varies depending on the facts and conditions of each case, the genuineness, veracity, and authenticity of digital data remains one of the most difficult issues that courts must address when deciding whether or not electronic evidence is admissible. As a result, it's important that the Courts guarantee the documents aren't tampered with, deleted, or destroyed between the time they're produced to the time they're used in court. Various Indian courts have made rulings about how different electronic media should be used as evidence over time.

1. Statement of Account

Statements of Accounts are governed by Sections 2(8), 2A and 4 of the Banker's Book Evidence Act, 1891 ("Banker's Book Act"). Section 2(8)(c) of the Banker's Book Act also provides that the print-out of an entry in the book of an account should ensure the accuracy of such print-out and contain the certificate in accordance with provisions of Section 2A of the Banker's Book Act. The Reserve Bank of India ("RBI") vide its order no.

RPCD.CO.RF.BC.No. 100/07.38.03/2008-09 dated 24 April 2009 has also directed all State and Central Co-operative Banks to comply with the provisions of the Banker's Book Act while furnishing certified copies and computer printouts to courts[vi]. Thus, a computer print-out of the entries in the book which does not contain certificate as provided under Section 2A of the Banker's Book Act would not be a certified copy within the meaning of Section 2(8) of the Banker's Book Act and would not be then admissible as the original entry itself under Section 4 of the Banker's Book Act. Further, any objection as to the person exhibiting the said statements of account i.e. an objection to the mode of proof and not admissibility, has to be taken at the time of exhibition of the documents[vii].

Interestingly, a printout of statement of account, duly certified by a responsible official of the bank along with a certificate under Section 65B of the Evidence Act has also been recognized by Courts as sufficient proof to lead such statements into evidence. It has been further clarified that merely because the printout is being filed as secondary evidence along with the necessary certificate, does not make it any less valid. In case of Bank statements, the certificate given by the authorized representative of the bank under Section 65B of the Evidence Act is adequate and supports the statement of account relied upon by banks.[viii]

2. E-mail

E-mail is one of the most commonly utilized electronic media for transmission of information. With most formal interactions between people taking place through e-mails, the Courts in India have allowed such e-mails to be admissible in evidence upon filing of a printout of the e-mails along with the certificate under Section 65B of the Evidence Act.[ix]

The certificate under Section 65B of the Evidence Act ought to specify that the computer during the relevant period was in the lawful control of the person proving the e-mail and that information was regularly fed into the computer in the ordinary course of the activities. Further, it is also important to state that the computer was operating properly and the contents printed on paper are derived from the information fed into the computer in the ordinary course of activities.[x]

Upon satisfying the aforementioned criteria, e-mails can be read into evidence in view of the presumption under Section 88A of the Evidence Act regarding the veracity of the contents of an electronic message, until specifically rebutted.[xi] However, this Section does not provide for any presumption as to the sender of the e-mail. Therefore, until and unless a party establishes as to who was the sender, a print out of an email cannot be given much importance.[xii]

3. SMS / instant messaging applications such as WhatsApp

Unlike e-mails, which are typically used for official correspondence, short message service (SMS) or instant messaging apps such as WhatsApp are widely used for both official and unofficial communications. Unlike standard computers, though, a cell phone that is readily available can be used as evidence. As a result, there will be no need to file a certificate under Section 65B of the Evidence Act in situations where the computer carrying the letter and/or instant message shared on WhatsApp or some other similar application is presented in court. However, in all situations, it is important to ensure there is no dispute over the device's ownership or any content changes.

The Hon'ble High Court of Telangana while drawing a comparison between a computer and a mobile phone has held that by the very definition of computer and computer network as defined in IT Act, a cell phone is a computer which is programmed to do among others the function of receiving digital audio signals, shall be construed to be a computer.[xiii]Therefore, in cases where the mobile phone containing the SMS or WhatsApp cannot be led into evidence, a certificate under Section 65B would be required to be filed by the person, who has received or sent the SMS / WhatsApp message. Although Indian courts are yet to independently rule on the admissibility of WhatsApp messages as evidence, it is wise to ensure proper cell phone custody. Since such communications would be subject to judicial review, it is therefore critical to ensure that no evidence has been tampered with, as this may jeopardize the messages' evidentiary value.

4. Hard-disk

A computer's hard disc is the primary storage device for all data. As a result, while acknowledging its value as an electronic proof, the Hon'ble Delhi High Court has explained

that a hard disc would be a mere electronic storage unit like any other computer hardware as long as nothing is written on it and it is not subjected to any alteration. However, after a hard disc has been changed, and though it is returned to its original state by restoring the change, the information about the two stages, including the change and its reverse, will be stored in the hard disk's subcutaneous memory and can be recovered using software built for that purpose.

Therefore, a hard disk that is once written upon or subjected to any change is itself an electronic record even if does not contain any accessible information at present. In this regard, the Courts have noted that there could also be active information available on the hard disk which is accessible and convertible into other forms of data and transferable to other electronic devices. The active information would also constitute an electronic record.[xiv]

5. Call Records

Most criminal investigations often commence from an analysis of the call records of the accused. Such call records are often useful as a starting point for also establishing conspiracy with other individuals. While noting that call records are stored in huge servers which cannot be easily moved and produced in the court, the Hon'ble Supreme Court has held that printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service-providing company can be led in evidence through a witness who can identify the signatures of the certifying officer or otherwise speak of the facts based on his personal knowledge. Further, irrespective of the compliance with the requirements of Section 65B of the Evidence Act, there is no bar to adduce secondary evidence under Sections 63 and 65 of the Evidence Act[xv].

6. Tape Recordings

Often parties record conversations with others, in order to utilize the same as evidence in trials. While the Courts have consistently held that such recordings shall constitute a 'document' under Section 3 of the Evidence Act, it is important that the voice of the person alleged to be speaking is duly identified by the maker of the record or by others who know it.[xvi] In addition, the accuracy of what was actually recorded had to be proved by the maker of the record and satisfactory evidence, direct or circumstantial, has to be there so as to rule out possibilities of

tampering with the record.[xvii] However, while dealing with a case of transcription of recorded conversations, the Courts have clarified that without the actual audio recording being made susceptible to analysis, no reliance can be placed on transcriptions of audio recordings[xviii].

7. Photographs

In the vast majority of cases, the digital camera is not created in court, and a party must rely on a printout or other recording media such as CDs, USB Drives, and so on. As a result, the person in charge of managing the digital camera, as well as taking the snapshot and transferring it to the storage medium, must certify that the printout or storage was managed appropriately. This is has been further clarified by the Hon'ble Delhi High Court by stating that when the party deposes that he took the photographs himself, got them developed and filed them in the Court; the non-filing of negatives cannot be a ground to reject them, especially when the photographs so relied upon are digital photographs.[xix]

8. Compact Disc (CD)

The Courts while dealing with the admissibility of a compact disc containing audio recordings have held that amended definition of "evidence" in Section 3 of the Evidence Act read with the definition of "electronic record" in Section 2(1)(t) of the IT Act, include a compact disc.[xx] Therefore, upon filing a certificate under Section 65B, a CD is admissible in evidence. However, in the absence of filing such evidence, the CD cannot be read into evidence.

The Hon'ble Delhi High Court has held that in a case where a CD is a copy obtained by the mechanical/electronic process of having the original tape recorded conversation uploaded on a computer from the original electronic record and copied on the CD, it shall constitute secondary evidence under section 63 of the Evidence Act and therefore, can be used only upon production of the original record of such taped conversation under section 65B of the Evidence Act.[xxi] Similarly, the Hon'ble Punjab & Haryana High Court has held that in a case where there is no link between the CD and memory chip that was said to have been the source for replication of data in CD; if the CD cannot stand test of authenticity by its comparison with its hash value with source, then transcript of what had been obtained through its audio footage shall not be of any value.[xxii]

USE OF ELECTRONIC MEDIA IN OTHER JUDICIAL PROCEEDINGS

In addition to electronic records being led in evidence, there has also been an increase in reliance on electronic media for other purposes in judicial proceedings. While recognizing the advantage of electronic media such as emails, WhatsApp messages, etc., the Supreme Court has encouraged parties / their advocates to serve the counter party through e-mail, in addition to the usual modes of service[xxiii] in commercial litigation and litigation wherein interim relief is prayed for. A similar view has also been taken by the Hon'ble Bombay High Court[xxiv]. In the recent times, even service through WhatsApp has been recognized by the Hon'ble Delhi High Court[xxv] and the Hon'ble Bombay High Court[xxvi].

ADMISSIBILITY OF ELECTRONIC RECORDS AS AN EVIDENCE

The right to privacy is a well-known human right that is jeopardized when it comes to electronic data processing methods. There is a violation of right to privacy where computer data is obtained by breaching or breaking passwords on someone's personal devices, when the act of cracking or breaking passwords on someone's personal devices allows one unauthorized access to someone's personal information as well. Access to someone's personal information can lead to a variety of other crimes, including fraud, blackmail and extortion, sexual harassment, and so on.

LOOPHOLES IN USING ELECTRONIC EVIDENCES IN THE LONG RUN

The digitalization of our country and the exponential development of technologies are the primary drivers of proof recording and legal reforms. The method of recording electronic documentation poses not only ethical concerns, but also social concerns. For most of us, our mobile phone holds a wealth of knowledge about many facets of our lives, and social media is the place where people express their feelings and meaningless everyday activities. In recent years, the media has placed a greater emphasis on the collection of electronic data. The use of

knowledge derived from social media is the most relevant subject on which the media is attempting to rely further. As a result, current issues and potential concerns of electronic proof must be discussed. It is necessary to establish a regulatory structure, to address various legal issues in various jurisdictions, and to consider potential challenges. The key issues are as follows:

(1) e-discovery and e-disclosure are tools for gathering and producing facts in court;

(2) The validity, admissibility, and trustworthiness of electronic proof submitted in court; and

(3) The use of social media and emoji in court, as well as the analysis and review of electronic data provided in court.

There are several challenges that can be made to the authenticity of digital records:

1. Identity Management Challenge:

Who Created the Records and Who Is the Author? This is the major concern. The author of the digital material offered into testimony is sought in a variety of forms by courts. It is critical for the proponent to provide testimony on who the author is, whether the letter, text, film, or photo was posted on a website.

The next question that arises that - Is the computer program that created the various documents trustworthy? Was the computer's performance as accurate as it should have been? Were the documents tampered with, corrupted, or destroyed after they were made? Photographs and images can be altered using various Photoshop websites and graphic design applications, while hackers can modify websites, databases, and other electronic media. They usually hide their trails by altering audit log data.

2. Information from Social Media Sites:

Because of the endless number of people who use social media sites like Facebook, Myspace, and LinkedIn, content has been generated that is beyond the reach of any one individual or organization. In addition, courts typically extend a higher requirement to the authentication of information from social networking networks where there are no restrictions on who can build a profile. Courts cannot always assign a single post to the person who owns the site since

anybody can build a social network profile anonymously. It's tough to figure out who wrote the post because it can be done on a public machine, such as one in a library or a hotel.

Lack of clarity in difference between Primary and Secondary Evidence: By incorporating all types of computer proof in the scope of primary evidence, the act effectively blurs the line between primary and secondary forms of evidence. Since the data derived by computer-generated records is complex and cannot be readily produced in physical form, an allowance has been made for it. As a result, it would be a good case to argue that if the word document is the original, then a printout of the same can be viewed as secondary evidence. However, it can be noted that creating a word document in court without the use of printouts or CDs is almost impossible.

Unfairly Prejudicial: The term prejudicial refers to a tendency to persuade based on historical experiences rather than real facts of the situation at hand. Proof that is detrimental, injurious, or skewed in favour of the case without establishing any valid facts or enraging the judge without presenting some material facts is often exempt from court proceedings. A child's photograph, for example, wrapped around the victim's neck.

Wastes Time: At court cases, attorneys defending their clients often offer testimony or witnesses that may waste the Court's time; however, those witnesses or evidences are usually omitted from the proceedings. For eg, it is a waste of time for the Court where the advocate would produce twenty different individuals to show that the accused is a trustworthy individual.

Misleading: If the testimony shown is diverting the jury's or judge's interest away from the core topic or substance of the prosecution, it is called false evidence and should be removed from the trial. For example, a minor's gender in a case of rape is irrelevant because the main fact to be established is whether rape was conducted or not on the minor and it is not important to know whether the minor was of which gender.

Hearsay evidence: When an individual is not directly present but has knowledge of an incident from someone else, this is known as hearsay testimony. Such testimony is inadmissible in court and everyone would fault the other one for rescuing the accused or allowing them to avoid prosecution. For example, if witness 'A' claims that another witness 'B' said the defendant hit

the victim with a stick and the prosecutor wants to use the testimony to prove that the defendant hit the victim, that testimony is considered as hearsay.

Character: To prove the character of the defendant the evidence produced by the plaintiff party has certain traits which are excluded from the court proceedings unless the defendant introduces the evidence of **character first in the hearing.**

Expert Testimony: Expert testimony is only admissible in court when it is originally given by an expert and not by a layman. A layman's testimony is not admissible in court.

Privileges: The Court does not admit any kind of privilege information obtained by any attorney-client privilege as well as any other information which is self-incriminating. Such information is confidential in nature and would perjure the attorney and is inadmissible in the court of law.

SOME IMPORTANT JUDGEMENTS

Anvar P.V. Versus P.K. Basheer & Ors[xxvii]

With this significant judgment in the year 2014, the Supreme Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and also the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible.

The judgment would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anticorruption where the reliance is being placed on the audio-video recordings which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD are being forwarded without a certificate U/s 65B Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as

to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. It was further observed that all these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice. In the anticorruption cases launched by the CBI and anticorruption/Vigilance agencies of the State, even the original recording which are recorded either in Digital Voice Recorders/Mobile Phones are not been preserved and thus, once the original recording is destroyed, there cannot be any question of issuing the certificate under Section 65B(4) of the Evidence Act. Therefore, in such cases, neither CD/DVD containing such recordings are admissible and cannot be exhibited into evidence nor the oral testimony or expert opinion is admissible and as such, the recording/data in the CD/DVD's cannot become a sole basis for the conviction.

In the aforesaid Judgment, the Court has held that Section 65B of the Evidence Act being a 'not obstante clause' would override the general law on secondary evidence under Section 63 and 65 of the Evidence Act. The Section 63 and Section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65A and 65B of the Evidence Act. The Constitution Bench of the Supreme Court overruled the judgment laid down in the State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru[xxviii] by the division bench of the Supreme Court. The court specifically observed that the Judgment of Navjot Sandhu supra, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this Court, does not lay down correct position and required to be overruled.

The only options to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence court or it's copy by way secondary evidence U/s 65A/65B of Evidence Act. Thus, in the case of CD, DVD, Memory Card etc. containing secondary evidence, the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

Relying upon the judgment of Anvar P.V. supra, while considering the admissibility of transcription of recorded conversation in a case where the recording has been translated, the Supreme Court held that as the voice recorder had itself not subjected to analysis, there is no point in placing reliance on the translated version. Without source, there is no authenticity for the translation. Source and authenticity are the two key factors for electronic evidence**. Sanjaysinh Ramrao Chavan Vs. Dattatray Gulabrao Phalke**[xxix]**.**

The Hon'ble High Court of Delhi, while deciding the charges against accused in a corruption case observed that since audio and video CDs in question are clearly inadmissible in evidence, therefore trial court has erroneously relied upon them to conclude that a strong suspicion arises regarding petitioners criminally conspiring with co-accused to commit the offence in question. Thus, there is no material on the basis of which, it can be reasonably said that there is strong suspicion of the complicity of the petitioners in commission of the offence in question. **Ankur Chawla Vs. CBI**[xxx]

The Hon'ble High Court of Calcutta while deciding the admissibility of email held that an email downloaded and printed from the email account of the person can be proved by virtue of Section 65B r/w Section 88A of Evidence Act. The testimony of the witness to carry out such procedure to download and print the same is sufficient to prove the electronic communication**. Abdul Rahaman Kunji Vs. The State of West Bengal**[xxxi]**.**

In the recent judgment pronounced by Hon'ble High Court of Delhi, while dealing with the admissibility of intercepted telephone call in a CD and CDR which were without a certificate u/s 65B Evidence Act, the court observed that the secondary electronic evidence without certificate u/s 65B Evidence Act is inadmissible and cannot be looked into by the court for any purpose whatsoever. **Jagdeo Singh Vs. The State and Ors**[xxxii]**.**

In another important judgment of Delhi High Court in the matter of **Dharambir Vs. CBI**[xxxiii] has held that compliance to Section 65B is mandatory and the accused is entitled to the active accessible information as well as subcutaneous memory thus, mirror image of the electronic media where the data is originally stored.

Section 65B of Indian Evidence Act and Section 69 of The Police and Criminal Act, 1984 of U.K. have substantially the same effect. The Law Commission in England reviewed the law relating to computer generated evidence and observed in its report that Section 69 fails to address the major causes of inaccuracy in computer evidence and Section 69 has been repealed by Section 60 of the Youth Justice and Criminal Evidence Act, 1999. And common law presumption "in the absence of evidence to the contrary the court will presume that mechanical instruments were in order at the relevant time", operates with full force. **State Vs. Mohd. Afzal and Ors.**[xxxiv] Similar situation have been emerged in India requiring the necessary amendments in the provision relating to the Digital Evidence.

ENDNOTES

[i] Sec. 3 of the Indian Evidence Act, 1872. "Evidence" means and includes — (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;] such documents are called documentary evidence.
[ii] The amendment to the Indian Evidence Act, 1872 has been made by virtue of Sec. 92 of Information Technology Act, 2000.
[iii] Electronic Evidence and its Challenges by Dr. Swaroopa Dholam
[iv] Burkhard Schafer and Stephen Mason, the characteristics of electronic evidence in digital format, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013.
[v] Anvar v. Basheer and the New (Old) Law of Electronic Evidence - The Centre for Internet and Society
[vi] RBI Notification- The Bankers' Books Evidence Act, 1891 - Submission of Certified Copies of Entries / Print out to Courts
[vii] *Om Prakash v Central Bureau of Investigation (CBI)*, 2017 SCC OnLine Del 10249
[viii] *M/s ICICI Bank Limited v Gurdev Singh*, 2018 SCC OnLine Del 6934
[ix] *Abdul Rahaman Kunji v. The State of West Bengal* 2014 SCC OnLine Cal 18816
[x] *Babu Ram Aggarwal v Krishan Kumar Bhatnagar & Ors*. 2013 SCC OnLine Del 324.
[xi] *M/s. Xact Studio International v M/s. Liwona SP. Z.O.O* 2018 SCC OnLine Del 9469
[xii] S. Karunakaran v Srileka 2019 SCC OnLine Mad 1402
[xiii] *Syed Asifuddin v State of Andhra Pradesh* 2005 SCC OnLine AP 1100
[xiv] *Dharambir v Central Bureau of Investigation* 2008 SCC OnLine Del 336
[xv] *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600
[xvi] *R.M. Malkani v State of Maharashtra* (1973) 1 SCC 471
[xvii] *Shamsher Singh Verma v State of Haryana* (2016) 15 SCC 485.
[xviii] *Sanjaysinh Ramrao Chavan v Dattatray Gulabrao Phalke* (2015) 3 SCC 123
[xix] *Puneet Prakash v Suresh Kumar Singhal & Anr* 2018 SCC OnLine Del 9857
[xx] *K.K. Velusamy v N. Palanisamy* (2011) 11 SCC 275
[xxi] *Havovi Kersi Sethna v Kersi Gustad Sethna* 2011 SCC OnLine Bom 120
[xxii] *Ram Kishan Fauji v State of Haryana*, 2015 SCC OnLine P&H 5058
[xxiii] *Central Electricity Regulatory Commission v National Hydroelectric Power Corporation Ltd. & Ors*. (2010) 10 SCC 280
[xxiv] *Dr. Madhav Vishwanath Dawalbhakta v M/s. Bendale Brothers* 2018 SCC OnLine Bom 2652

[xxv] *Tata Sons Limited & Ors. v John Doe(s) & Ors* 2017 SCC OnLine Del 8335
[xxvi] *SBI Cards & Payments Services Pvt. Ltd. v Rohidas Jadhav* 2018 SCC OnLine Bom 1262
[xxvii] MANU/SC/0834/2014
[xxviii] [(2005) 11 SCC 600]
[xxix] MANU/SC/0040/2015
[xxx] MANU/DE/2923/2014
[xxxi] MANU/WB/0828/2014
[xxxii] MANU/DE/0376/2015
[xxxiii] 148(2008)DLT289
[xxxiv] MANU/DE/1026/2003