“RELEVANCE OF ELECTRONICS EVIDENCE”

DISSERTATION

SUBMITTED IN THE PARTIAL FULFILMENT FOR THE DEGREE OF

MASTER OF LAW’S (LL.M)

SESSION: 2019-2020

UNDER SUPERVISION OF:

Ms.SONALI YADAV

(Associate Professor)

School of Legal Studies, BBDU

SUBMITTED BY:

KAMNA MISHRA

ROLL No.: 1190997026

School of Legal Studies, BBDU

BABU BANARASI DAS UNIVERSITY LUCKNOW

DECLARATION

Title of Project Report "**Relevance of Electronics Evidence",** I understand what plagiarism is and am aware of the University's policy in this regard. **KAMNA MISHRA.**

I declare that,

(a) The work submitted by me in partial fulfilment of the requirement for the award of degree **LLM** Assessment in this **DISSERTATION** is my own; it has not previously been presented for another assessment.

(b) I declare that this **DISSERTATION** is my original work. Wherever work from other source has been used, all debts (for words, data, arguments and ideas) have been appropriately acknowledged.

(c) I have not used this work previously produced by another student or any other person to submit it as my own.

(d) I have not permitted, and will not permit, anybody to copy my work with the purpose of passing it off as his or her own work.

(e) The work conforms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Date: ……

KAMNA MISHRA

University Roll No.-1190997026

LL.M. (2019-2020)

CERTIFICATE

This is certified that **Ms. Kamna Mishra,** Student of LL.M. II Semester **ROLL NO.** 1190997026, **Babu Banarasi Das University, Lucknow** has written dissertation entitled "**RELEVANCE OF ELECTRONICS DEVICES",** under my supervision. To the best of my knowledge this dissertation embodies the authentic and genuine work done by her and findings put forth in the dissertation are his own, formulated after perusal of primary and secondary resources cited in this dissertation.

(**Ms. SONALI YADAV**.)
Associate Professor
School of Legal Studies

ACKNOWLEDGEMENT

I acknowledge the heartfelt thanks to the School of Legal Studies, **Babu Banarasi Das University**, to provide me the opportunity to complete my dissertation for the Partial Fulfillment of the Degree in Master of Law.

I am thankful to my Supervisor Prof. **Ms.Sonali Yadav**, for not only helping me to choose the dissertation topic but also for his valuable suggestions and co-operation till the completion of my dissertation. She provided me every possible opportunity and guidance and being a support in completing my work.

I also thank to all the respondents without whom this study would have never been completed. I

am thankful to everyone from core of my heart.

Kamna Mishra
LL.M. (Criminal and Security Law)
Roll No.-1190997026
School of Legal Studies, BBDU

ABBREVIATIONS

1. ACJ	Accidents Claims Journal,
2. ACC	Accidents Compensation Cases
3. AJR	Accidents Judicial Reports
4. AI Hin L Rtr	All India Hindu Law Reporter
5. AILLR	All India Land Law Reporter
6. AIR	All India Reporter
7. AIR (SC)	All India Reporter (Supreme Court)
8. All Cr LJ	Allahabad Criminal Law Journal
9. BC	Banking Cases
10. CLR	Calcutta Law Reporter
11. CAR	Criminal Appeal Reporter
12. CLC	Criminal Law Cases
13. HCJ	High Court Judgments (Hindi)
14. CJI	Chief Justice of India
15. IPS	Indian Police Service
16. SC	Supreme Court
17. Art.	Article
18. SCC	Supreme Court Cases
17. Cr.P.C	Criminal Procedure Code
18. C.P.C	Civil Procedure Code
20. ILR	Indian Law Reporter
21. IEA	Indian Evidence Act
22. S.C.J.	Supreme Court Journal
23. UJ	Unreported Judgements
24. Vol.	Volume

TABLE OF CONTENT

CHAPTER-I

1. INTRODUCTION:

Today, virtually every crime has an electronic component in terms of computers and electronic technology being used to facilitate the crime. Computers used in crimes may contain a host of evidence related to the crime, whether it is a conventional crime or a terrorist act. In light of this, judicial officers should not become complacent with individuals or their environment simply because the crime may involve a computer. Judiciary should provide assurance to litigants, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. The influence of electronic media has been spread over all branches of society including law and the judiciary.

Maintaining the integrity of electronic evidence throughout the process of investigation and trial presents different problems from the handling of traditional physical or documentary evidence. Some common problems are greatly exacerbated by the complexity of networked computers. This article does not address the unique issues resulting from networked environments but focuses on selected issues of maintaining the integrity of information taken from stand-alone electronic media. Electronic documents are easy to manipulate: they can be copied, altered, up-dated, deleted (deleted does not mean expunged) or intercepted.

The judge must be able to understand and appreciate that the information obtained from the media is a true and accurate representation of the information originally contained in the media irrespective of whether the acquisition was done entirely by law enforcement or in part or entirely by a civilian witness or victim.

This article does not contain interpretation of any existing law. But it gives idea to interpret those provisions related to electronic evidence.

1.1.2 Meaning of electronic evidence

The type of evidence that we are dealing with has been variously described as 'electronic evidence', ' Electronic evidence' or 'computer evidence'. The word Electronic is commonly used in computing and electronics, especially where physical-world information is converted to binary

numeric form as in Electronic audio and Electronic photography.[4] Definitions of Electronic 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. While the term ' Electronic' is too wide, as we have seen the use of 'binary' is too restrictive, because it only describes one form of data. Electronic evidence: data (comprising the output of analogue devices or data in Electronic 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.[1] This definition has three elements. First, it is intended to include all forms of evidence that is created, manipulated or stored in a product that can, in its widest meaning, be considered a computer, excluding for the time being the human brain. Second, it aims to include the various forms of devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition 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. The third element 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 part of the definition 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. The last criteria, however, restricts the definition of electronic evidence to those items offered by the parties as part of the fact finding process.[2]

Due to enormous growth in e-governance throughout the Public & Private Sector and ecommerce activities Electronic Evidence have involved into a fundamental pillar of communication, processing and documentation. The government agencies are opening up to introduce various governance policies electronically and periodical filings to regulate and control

[1] Ibid.

[2] Burkhard Schafer and Stephen Mason, The characteristics of electronic evidence in digital format, in Electronic Evidence, Edited by Stephen Mason, LexisNexis, 2013

the industries are done through electronic means. These various forms of Electronic Evidence/ Electronic Evidence are increasingly being used in the judicial proceedings. At the stage of trial, Judges are often asked to rule on the admissibility of electronic evidence and it substantially impacts the outcome of civil law suit or conviction/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.

1.1.3 What is meant by electronic evidence:

The type of evidence that we are dealing with has been variously described as 'electronic evidence', ' Electronic evidence' or 'computer evidence'. The word Electronic is commonly used in computing and electronics, especially where physical-world information is converted to binary numeric form as in Electronic audio and Electronic photography.

Definitions of Electronic 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. While the term ' Electronic' is too wide, as we have seen the use of 'binary' is too restrictive, because it only describes one form of data.

Electronic evidence : data (comprising the output of analogue devices or data in Electronic 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.

This definition has three elements. First, it is intended to include all forms of evidence that is created, manipulated or stored in a product that can, in its widest meaning, be considered a computer, excluding for the time being the human brain. Second, it aims to include the various

forms of devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition 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. The third element 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 part of the definition 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. The last criteria, however, restricts the definition of electronic evidence to those items offered by the parties as part of the fact finding process.

1.1.4 Types of evidence available on a computer:

An Electronic evidence specialist can make a range of Electronic evidence available from a computer. This section provides an outline of some types of evidence that can be gleaned.

(a) FILES AND LOGS:

A wide range of application software is used on a computer, including programs that enable a user to prepare spreadsheets, databases, text documents, graphic files, multimedia and presentations. The files themselves include Electronic evidence, as do system logs. A great deal of data can be retrieved, depending on the method of storage, the media it is stored on and how the device manages data storage.

(b) DOCUMENTS AND FILES CREATED OR MODIFIED BY THE USER :

Files containing text can be searched for keywords; forensic tools can then be used to view the ‘metadata’: that is, the data that describes or interprets the meaning of data. The metadata can include information such as the storage location of the file on the disk, the last user to modify the file, and the date and time the file was originally created.

(c) SYSTEM AND PROGRAM FILES:

A system file in computing is a critical computer file without which a computer system may not operate correctly. These files may come as part of the operating system, a third-party device driver or other sources. Specific example of system files include the files with .sys filename extension in MS-DOS and Windows, the System suitcase on Mac OS and the files located in sys, the root folder of the Linux file system.

Program Files is the directory name of a standard folder in Microsoft Windows operating systems in which applications that are not part of the operating system are conventionally installed. Typically, each application installed under the 'Program Files' directory will have a subdirectory for its application-specific resources.

(d) TEMPORARY FILES AND CACHE FILES:

When a computer connects to the Internet, a range of information is recorded and retained in different locations, including a list of the websites that have been visited. Temporary files of websites that have been visited are stored in cache folders.

(e) DELETED FILES:

File systems keep a record of where data are located on a disk. The way data are stored will differ, depending on the operating software and the architecture of the method used to allocate blocks of storage for files. In simple terms, the location of data on a disk is controlled by a file system.

(f) NETWORKS:

Gone are the days when most computers stood alone on a desk. The majority of computers are now connected, or are intermittently connected, to some form of network. The trials left by the assortment of logs and files in computers can produce Electronic evidence in abundance, including use of email, connecting to the Internet and viewing websites, and the transfer of files between computers. Other sources of Electronic evidence can be obtained from server.

1.1.5 Types of network -

(a) Internet - The Internet is a global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link several billion devices worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to-peer networks for file sharing.

(b) Corporate intranets - An intranet, usually run by a large organisation, is a network that is based on the Internet protocols. In Principle, an intranet is only available to members, employees or others with authorisation to enter it and use the information contained on the intranet.

(c) Wireless networking - Wireless networking is also known as Wi-Fi meaning wireless fidelity. (d) Cellular networks - The technology that enables devices to transfer data between a computer and a cellular telephone, and between cellular telephones, is developing rapidly. (e) Dial-up - Occasionally, computers are still connected to the Internet by means of the traditional copper telephone line.

I. DATA DESTRUCTION:

Data destruction is the most obvious and most widely discussed anti-forensics measure, and has created a considerable legal and technological debate. Unlike a physical object or piece of paper that can be destroyed effectively, it is much more difficult to obliterate a document in electronic format. All a user does when they click the 'delete' icon on a computer is, in general terms, remove the pointer to the data. The document or data remains, and it is possible to retrieve this data in certain circumstances, even if it is partly overwritten.

II. FALSIFYING DATA:

Tampering with evidence is not new. An early example of erasing part of a tape recording and re-recording part of a conversation occurred.

Such attempts to adduce fraudulent evidence before a court are rare, but increasing. However, it is conceivable, given the ease with which electronic data is so easily manipulated and altered, that attempts will be made in the future to falsify and alter documents before a trial takes place.

III. HIDING DATA:

Tampering with and destroying data work best when the criminal no longer needs the data. For possession crimes such as the possession of illegal images, this is not possible. Hiding the data rather than destroying or altering it therefore, becomes an important objective. Cryptography is the best known anti-forensic method to hide data from third parties.

1.1.6 Guidelines for handling Electronic evidence:

Step 1. Identifying Electronic evidence:

Evidence discovered in Electronic format may be the first sign that something is wrong. For instance, a security administrator to a bank might consider an investigation may be needed where the intrusion detection system sets off an alarm, or where the email logs indicate that a particular member of staff is receiving an excessive number of emails during a day or over an extended period.

In such a case, the source and reliability of the information needs to be assessed, which requires an investigation into the facts.

Step 2. Gathering Electronic evidence:

Once it has been established that it is necessary to seize or gather evidence in Electronic format, a further set of procedures should be in place to guide the Electronic evidence specialist in respect to the scene itself, including the identification and seizure of the evidence if necessary.

It is important not to permit anybody to disturb the hardware or the network, or work on a computer that is liable to being seized and retained, and it is admissible that the police officers that are engaged in searching for Electronic evidence should be properly trained. Data can be

Deleted on a remote server or cloud storage before it can be secured. There are two fundamental principles in relation to copying Electronic evidence that an Electronic evidence specialist should be aware of:

(a) The process of making the image should not alter the original evidence. This means that the appropriate steps should be taken to ensure that the process used to take the image should not write any data to the original medium.

(b) The process of copying data should produce an exact copy of the original. Such a reproduction should allow the specialist to investigate the files in the way they that existed on the original medium.

1.1.7 Electronic evidence and the Indian evidence act 1872

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.[3] 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".[4] Regarding the documentary evidence, in Section 59, for the words "Content of documents" the words "Content of documents or electronic records" have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence. Traditionally, the fundamental rule of evidence is that direct oral evidence may be adduced to prove all facts, except documents. The hearsay rule suggests that any oral evidence that is not direct cannot be relied upon unless it is saved by one of the exceptions as outlined in sections 59 and 60 of the Evidence Act dealing with the hearsay rule. However, the hearsay rule[5] is not as restrictive or as straightforward in the case of documents as it is in the case of oral evidence. This is because it is settled law that oral

[3] Section 3 of the Indian Evidence Act, 1872.
[4] The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000.
[5] Hearsay evidence is anything said outside a court by a person absent from a trial, but which is offered by a third person during the trial as evidence. The law excludes hearsay evidence because it is difficult or impossible to determine its truth and accuracy, which is usually achieved through cross examination. Since the person who made the statement and the person to whom it was said cannot be cross examined, a third person's account of it is excluded. There are a few exceptions to this rule which need no explanation here.

evidence cannot prove the contents of a document, and the document speaks for itself. Therefore, where a document is absent, oral evidence cannot be given as to the accuracy of the document, and it cannot be compared with the contents of the document. This is because it would disturb the hearsay rule (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.[6]

While primary evidence of the document is the document itself, it was realized that there would be situations in which primary evidence may not be available. Thus secondary evidence in the form of certified copies of the document, copies made by mechanical processes and oral accounts of someone who has seen the document, was permitted under section 63 of the Evidence Act for the purposes of proving the contents of a document. 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.[7?]

1.1.8 Electronic document

As documents came to be digitized, the hearsay rule faced several new challenges. While the law had mostly anticipated primary evidence (i.e. the original document itself) and had created

[6] Anvar v. Basheer and the New (Old) Law of Electronic Evidence - The Centre for Internet and Society,
[7] Manisha T. Karia and Tejas D. Karia, 'India' (Chapter 13) in Stephen Mason, ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012).

special conditions for secondary evidence, increasing digitisation meant that more and more documents were electronically stored. As a result, the abduction of secondary evidence of documents increased.[8] In the Anvar case, [9] the Supreme Court noted that "there is a revolution in the way that evidence is produced before the court. In India before 2000, electronically stored information was treated as a document and secondary evidence of these electronic 'documents' was adduced through printed reproductions or transcripts, the authenticity of which was certified by a competent signatory. The signatory would identify her signature in court and be open to cross examination. This simple procedure met the conditions of both sections 63 and 65 of the Evidence Act. In this manner, Indian courts simply adapted a law drafted over one century earlier in Victorian England. However, as the pace and proliferation of technology expanded, and as the creation and storage of electronic information grew more complex, the law had to change more substantially.[10] Under the provisions of Section 61 to 65 of the Indian Evidence Act, 1872, the word "Document or content of documents" have not been replaced by the word "Electronic documents or content of electronic documents". Thus, the intention of the legislature is explicitly clear i.e. not to extend the applicability of section 61 to 65 to the electronic record. It is the cardinal principle of interpretation that if the legislature has omitted to use any word, the presumption is that the omission is intentional. It is well settled that the Legislature does not use any word unnecessarily.[11] In this regard, the **Apex Court in Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa[12]** held that "...Parliament is also not expected to express itself unnecessarily. Even as Parliament does not use any word without meaning something, Parliament does not legislate where no legislation is called for. Parliament cannot be assumed to legislate for the sake of legislation; nor indulge in legislation merely to state what it is unnecessary to state or to do what is already validly done. Parliament may not be assumed to legislate unnecessarily."

The IT Act amended section 59 of the Evidence Act, 1872 to exclude electronic records from the probative force of oral evidence in the same manner as it excluded documents. This is the re-application of the documentary hearsay rule to electronic records. But, instead of submitting

[8] Supra note 12.
[9] Anvar P. K. vs. P.K Basheer &Ors. (2014) 10 SCC 473
[10] Supra note 12.
[11] E-Evidence in India by Prashanti, available at www.legalservicesindia.com, last accessed on 09/02/2017.
[12] Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa reported as AIR 1987 SC 1454.

electronic records to the test of secondary evidence - which, for documents, is contained in sections 63 and 65, it inserted two new evidentiary rules for electronic records in the Evidence Act: section 65A and section 65B. The intention of the legislature is to introduce the specific provisions which has its origin to the technical nature of the evidence particularly as the evidence in the electronic form cannot be produced in the court of law owing to the size of computer/server, residing in the machine language and thus, requiring the interpreter to read the same. Section 65A of the Evidence Act creates special law for electronic evidence - The contents of electronic records may be proved in accordance with the provisions of section 65B.[20] This section performs the same function for electronic records that section 61 does for documentary evidence: it creates a separate procedure, distinct from the simple procedure for oral evidence, to ensure that the adduction of electronic records obeys the hearsay rule. It also secures other interests, such as the authenticity of the technology and the sanctity of the information retrieval procedure. But section 65A is further distinguished because it is a special law that stands apart from the documentary evidence procedure in sections 63 and 65.

Section 65B of the Evidence Act details this special procedure for adducing electronic records in evidence. Sub-section (2) lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used:

1. At the time of the creation of the electronic record, the computer that produced it must have been in regular use,
2. The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer,
3. The computer was operating properly; and,
4. The duplicate copy must be a reproduction of the original electronic record.

The Section 65B of the Evidence Act makes the secondary copy in the form of computer output comprising of printout or the data copied on electronic/magnetic media admissible. It provides: 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 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.

Sec. 65B (2)

The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by a person having lawful control over the period, and relates to the period over which the computer was regularly used; Information was fed in computer in the ordinary course of the activities of the person having lawful control over the computer; The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy; Information reproduced is such as is fed into computer in the ordinary course of activity.[13]

Sec.65 B (3)

The following computers shall constitute as single computer

1. By a combination of computers operating over that period; or
2. By different computers operating in succession over that period; or
3. By different combinations of computers operating in succession over that period; or
4. In any other manner involving the successive operation over that period, in whatever order, of one or more
5. 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.

Sec. 65B (4)

Regarding the person who can issue the certificate and contents of certificate, it provides the certificate doing any of the following things: identifying the electronic record containing the statement and describing the manner in which it was produced; giving the particulars of device, dealing with any of the matters to which the conditions mentioned in subsection (2) relate and

[13] Section 65 B (2) of the Indian Evidence Act, 1872 lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used.

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 subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.[14] This contention is further strengthened by the insertion words "Notwithstanding anything contained in this Act" to Section 65A & 65B, which is a non obstante clause, further fortifies the fact that the legislature has intended the production or exhibition of the electronic records by Section 65A & 65B only. A non obstante clause is generally appended to a Section with a view to give the enacting part of the Section, in case of conflict, an overriding effect over the provision in the same or other act mentioned in the non obstante clause. It is equivalent to saying that despite the provisions or act mentioned in the non obstante clause, the provision following it will have its full operation or the provisions embraced in the non obstante clause will not be an impediment for the operation of the enactment or the provision in which the non obstante clause occurs. The aforesaid principles of interpretation with respect to the non obstante clause in form of "Notwithstanding anything contained in this Act" is further supported by the Hon'ble **Apex Court in Union of India and Anr., v. G.M. Kokil and Ors.**[15] observed "It is well known that a non obstante clause is a legislative device which is usually employed to give overriding effect to certain provisions over some contrary provisions that may be found either in the same enactment or some other enactment, that is to say, to avoid the operation and effect of all contrary provisions." Further, the Hon'ble Apex Court in the case cited as Chandavarkar Sita Ratna Rao v. Ashalata S. Guram, [25] explained the scope of non obstante clause as "It is equivalent to saying that in spite of the provision of the Act or any other Act mentioned in the non obstante clause or any contract or document mentioned the enactment following it will have its full operation".

[14] Section 65B (4) of the Evidence Act lists additional non-technical qualifying conditions to establish the authenticity of electronic evidence. This provision requires the production of a certificate by a senior person who was responsible for the computer on which the electronic record was created, or is stored. 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.

[15] Union of India and Anr., v. G.M. Kokil and Ors. [(1984)SCR196].

1.2 OBJECTIVES

• Whether the role of Electronic evidence in evidence Act is effective or not?

• A analysis on Indian evidence Act sec 63 in India and USA

• Increasing of technologies in society leads to acceptance of electronic evidence judicial.

1.3 HYPOTHESIS

NULL HYPOTHESIS: Electronic evidence does not have profound value as evidentiary value in court of law

1.4 ALTERNATIVE HYPOTHESIS

Electronic evidence has profound value as evidentiary value in court of law

1.5 RESEARCH METHODOLOGY

This is a doctrinal research. The researcher has referred books, research articles, unpublished thesis and e-sources as a part of secondary source of the writing of the project.

CHAPTER-2

2. RELEVANCY AND ADMISSIBILITY OF ELECTRONIC EVIDENCE

In today's world Electronic devices used everywhere. It helps people to communicate locally and globally with ease. Due to which the reliance on electronic means of communication, e-commerce and storage of information in Electronic form increasing rapidly. It caused a need to transform the law relating to information technology and rules of admissibility of electronic evidence both in civil and criminal matters. Electronic evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device. It is any probative information stored or transmitted in Electronic form that a party to a court case may use at trial. It is "information of probative value that is stored or transmitted in binary form. It is not only limited to that found on computers but may also extend to include evidence on Electronic devices such as telecommunication or electronic multimedia devices. The e-evidence can be found in e-mails, Electronic photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories databases, Contents of computer memory, Computer backups, Computer printouts, Global Positioning System tracks, Logs from a hotel's electronic door locks, Electronic video or audio files. Electronic Evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available[16].

First, it is intended to include all forms of evidence that is created, manipulated or stored in a product that can, in its widest meaning, be considered a computer, excluding for the time being the human brain.

Second, it aims to include the various forms of devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition 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

[16] Vivek Dubey, "Admissibility of Electronic Evidence: An Indian Perspective"4, FRACIJ (2017)

Internet; and computer systems that are embedded into a device, such as mobile telephones, smart cards and navigation systems.

The third element 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 part of the definition 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. The last criteria, however, restricts the definition of electronic evidence to those items offered by the parties as part of the fact finding process[17].

2.1 ELECTRONIC EVIDENCE IN INDIA

Due to enormous growth in e-governance throughout the public and private sector, electronic evidence have involved into a fundamental pillar of communication, processing and documentation and various forms of Electronic evidence are increasingly being use in both civil and criminal litigation. With this Indian courts have developed case law regarding reliance on electronic evidence and have all necessitated amendments in Indian law to incorporate the provisions on the appreciation of Electronic evidence. The Information Technology Act, 2000 and its amendment are based on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce. The Information Technology (IT) Act 2000 was amended to allow for the admissibility of Electronic evidence. An amendment to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in electronic world.

As per provision Sec 2(t) of Information Technology Act 2000, [18] 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"

1. **Electronic Evidence & the Indian Evidence Act 18724**

   Following sections of Indian Evidence Act, 1872 deals with electronic evidence:-

[17] 2 Stephen Mason (ed), "Electronic Evidence" (Lexis Nexis , 2013).
[18] The Information Technology Act, 2000, No. 21, Acts of Parliament 2000.

Section 3 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. 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". Regarding the documentary evidence, in Section 59, for the words "Content of documents" the words "Content of documents or electronic records" have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence.

2. **Admission Defined.**

The definition of 'admission' (Section 17 of the Evidence Act) has been changed to include a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or of relevance.

3. When oral admissions as to contents of electronic records are relevant.—

New Section 22-A has been inserted into Evidence Act, to provide for the relevancy of oral evidence regarding the contents of electronic records. It provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question. So remember until your evidence's admissibility is in question, none of the corroboration that you provide about its genuineness along is going to be valid.

Entries in books of accounts including those maintained in an electronic form, regularly kept in the course of business, and are relevant.

An entry in any public or other official book, register or record or an electronic record made by a public servant in the discharge of his official duty, or by any other person in performance of a duty is kept, is itself a relevant fact,

What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.

Where there is, — (i) a longer statement, or (ii) a conversation, or (iii) an isolated document, or (iv) a document contained in a book, or (v) a series of letters of papers, the court has discretion to use the relevant portion of the conversation, document, books or series of letters or papers and requires the production of that portion or pages.

In other words, the evidence shall be given of only explanatory or qualifying part of the statement, document, book etc. Same is applicable to electronic record under the section. The statements made in books cannot be relied on unless supported by contemporaneous records.

What evidence is to be given and to be taken is total discretion of the judge. His discretion is always guided by principles of justice, conscience and convenience.

4. Opinion of Examiner of Electronic Evidence

When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or Electronic form, the opinion of the Examiner of Electronic Evidence referred to in Section 79 A of the Information Technology Act, 2000, is a relevant fact. Explanation: For the purposes of this section, an Examiner of Electronic Evidence shall be an expert.

5. Opinion as to electronic signature where relevant

Opinion given by examiner of electronic evidence regarding any information transmitted or stored in any computer resource or any other electronic or Electronic form is relevant fact.

6. Proof as to Electronic signature

Except in the case of a secure Electronic signature, if the electronic signature of any subscriber is alleged to have been affixed to an electronic record the fact that such electronic signature is the electronic signature of the subscriber must be proved.

Section 65B of Indian Evidence a Act is under focus in the Judicial and Law Enforcement circles. The main points that makes here are:

a) Section 65B (as well as 65A) of Indian Evidence Act refer to the special provisions of the Act in respect of Electronic Documents. Though Section 65 is referring to "Secondary" documents in paper form, there is no such distinction made as to the electronic document.

b) There is no need to distinguish primary and secondary and all documents need to be interpreted by a human being which takes the form of a Section 65B certificate.

c) A "Hard disk" which may contain an electronic document also cannot be considered the "Primary Document" since it is only a "Container" and the real Electronic document is an expression in binary language which cannot be read by a human being and needs to be interpreted with the assistance of a binary reading device (Computer + operating system +Application)

d) Section 65B explains the conditions under which an electronic document can be considered as Admissible in a Court as a "Document and it needs to be suitably confirmed for the Court to accept the document, which is often termed as "Section 65B certificate or Statement

e) Section 65B refers to a process of producing a "Computer Output" of the electronic document which is the evidence to be admitted and such computer output can be either in the form of a "Print Out" or a "Copy".

f) There is a Process by which the electronic document becomes the "Computer output" and Section 65B identifies this as the subject activity which needs to be conducted by a person having lawful control over the computer producing such output and that during the period of such production, the Computer should be working properly etc.

g) The focus of Section 65B is the activity of conversion of the electronic document residing inside a system which can be seen by an observer into a "Computer Output".

h) The other clarifications contained in the Section 65B such as that the Computer Output could be produced by a combination of computers, acting in succession etc as relating to dynamic creation of an electronic document from a data base and routing it through multiple devices onto a final visible form in the computer of the observer and thereafter its porting into a Printer.

i) Considering these interpretations, the Section 65B certification is a matter of fact" certification to the effect that "What I saw is what I reproduced as a computer output faithfully" and this can be done by any person who is observing an electronic document in his computer and wants it to be produced as an evidence. It is not necessary that a document from yahoo website has to be certified only by a Yahoo server administrator. Similarly, a statement of account downloaded from an ICICI bank website need not be certified only by the ICICI Bank manager but by any person who can lawfully access the document in electronic form.

j) There is also an important distinction that "Content Owner" is different from "Content Viewer" and Section 65B is meant to be produced by a content viewer. On the other hand the content owner in respect of say a Bank statement is the official Bank manager and he can provide a print out as the owner of the content who understands the content and is considered as an "Expert" in the domain. Anybody else who views the document provides a Section 65B certificate that the print out (or a soft copy) is a faithful reproduction.

It is very important that the legal fraternity and the Judiciary interpret the section properly. Any interpretation that only a "Server Administrator" can provide a certificate under Section 65B is considered incorrect. The server administrator can however provide the certificate but it is not mandatory. The Section 65B certifier is like a photographer who captures a photograph of an event and confirms the process of taking the photograph though he may not be aware of who is there in the picture and what they are doing. It is left to other "Experts" to interpret the "Content" and impute meaning as only a subject matter expert can do.

7. Proof as to verification of electronic signature

In order to ascertain whether a electronic signature is that of the person by whom it purports to have been affixed, the Court may direct (1) to produce electronic signature certificate, (2) to apply the public key listed in Electronic Signature Certificate and verify the electronic signature.

8. Presumption as to Gazettes in electronic forms.

The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law.

9. Presumption as to electronic agreements

The Court shall presume that every electronic record purporting to be an agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties.

10. Presumption as to electronic records and electronic signatures.-

Unless contrary is proved, the Court shall presume that the secure electronic record has not been altered and the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record. Nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any electronic signature.

11. Presumption as to Electronic Signature Certificates.-

Unless contrary is proved, the Court shall presume that the information listed in a Electronic Signature Certificate is correct.

12. Presumption as to electronic records and electronic signatures.-

Unless contrary is proved, the Court shall presume that the secure electronic record has not been altered and the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record. Nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any electronic signature. S. 85C Presumption as to Electronic Signature.

13. Presumption as to Electronic Signature Certificates.-

Unless contrary is proved, the Court shall presume that the information listed in a Electronic Signature Certificate is correct.

14. And S 88A deals with Presumption as to telegraphic messages and to electronic messages

88 concerns with the presumption that the message had been forwarded from the telegraph office and such message had been received by the addressee. There is no presumption as to the person

who delivered such message for transmission and S 88A concerns with the presumption of electronic message.

15. Presumption as to electronic records five years old -

Concerns with the presumption that the message had been forwarded from the telegraph office and such message had been received by the addressee. There is no presumption as to the person who delivered such message for transmission and S 88A concerns with the presumption of electronic message.

16. Presumption as to electronic records five years old -

Where an electronic record purports to be or is proved to be five years old and is produced from the proper custody, the court may presume that the Electronic signature which purports to be the Electronic signature of any particular person was so affixed by him or any person authorized by him in this behalf.

17. Production of documents or electronic records which another person, having possession, could refuse to produce

No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.

18. Amendments in Evidence Act 1872

In the ANVAR CASE[19] the Supreme Court noted that "there is a revolution in the way that evidence is produced before the court. In India before 2000, electronically stored information was treated as a document and secondary evidence of these electronic documents" was adduced through printed reproductions or transcripts, the authenticity of which was certified by a competent signatory. The signatory would identify her signature in court and be open to cross examination. This simple procedure met the conditions of both sections 63 and 65 of the Evidence Act. In this manner, Indian courts simply adapted a law drafted over one century earlier in Victorian England. However, as the pace and proliferation of technology expanded, and

[19] 5 (2014) 10 SCC 473

as the creation and storage of electronic information grew more complex, the law had to change more substantially. Under the provisions of Section 61 to 65 of the Indian Evidence Act, 1872, the word "Document or content of documents" have not been replaced by the word "Electronic documents or content of electronic documents". Thus, the intention of the legislature is explicitly clear i.e. not to extend the applicability of section 61 to 65 to the electronic record. It is the cardinal principle of interpretation that if the legislature has omitted to use any word, the presumption is that the omission is intentional. It is well settled that the Legislature does not use any word unnecessarily.

The IT Act amended section 59 of the Evidence Act, 1872 to exclude electronic records from the probative force of oral evidence in the same manner as it excluded documents. This is the re-application of the documentary hearsay rule to electronic records. But, instead of submitting electronic records to the test of secondary evidence - which, for documents, is contained in sections 63 and 65, it inserted two new evidentiary rules for electronic records in the Evidence Act: section 65A and section 65B. The intention of the legislature is to introduce the specific provisions which has its origin to the technical nature of the evidence particularly as the evidence in the electronic form cannot be produced in the court of law owing to the size of computer/server, residing in the machine language and thus, requiring the interpreter to read the same.8 Section 65A of the Evidence Act creates special law for electronic evidence - The contents of electronic records may be proved in accordance with the provisions of section 65B. This section performs the same function for electronic records that section 61 does for documentary evidence: it creates a separate procedure, distinct from the simple procedure for oral evidence, to ensure that the abduction of electronic records obeys the hearsay rule. It also secures other interests, such as the authenticity of the technology and the sanctity of the information retrieval procedure. But section 65A is further distinguished because it is a special law that stands apart from the documentary evidence procedure in sections 63 and 65.

Section 65B of the Evidence Act details this special procedure for adducing electronic records in evidence and makes the secondary copy in the form of computer output comprising of printout or the data copied on electronic/magnetic media admissible.

2.2. RELEVANCY & ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIA

In **R.M MALKANI V. STATE OF MAHARASTRA**[20], it was held that the tape is primary and direct evidence of what has been said and recorded. The court made it clear that electronically recorded conversation is admissible in evidence, if the conversation is relevant to the matter in issue and the voice is identified and the accuracy of the recorded conversation is proved by eliminating the possibility of erasure, addition or manipulation. This Court further held that a contemporaneous electronic recording of a relevant conversation is a relevant fact comparable to a photograph of a relevant incident and is admissible as evidence under Section 8 of the Act. There is therefore no doubt that such electronic record can be received as evidence.

2.2.1 Supplying Copy of Electronic Record

State of Punjab v. Amritsar Beverages Ltd[21]

S 14(3) of Punjab General Sales Tax Act provided for inspection of books, documents and accounts and their seizure. The officer seizing book, account, register or document shall forthwith grant a receipt to receipt, retaining copy, affixing signature and seal of officer on document and return of books to dealer. But seized record was cash book, ledger and other registers maintained in hard disk. Hence it was not possible to put signature and seal of official on seized documents. However, a copy was taken from hard disk and hard disk was returned.

It was held that the proper course of action for officers in such circumstances was to make copies of the hard disk or obtain a hard copy, affix their signatures or official seal on the hard copy and furnish a copy to the dealer or person concerned.

2.2.2Video Conferencing

IN AMITABH BAGCHI V. ENA BAGCHI, [22] sections 65-A and 65-B of Evidence Act, 1872 were analyzed. The court held that the physical presence of person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing. Sections 65-A and 65-B provide provisions for evidences relating to electronic

[20] AIR 1973 SC 57
[21] AIR 2007 SC 590.
[22] 2005 Cal. 11

records and admissibility of electronic records, and that definition of electronic records includes video conferencing.

IN STATE OF MAHARASHTRA V. DR PRAFUL B DESAI,[23] the question involved whether a witness can be examined by means of a video conference. The Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. The court allowed the examination of a witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence.

IN TWENTEITH CENTURY FOX FILM CORPORATION V. NRI FILM PRODUCTION ASSOCIATES (P) LTD[24] certain conditions have been laid down for video-recording of evidence:

• Before a witness is examined in terms of the Audio-Video Link, witness is to file an affidavit or an undertaking duly verified before a notary or a Judge that the person who is shown as the witness is the same person as who is going to depose on the screen. A copy is to be made available to the other side. (Identification Affidavit)

- The person who examines the witness on the screen is also to file an affidavit/undertaking before examining the witness with a copy to the other side with regard to identification.
- The witness has to be examined during working hours of Indian Courts. Oath is to be administered through the media.
- The witness should not plead any inconvenience on account of time different between India and USA.
- Before examination of the witness, a set of plaint, written statement and other documents must be sent to the witness so that the witness has acquaintance with the documents and an acknowledgement is to be filed before the Court in this regard.

[23] 2 AIR 2003 SC 2053.
[24] AIR 2003 KANT 148.

- Learned Judge is to record such remarks as is material regarding the demur of the witness while on the screen.
- Learned Judge must note the objections raised during recording of witness and to decide the same at the time of arguments.

☐ After recording the evidence, the same is to be sent to the witness and his signature is to be obtained in the presence of a Notary Public and thereafter it forms part of the record of the suit proceedings.

☐ The visual is to be recorded and the record would be at both ends. The witness also is to be alone at the time of visual conference and notary is to certificate to this effect.

☐ The learned Judge may also impose such other conditions as are necessary in a given set of facts.

☐ The expenses and the arrangements are to be borne by the applicant who wants this facility.

2.1.3 Proof of The Electronic Signature Of A Person

Section 67A of IEA provides that except in the case of secure Electronic signature, if the Electronic signature of any subscriber is alleged to have been affixed to an electronic record the fact that such Electronic signature is Electronic signature of subscriber must be proved. It is necessary to prove in manner of proof of electronic record. Section 65B will be applicable.

In BODALA MURALI KRISHNA V. SMT. BODALA PRATHIMA the court held that the amendments carried to the Evidence Act by introduction of Sections 65-A and 65-B are in relation to the electronic record. Sections 67-A and 73-A were introduced as regards proof and verification of Electronic signatures. As regards presumption to be drawn about such records, Sections 85-A, 85-B, 85-C, 88-A and 90-A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and Electronic signatures, as admissible pieces of evidence.

2.1.4 Electronic Messages - Email

IN DHARAMBIR V. CENTRAL BUREAU OF IINVESTIGATION16, the court arrived at the conclusion that when Section 65-B talks of an electronic record produced by a computer referred

to as the computer output) it would also include a hard disc in which information was stored or was earlier stored or continues to be stored. It distinguished as there being two levels of an electronic record. One is the hard disc which once used itself becomes an electronic record in relation to the information regarding the changes the hard disc has been subject to and which information is retrievable from the hard disc by using a software program. The other level of electronic record is the active accessible information recorded in the hard disc in the form of a text file, or sound file or a video file etc. Such information that is accessible can be converted or copied as such to another magnetic or electronic device like a CD, pen drive etc. Even a blank hard disc which contains no information but was once used for recording information can also be copied by producing a cloned had or a mirror image.

In the landmark decision of United States district court, for MAYLAND IN LORRAINE V. MARKEL AMERICAN INSURANCE COMPANY 17 held that when electronically stored information is offered as evidence, the following to be ascertained:

1. Is information relevant

2. Is it authentic

3. Is it hearsay

4. Is it original or, if it is a duplicate, is there admissible secondary evidence to support it and

5. Does its probative value survive the test of unfair prejudice ?

In SOM PRAKASH V. STATE OF DELHI[25] , the Supreme Court has rightly observed that "in our technological age nothing more primitive can be conceived of than denying discoveries and nothing cruder can retard forensic efficiency than swearing by traditional oral evidence only thereby discouraging the liberal use of scientific aids to prove guilt." Statutory changes are needed to develop more fully a problem solving approach to criminal trials and to deal with heavy workload on the investigators and judges.

[25] AIR 1974 SC 989.

In SIL IMPORT, USA V. EXIM AIDES EXPORTERS, BANGALORE,[26] the Supreme Court held that "Technological advancement like fascimile, Internet, e-mail, etc. were in swift progress even before the Bill for the Amendment Act was discussed by Parliament. So when Parliament contemplated notice in writing to be given we cannot overlook the fact that Parliament was aware of modern devices and equipment already in vogue.

In STATE V. MOHD AFZAL AND ORS , the court held that Computer generated electronic records is evidence, admissible at a trial if proved in the manner specified by Section 65B of the Evidence Act.

2.1.5 Proof of Contents of C.D

IN JAGJIT SINGH V. STATE OF HARYANA[27] the speaker of the Legislative Assembly of the State of Haryana disqualified a member for defection. When hearing the matter, the Supreme Court considered the Electronic evidence in the form of interview transcripts from the Zee News television channel, the Aaj Tak television channel and the Haryana News of Punjab Today television channel. The court determined that the electronic evidence placed on record was admissible and upheld the reliance placed by the speaker on the recorded interview when reaching the conclusion that the voices recorded on the CD were those of the persons taking action. The Supreme Court found no infirmity in the speaker's reliance on the Electronic evidence and the conclusions reached by him. The comments in this case indicate a trend emerging in Indian courts: judges are beginning to recognize and appreciate the importance of Electronic evidence in legal proceedings.

In the years that followed, printed versions of CDRs were admitted in evidence if they were certified by an officer of the telephone company under sections 63 and 65 of the Evidence Act. The special procedure of section 65B was ignored. This has led to confusion and counter-claims. For instance, the 2011 case of AMAR SINGH V. UNION OF INDIA23 saw all the parties, including the state and the telephone company, dispute the authenticity of the printed transcripts of the CDRs, as well as the authorisation itself.

[26] AIR (1999) 4 SC 567
[27] 2 (2006) 11 SCC 1.

Currently, in the case of RATAN TATA V. UNION OF INDIA , a compact disc (CD) containing intercepted telephone calls was introduced in the Supreme Court without following any of the procedure contained in the Evidence Act.

The recent judgment of the Hon'ble Supreme Court delivered in ANVAR P.V. V. P.K. BASHEER & OTHERS[28], in CIVIL APPEAL NO. 4226 OF 2012 decided on Sept., 18, 2014, That Computer Output is not admissible without Compliance of 65B,EA overrules the judgment laid down in the State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru26 by the two judge 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 is required to be overruled.

In SANJAYSINH RAMRAO CHAVAN V. DATTATRAY GULABRAO PHALKE27 the court relying upon the judgment of Anvar case while considering the admissibility of transcription of recorded conversation in a case where the recording has been translated, it was 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.

In the recent judgment, JAGDEO SINGH V. THE STATE AND ORS 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.

2.1.6 Challenges to Authenticity tf Electronic Evidence

a. A claim that the records were altered, manipulated or damaged between the time they were created and the time they appear in court as evidence;

b. The reliability of the computer program that generated the record may be questioned

[28] Anvar P.V. v. PK Basheer & others, in civil appeal no. 4226 of 2012.

c. The identity of the author may be in dispute: for instance, the person responsible for writing a letter in the form of a word processing file, SMS or email may dispute they wrote the text, or sufficient evidence has not been adduced to demonstrate the nexus between the evidence and the person responsible for writing the communication;

d. The evidence from a social networking website might be questioned as to its reliability

e. It might be agreed that an act was carried out and recorded, but at issue might be that the party introducing the evidence has failed to prove that where others might have access to a device (such as a mobile telephone), there was no proof to show that the message was directed to a particular person; or f. Whether the person alleged to have used their PIN, password or clicked the 'I accept' icon was the person that actually carried out the action.

g. The data on local area networks, and whether there is a need to obtain an image of the complete network, if this is possible. If an image of each computer comprising the network is taken, the issue with networked computers is to demonstrate who had access to which computers at what time, and whether this access is audited. The security mechanisms in place on the network will be an important consideration when proving authenticity.

h. Data from the Internet is also subject to problems, because reliance may be placed on data obtained from remote computers, the computer of an investigator, and perhaps intercepted evidence. With the increased use of cloud computing where data is stored on 'server farms', accessible via the Internet, obtaining a copy of the data may be subject to contractual restrictions, or the data may be stored in another jurisdiction, which in turn may mean it will be necessary to take local legal advice in relation to the obtaining of the data.

i. Where data is being updated constantly, such as transactional data-bases, or websites that are continually updated, this poses problems, as the relevant evidence is point-in-time, which may be extremely difficult to obtain. j. Authentication of information on social media sites presents its own unique set of issues. Firstly, it can be difficult to establish the author of the document, because social media sites often have a number people writing to the one page. Secondly, proving the identity of an author can be difficult, since it is still possible to create an internet profile without having to prove identity.

2.1.7 Effects of Considering Electronic Evidence As Primary And Direct[29]

Blurring the Difference between Primary and Secondary Evidence

By bringing all forms of computer evidence into the fold of primary evidence, the statute has effectually blurred the difference between primary and secondary forms f evidence. While the difference is still expected to apply with respect to other forms of documents, an exception has been created with respect to computers. This, however, is essential, given the complicated nature of computer evidence in terms of not being easily producible in tangible form. Thus, while it may make for a good argument to say that if the word document is the original then a print out of the same should be treated as secondary evidence, it should be considered that producing a word document in court without the aid of print outs or CDs is not just difficult, but quite impossible.

2.1.8 Making Criminal Prosecution Easier

In light of the recent spate of terrorism in the world, involving terrorists using highly sophisticated technology to carry out attacks, it is of great help to the prosecution to be able to produce electronic evidence as direct and primary evidence in court, as they prove the guilt of he accused much better than having to look for traditional forms of evidence to substitute the electronic records, which may not even exist. As we saw in the Ajmal Kasab case, terrorists these days plan all their activities either face-to-face, or through software. Being able to produce transcripts of internet transactions helped the prosecution case a great deal in proving the guilt of the accused. Similarly, in the case of State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, the links between the slain terrorists and the masterminds of the attack were established only through phone call transcripts obtained from the mobile service providers.

2.1.9 Risk of Manipulation

While allowing all forms of computer output to be admissible as primary evidence, the statute has overlooked the risk of manipulation. Tampering with electronic evidence is not very difficult and miscreants may find it easy to change records which are to be submitted in court. However, technology itself has solutions for such problems. Computer forensics has developed

29

enough to find ways of cross checking whether an electronic record has been tampered with, when and in what manner.

2.1.10Opening Potential Floodgates

Computers are the most widely used gadget today. A lot of other gadgets involve computer chips in their functioning. Thus, the scope of Section 65A and 65B is indeed very large. Going strictly by the word of the law, any device involving a computer chip should be adducible in court as evidence. However, practical considerations as well as ethics have to be borne in mind before letting the ambit of these Sections flow that far. For instance, the Supreme Court has declared test results of narco-analysis to be inadmissible evidence since they violate Article 20(3) of the Constitution. It is submitted that every new form of computer technology that is sought to be used in the process of production of evidence should be subjected to such tests of Constitutionality and legality before permitting their usage.

- **UNITED KINGDOM**

  There are different rules regarding admissibility of electronic evidence than those applicable to traditional documentary evidence. These provisions are found in the Civil Evidence Act 1968 and the Police and Criminal Evidence Act 1984. A computer-produced document shall be admissible as evidence of the statement contained therein, provided the proponent demonstrates its authenticity. The party who wishes to tender an electronically-produced document as evidence must establish that[30].

a. the document was prepared during a period over which the computer regularly stored or processed information;

b. over the relevant period of time, information of this type was regularly supplied to the computer

c. the computer was operating properly and

d. the inform ation co ntained in the st at ement r eprodu ces information supplied to the computer

[30] Civil Evidence Act, 1968

If one of these conditions is not met, the document is simply inadmissible as evidence

In addition to proving the authenticity of the document, the proponent of an electronicallyproduced document must also demonstrate its reliability, through the production of a certificate signed by a person responsible for the operation of the computer

As for probative weight of computer-produced evidence, section 6 of the Civil Evidence Act 1968 requires that in estimating the weight of the document, the Court must examine the contemporaneity of the recording of the information with the events described in that record, and the motive of any person to misrepresent the facts recorded.

Section 8[31] of the Civil Evidence Act establishes that the Rules of Court must require that the proponent of such evidence give notice to its adversary of its intention to use electronically-produced evidence.

Section 69[32] of the Police and Criminal Evidence Act 1984 provides that computer-produced evidence is admissible in criminal proceedings as long as there exists no reasonable grounds for believing that the statement it contains is inaccurate because of improper use of the computer and that, at all material times, the computer was operating properly or that the malfunction did not affect the production of the document or the accuracy of the statement. Finally, section 69 of the Police and Criminal Evidence Act 1984 requires that the Rules of Court concerning giving notice are satisfied. IN R. V. SPIBY , the Court of Appeal held that printouts from an automatic telephone call logging computer installed in a hotel were admissible as they constituted real evidence. The Court concluded that in the absence of evidence to the contrary, the machine is held to be in working order at the material time.

In CAMDEN LONDON BOROUGH COUNCIL V. HOBSON[33] , the Court stated that computer-generated evidence constituted real evidence if the statement originated in the computer. It would then be admissible as the record of a mechanical operation in which human information had played no part; however, a statement originating from a human mind and subsequently processed by a computer would be inadmissible as hearsay. Proof of the reliability

[31] Civil Evidence Act, 1968.
[32] 3 Police and Criminal Evidence Act, 1984.
[33] [19911 Chin_ L.R. 199 (C.A.Cr.D.).

of a computer-generated document is also a crucial condition to its admissibility. The Lords found that the inaccuracy did not affect the processing of the information supplied to the computer. Section 69 of the Police and Criminal Evidence Act 1984 should be interpreted according to its purpose so as to not exclude otherwise accurate evidence. Lord Hoffman concluded that:

- **UNITED STATES**

  The Federal Rules of Evidence provide the requirements for the authentication of documentary evidence, a prerequisite step for the admission of such evidence. The Federal Rules of Evidence deal with authentication without distinguishing between computer-generated evidence and other forms of documentary evidence. One must then conclude that the requirements for traditional documentary evidence also apply to computer-generated evidence[34]

  Federal Rule of Evidence 901 37 describes authentication as a condition precedent to admissibility, "satisfied by evidence sufficient to support a finding that a matter in question is what its proponent claims". If a document is produced by a process or system, one must demonstrate that such process or system produces an accurate result.

  IN KING V. STATE EX. REL MURDOCH ACCEPTANCE CORP38 , the Supreme Court of Mississippi suggested that hardware is reliable in light of its general use and reliance in the business community. However, the Court, in this case, established guidelines for the admissibility of computer-generated business.

  records. These guidelines included proof that the computing equipment was recognized as standard equipment, that the entries were made in the regular course of business, contemporaneously the event recorded, and that foundation testimonies satisfied the Court that the source of information method and time of preparation was such as to indicate its trustworthiness and justify its admission'

  Although these guidelines are very similar to those established by Federal Rule of Evidence 803(6)39

  ,

[34] 6 Federal Rules of Evidence, 2015.

modern case law has been more generous with the admission of computer-generated evidence,
shifting the debate towards the probative weight of such documentary evidence. In UNITED STATES V. LINN40 , t h e t e s t i m o n y o f a h o t e l D i r e c t o r o f Communications was sufficient to authenticate a record of telephone calls as he was on duty when the computer recorded the call in question.

In UNITED STATES V. CATABRANIS, the Court admitted into evidence business records, although it was demonstrated that they contained inaccuracies. The Court held that these inaccuracies affected the weight and not the admissibility of the records.

CHAPTER 3

3. ADMISSIBILITY OF SCIENTIFIC EVIDENCE UNDER INDIAN LAWS

Since time immemorial, the concept of State has been intertwined with the concept of Law, although the latter originated before the former. With the evolution of society, the legal concepts and theories were contemplated by the system. With the existence of such legal concept and theories, the concept of fair trial was introduced which demanded evidence i.e. testamentary or materialistic evidence. To find and collect testamentary and material evidence, the authorities devised several methods. The best evidence to convict an accused was considered to be a confession by the accused himself but no criminal would easily confess to his crimes. Throughout ages, the system of procurement of confession had led to inhumane inquiry methods ranging from the common 'thrashing and beating' of a suspect to torture set-ups. With the advancement of time and innovation in the science and technology, investigative authorities developed several scientific methods which could help in investigation of a crime without the use of inhumane and torturous investigative techniques.

The necessity of rapidly introducing scientific methods in investigation can be deduced from the recommendation of the 14th Law Commission Report which stated that, 'There is a paramount need to train the Inquiry Officer or the Investigation Agency like the Police in scientific methods'. We know that the principles of fairness, transparency and human rights form the bedrock of Indian Criminal Justice System. As such the Criminal Justice System also demands an efficient investigation, which in the absence of scientific methods might infringe upon the 'Right of Speedy Trial'. In the case of Hussainara Khatoon v. State of' Bihar112 the Apex Court recognised the Right of Speedy Trial as a Fundamental Right. The Court held that.

'Speedy trial is the essence of criminal justice and there can be no doubt that delay in trial by itself constitutes denial of justice. It is interesting to note that in the United States, speedy trial is one of the constitutionally guaranteed rights. The Sixth Amendment to the observed Constitution provides that ''In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial' So also Article 3 of the European Convention on Human Rights provides that 'Everyone arrested or detained-shall be entitled to trial within a reasonable time or to release pending trial'.

We think that even under our Constitution, though speedy trial is not specifically enumerated as a fundamental right, it is implicit in the broad sweep and content of Article 21 as interpreted by this **Court in Maneka Gandhi v. Union of India**. We have held in that case that Article 21 confers a fundamental right on every person not to be deprived of his life or liberty except in accordance with the procedure prescribed by law and it is not enough to constitute compliance with the requirement of that Article that some semblance of a procedure should be prescribed by law, but that the procedure should be 'reasonable, fair and just. If a person is deprived of his liberty under a procedure which is not 'reasonable, fair and just', such deprivation would be violative of his fundamental right under Article 21 and he would be entitled to enforce such fundamental right and secure his release. Now obviously procedure prescribed by law for depriving a person of his liberty cannot be 'reasonable, fair or just' unless that procedure ensures a speedy trial for determination of the guilt of such person. No procedure which does not ensure a reasonable, quick trial can be regarded as 'reasonable, fair or just' and it would fall foul of Article 21. There can, therefore, be no doubt that speedy trial and by speedy trial we mean reasonably expeditious trial, is an integral and essential part of the fundamental right to life and liberty enshrined in Article 21.

It is to be remembered that since the boom of information & technology, certain crimes in the modern world like cyber crimes can only be solved by using scientific aids like surveillance, hacking etc. Failure of the investigative agencies to adapt to these modern aids will result only in delay, or worst of all, even miscarriage of justice.

3.1.1 Admissibility of Scientific Evidence under Indian Laws

The Hon'ble Supreme Court of **India in State of Maharashtra v. Indian Hotels** and Restaurants Association[35] held that, "It must be presumed that the legislature understands and correctly appreciates the need of its own people, that its laws are directed to problems made manifest by experience."

Thus the first rule of interpretation is that the words of a statute should be given their ordinary and natural meaning as the intention of the law makers is expressed through words. If the language of a statute is plain, then the duty of the court is to give effect to it. At this juncture it is

[35] 2013(2) RCR (civil) 859.

pertinent to mention the legal maxim, ut res magis valeat quam pereat, which means that where an alternate construction is possible, the Court must give effect to that interpretation which will help in smooth functioning of the system rather than that interpretation that shall place hindrance in the way of effective implementation of the statute. Therefore, different provisions of various statutes in our country should be interpreted keeping in mind the changed circumstances of society and advancement in crimes and techniques adopted by criminals. The modern and hi-tech criminal should not get the benefit of the old Indian laws just because the latest crimes are not defined in Indian Statue. It is also pertinent to point out that Indian Courts have given several judgments acquitting the accused on the basis of the concept of benefit of doubt. To check the aforesaid situation, law has been amended from time to time by the legislature to incorporate new crimes in the old statutes since it is a time taking process, at times it creates dissatisfaction among the common masses and encourages the criminals. It is also an accepted fact that the victims of a crime deserve our empathy. The victim do not get victimized only once but finds himself/herself victimized time and again by the Criminal Justice System during various stages of the case and especially when the accused goes scot free due to benefit of doubt.

Therefore, at present, when modern crimes are being committed by hi-tech criminals with the help of advanced technologies, it's high time that investigative agencies and the Courts should rely on advanced scientific aids. Scientific and technological advancement could be an essential tool for the investigating agencies in collecting evidence. There are enough provisions in our Indian laws which are related to applicability of science and technology in criminal investigation and prosecution, the only requirement is to give them the widest possible interpretation so that the criminals cannot escape the clutches of law.

3.1.2 Admissibility of Scientific Evidence under the Constitution of India[36]

The Constitution of India was drafted by the Constituent Assembly after extensive research and analysis. The Constituent Assembly had geographical necessities, historical development and cultural and social diversities in their mind while drafting the Constitution. Hence, it would be proper for us to interpret and understand every provision of the Constitution in the light of the present needs of our country.

[36] The Constitution of India, 1950

3.1.3 Article 20(3) - Right against Self Incrimination

The Indian Constitution in Article 20(3) deals with Self Incrimination of an accused. Article 20(3) provides, "No person accused of any offence shall be compelled to be a witness against himself.

This provision is based upon the latin maxim, Nemo tenetur se ipsum prodere, which means that no man is bound to accuse himself115 i.e. no person can be forced to give a statement exposing himself to criminal prosecution either in the future or in present times. The concept of Article 20(3) is borrowed from the 5th Amendment of the United States Constitution, which provides restriction on the government to force any person to produce any sort of evidence that would be self incriminating. This immunity is provided to each and every individual against whom some accusation has been leveled.[37]

The scope of the immunity provided by the 5th amendment in US Constitution has been widened by the Indian Supreme Court by interpreting the word 'witness' to comprise of both documentary and oral evidences which play an important role in strengthening the prosecution case against the accused. However, the evidence should be in the nature of communication117. Similarly, protection is also available against testimonial compulsions. This protection is not available to a person who is not an accused. It is irrelevant in this case that he becomes an accused subsequently118. Also, the accused loses this protection if any sort of recovery is made, be that of an object from his/her possession. A general statement given by a person during formal inquiry or investigation without leveling any charge against him would not attract Article 20(3) even if such statement made by the person during such inquiry or investigation turns to be incriminating at some later stage[38]. In the landmark case of Pakhar Singh and Anr. v. State120, the court held that the word 'witness' must be understood in its natural sense, i.e. as referring 'to a person who' furnishes evidence. In fact, every positive volitional act which furnishes evidence is a testimony. Therefore, the information or statement provided by the accused person to the investigative agency during investigation is evidence. Hence, the statement made during Narco Analysis should be kept outside the purview of article 20(3) as it is merely a statement made by the accused during the investigation.

[37] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300
[38] Veera v. State of Maharashtra, AIR 1976 SC 1167.

In **Dinesh Dalmia v. State of Maharashtra**[39], the Hon'ble High Court held that "Narco-analysis testimony was not by compulsion because the accused may be taken to the laboratory for such tests against his will, but the revelation during such tests is quite voluntary". In this the Indian Courts limited the scope of Article 20(3) on the basis of "Minimal Bodily Harm Doctrine". Similarly, in another landmark case of **Ramachandra Reddy and others v. State of Maharashtra,**[40] the Bombay High Court upheld the use of P300 or Brain Mapping, Narco Analysis and Lie Detection test by investigative agencies during investigation. Another landmark **judgement was of Rojo George v. State of Kerala**[41], in which the petitioner expressed his willingness to subject himself for two tests namely Brain Mapping & Lie Detection but refused to subject himself to Narco Analysis, as he believed it to be unscientific in nature. However, the court relied upon the Kathi Kallu Case ratio and refused to grant relief to the petitioner.

In the case of Nandini Satpathy v. P.L. Dani,125 the Hon'ble Apex Court held that no person can forcefully extract a statement from an accused, as he has a right to remain silent during the course of interrogation or investigation. The object behind the concept of protection against self incrimination is that a free atmosphere should be provided to the accused to come forth and furnish relevant evidence to the investigating authorities or Courts with reference to his/her knowledge and possessions and no scope should be given to the investigative authorities to coerce out a confession by using unlawful and torturous means to implicate some innocent person.

Anything extracted out of an accused by any kind of threat or inducement or violence which results into incriminating the accused shall be violative of their fundamental right guaranteed under Article 20(3) of the Constitution of India. In People's Union for Civil liberties v. Union of India[42], Hon'ble Apex Court held that '' A person can only become a witness when he makes oral or documentary statement in or out of the court, in relation to the accused person or the offence. Providing any sort of identification i.e., thumb impression or foot or palm impression or giving hand writing samples are not covered under Article 20(3). For testimonial compulsions it is necessary to put forward the personal knowledge of the person about the

[39] Cr. L.J. (2006) 2401.
[40] Supra 79
[41] 1979 KLT 337.
[42] AIR 2004 SC 456.

happening or non happening of an event. The practice of producing documents which may reveal any of the controversial point does not amount to self incrimination'. In Brain Mapping and Polygraph tests however no statements are made, neither oral nor written. In Brain Mapping only brain impressions are measured and under a Polygraph test only physiological changes are measured, so these scientific aids are not violative of Article 20 (3).

3.1.4 Admissibility of Scientific Evidence under Indian Evidence Act

Section 3 of the Indian Evidence Act defines 'Evidence'. The term 'Evidence' includes in itself all the instruments by which relevant facts can be brought before the Court151. With respect to the present research, Section 27 and Section 45 of the act are most pertinent.

Section 27 of Indian Evidence Act provides When any fact is deposed to as discovered in consequences of information received from a person accused of any offence, in the custody of a police officer, so much of such information, whether it amounts to a confession or not, as relates distinctly to the fact thereby discovered, may be proved.

It means that if some fact is discovered in furtherance of the information received from an accused of an offence in police custody, so much of the information as relates to the facts discovered by that information, can be proved irrespective of the fact whether that particular information amounts to a confession or not.

3.1.5 Admissibility of Scientific Evidence under Code of Criminal Code

Section 2 (h) CrPC159 defines the term investigation as "Investigation includes all the proceedings under this Code for the collection of evidence conducted by a police officer or by any person (other than a Magistrate) who is authorized by a Magistrate in this behalf" This involves all the proceedings for the collection of evidence by the police officers. Thus there is no restriction under this provision on police officers to collect evidence even by scientific means or with the help of scientific aids.

In 2005 an amendment was made in Section 53 of Cr.PC160 which provides for recognition of scientific tests.

Section 53 of Cr.PC provides "(1) When a person is arrested on a charge of committing an offence of such a nature and alleged to have been committed under such circumstances that there are reasonable grounds for believing that an examination of his person will afford evidence as to the commission of an offence, it shall be lawful for a registered medical practitioner, acting at the request of a police officer not below the rank of sub-inspector, and for any person acting in good faith in his aid and under his direction, to make such an examination of the person arrested as is reasonably necessary in order to ascertain the facts which may afford such evidence, and to use such force as is reasonably necessary for that purpose.

(2) Whenever the person of a female is to be examined under this section, the examination shall be made only by, or under the supervision of a registered female medical practitioner

In furtherance of this section medical examination may be conducted of an accused on the request of police officer. In fact, Section 53A specifically incorporates DNA testing[43].

It states that " Examination of person accused of rape by medical practitioner

1. When a person is arrested on a charge of committing an offence of rape or an attempt to commit rape and there are reasonable grounds for believing that an examination of this person will afford evidence as to the commission of such offence, it shall be lawful for a registered medical practitioner employed in a hospital run by the Government or by a local authority and in the absence of such a practitioner within the radius of sixteen kilometers from the place where the offence has been committed by any other registered medical practitioner, acting at the request of a police officer not below the rank of a sub-inspector, and for any person acting in good faith in his aid and under his direction, to make such an examination of the arrested person and to use such force as is reasonably necessary for that purpose.

2. The registered medical practitioner conducting such examination shall, without delay, examine such person and prepare a report of his examination giving the following particulars, namely

(i) the name and address of the accused and of the person by whom he was brought,

(ii) the age of the accused,

[43] Sec. 53-A(2) (IV) of Code of Criminal Procedure, 1973

(iii) marks of injury, if any, on the person of the accused,

3.1.6 Admissibility of Scientific Evidence in Code of Civil Procedure

The Code of Civil Procedure does not specifically provide for scientific tests nor has any amendment been made to that effect, but if proper interpretation is done and provisions are perused in the light of modern day technologies, then there are some provisions in the Code of Civil Procedure under which courts may issue orders for testing of DNA, etc. and examine the report of its experts.

Section 75 of the CPC empowers the court to issue 'Commissions'. It provides that

Subject to such conditions and limitations as may be prescribed, the court may issue a commission-:

(a) to examine any person;

(b) to make local investigation

(c) to examine or adjust account; or

(d) to make a partition;

(e) to hold a scientific, technical or expert investigation;

(f) to conduct sale of property which is subject to speedy and natural

decay and which is in the custody of the court pending the determination of the suit.

(g) to perform any ministerial act.

Thus, a power is vested in the Civil Court, to issue 'Commissions' for examining any person, who may be a DNA expert or a Brain Mapping expert or incharge of a Laboratory which has performed the DNA sampling and testing, etc. Moreover, in civil matters and in property dispute cases or cases of inheritance, the civil court has full power to issue Commissions for DNA testing or other scientific tests which in the eyes of court are relevant and will aid the court in deciding the matter. Unfortunately, the Courts in India have refrained from using this

provision which without any doubt is of significant value. The detailed provision regarding the procedure in this respect is order 26 of the CPC.

Order 26 Rule 10 of the CPC lays down that-:

(1) The Commissioner after such local inspection as he deems necessary and after reducing to writing the evidence taken by him, shall return such evidence, together with his report in writing signed by him, to the court.

(2) Report and depositions to be evidence in suit- The report of the Commissioner and the evidence taken by him (but not the evidence without the report) shall be evidence in the suit and shall form part of the record; but the court or, with the permission of the court, any of the parties to the suit may examine the Commissioner personally in open Court touching any of the matters referred to him or mentioned in his report; or as to his report or as to the manner in which he has made investigation.

(3) Commissioner may be examined in person-: Where the court is for any reason dissatisfied with the proceedings of the Commissioner, it may direct such further enquiry to be made as it may think fit.

In compliance with this provision, the Commissioner is required to submit his report in writing and he may also be examined by the court with respect to such report. Later if found suitable, such report shall be treated as evidence in the suit in which it is submitted to the court of law. Further, under Order 26 Rule 10A of the Code of Civil Procedure, specific provision as to scientific investigations has been laid down.

3.2 LEGAL STATUS OF SCIENTIFIC TECHNIQUES IN INDIA

3.2.1 Polygraph Test

The Indian Judiciary like most of its counterparts in the developing world dismisses the Polygraph Test as evidential material and the report of the Polygraph test is not admissible in a court of law. Japan is the only exception where the Polygraph test is largely used by law enforcement agencies to decide the future course of investigation.

To enable the Indian law enforcement agencies for using the test to aid investigation, NHRC has issued some Guidelines which are to be followed while administering the procedure on the accused. These are as follows-

i. Consent of the accused with full explanation of the procedure and its legal implications is a prerequisite condition for the conducting the test.

ii. Granting of Legal support & access to personal lawyer is a necessity to be given to accused.

iii. The site of the procedure and its recording should be an independent institution. In majority cases it tends to be a Hospital.

iv. The manner in which information is received should be put in medical terms on the records.

The Polygraph test has been established as a valuable aid in investigation of crime. It provides immense help to investigating agency in exonerating an innocent person and apprehending the guilty. However, like any other test based on diagnostic device or technique, the veracity and validity of the polygraph test results heavily depend upon the competency and integrity of the examiner.[44]

The prevalent use of Polygraph techniques in criminal investigations and evidence gathering raises concerns about various factors that may adversely affect the accuracy of the test and further affect its use in administrative and judicial proceeding166. Thus the Hon'ble High Court of Gujarat in Abbasbaig **Habibbaig Mirza v. State of Gujarat**[45] held that "The legality, validity or evidentiary value of the Lie Detector test is again a question which has to be determined at the trial.

Further in Yelchuri Manohar v. State of A.P.[46] case, Polygraph Test of an accused was conducted and the court held that that the report of Polygraph Test is admissible under section 293 of the Code of Criminal Procedure. The court further added that as per the provisions of Section 293 of the Criminal Procedure Code, any report submitted by a Government scientific expert upon any subject, after examination and analysis, shall be admissible as evidence in any

[44] An demy of Polygraph (Lie Detector") Examiners" available at: www.jstore.org/stable/1139536 (visited on 04-12-2014).
[45] (2005) 3 GLR 2418
[46] 2005CriLJ 4593

trial in a court of law. The sub section (4) (e) of Section 293, Cr.PC also applies to the Director of a State Forensic Laboratory and therefore there is no compulsion on the court to examine the expert if the court feels it necessary. However, such a report is only opinion evidence, which requires further corroboration.

3.2.2 Narco Analysis Test - Legal Status

It is often argued that once established as an accused (a prima facie condition for imposition of Art 20(3)), Article 20(3) can be used to evade the legal power of questioning by the law enforcement agencies related to crime investigation. Now the question to be posed should be: Did the Constitution framers create hindrance in an otherwise effective investigation practice of cross examination by questioning the accused with the introduction of Article 20(3)

Before 2010, the scope of Article 20(3) was hazy. Various courts differed on the opinion of acceptance or rejection of the Narco-Analysis Test based on their own interpretation of the limit of Article 20(3) and the right of the accused. For instance in the celebrated Telgi's case, the Bombay High Court observed that Narco- Analysis does not violate constitutional rights. But the conclusion drawn by the court raised the question of compulsion in conducting these test. The Madras High Court too recognized that on being subjected to Narco-Analysis, the subject is not under compulsion. In fact, the High Court went on to add that revelations during the analysis are anything but voluntary **Dinesh Dalmia v. State**[47] . But again the issue of intoxication with respect to the witness undergoing the process arose and the technique's validity was put under question. Section 132 of the Indian Evidence Act says that the witness shall not be excused from answering on the ground that such answers may tend to criminate him directly or indirectly; or criminate or expose or tend to expose him/her to a penalty or forfeiture of any kind. So, if a non-accused is compelled to give evidence, such evidence is not prohibited under the law even if it ultimately leads to accusations against the witness himself/herself. The court has also put forward the logic that during the time that the statement was made, which criminated him or her, the person was not an accused per se. It was only when the statement was sought to be proven in the court of law that the said person stands accused (Kathi Kalu case)[48].

[47] Supra 106
[48] AIR 1961 SC 1808.

3.2.3 The Brain Mapping Test or P300 Test - Legal Status

The technological development had a great impact on the law. The government of various countries including India has taken note of recent development in science and technology and made appropriate legislations to reap the benefit of them. Courts are bound to follow the legislations and enforce the same wherever it is required. As such courts and legislature cannot remain ignorant of the latest scientific advancements in field of Criminal Justice System. Even in cases where appropriate legislation is missing, the courts have to apply the scientific technique in resolving the dispute provided they did not contravene any existing legislation or enactment. One of the examples is that of Brain Mapping test where in many countries of the world, the test is relied upon and admitted in the court of law even though there might not be any express provision for the same[49].

In India, however, the admissibility of Brain mapping has to face prohibitive mandates of Article 20(3) and Article 21 of Constitution. While Article 20(3) prohibits evidence regarding self incrimination, Article 21 deals with the implied right to privacy for an individual. Though DNA and Fingerprinting has been made admissible by various court pronouncements but no authentic ruling regarding Brain Mapping has yet been given. It has been held in **State of Bombay v. Kathi Kalu Oghad**, that taking thumb-impression or fingerprints is not covered by Article 20(3) and is not self-incriminating. "Self-incriminating" means that the accused is compelled to give information from his/her personal knowledge. If logic of the court is accepted, Brain Mapping would not be admissible in court in criminal trial.

Again, law against intrusion of an individual's privacy would not allow Brain mapping evidence to be given in court. The prosecution cannot be allowed to violate the privacy of an individual which even extent to the realm of the Brain of the person. The big question, however, is "Whether the contents of brain are sacrosanct or it can be read and analyzed for betterment of the society?" This question has obtained much importance in view of growing terrorism and technological advances in the commission of the crimes.

[49] The Gene Age- A legal Prospective, organize by centre for DNA Fingerprinting and Diagnostics, Hyderabad and NALSAR university of law, Hyderabad, document prepared by Hon'ble Mr. Justice R.K. Abhichandani, Judge High Court of Gujarat, p. 20.

Of course this new advancement in scientific technology is helpful in detecting lies, solving crimes and apprehending criminals and may prove to be a boon for the Criminal Justice System. However, the Hon'ble Courts in India have yet not accepted this advanced scientific technology completely. But certainly this type of scientific test does provide some evidence or clue about the culpability of the accused which may corroborate other oral testimonies. At best, it is a piece of evidence just like other evidences to be evaluated by Judges according to the fact and circumstances of the case.

The protagonist of Brain Mapping test in India to be administered to an accused or a witness argue that since no statement comes out of the involuntary tests of the offender, no incrimination of the test subject really occurs. Moreover the test is being carried out under the supervision of an expert who can very well depose before the court of law in relation to the tests, the existence of the knowledge of the crime in the Brain of the accused or the witness undergoing the tests. Also, there is no question of protection from compulsory testimony in this particular test. However the courts in India have rejected all these contentions in relation to this test. The Courts are of the opinion that Brain Mapping test administered against the will of the person does violate the Constitutional guarantee to individuals in the country. This stand of the court in Selvi's Case has caused more of the hindrance in criminal investigation and subsequent prosecution. Earlier the court in the landmark Ramachandra Reddy case rejected the contention of the violation of the constitutional guarantee in case a person is being subjected to Brain mapping Test, stating that any question of incrimination only arises when statement inculpating the accused is placed on the records. Whether it is so or not can be ascertained only after the test is administered and not before. Therefore, there is no reason to prevent administration of performing this test upon the accused.

3.2.4 Electronic Evidence - Legal Status

Indian law makers have shown dynamism in replying to the challenge posed by the proliferation of Information technology especially relating to electronic evidence. The Information Technology Act, 2000 which was passed by the Indian Parliament on the 17th of October[50], amended the Indian Evidence Act, 1872 and made electronic evidence admissible in

[50] The United Nations Commission on International Trade Law

Indian court of law. The Information Technology Act, 2000 is based on the UNCTRAL200 Model Law on Electronic Commerce and apart from amending provisions of the Indian Evidence Act, 1872, the Indian Penal Code, 1860 and the Banker's Book Evidence Act,1891, it has recognized transactions that are accomplished with the help of electronic data interchange and other means of electronic communication.

There are mainly two types of evidences that are dealt by the Indian Evidence Act, 1872:

i. Oral Evidence

ii. Documentary Evidence

The definition of 'Evidence' under Section 3 of the Act was amended to meet the requirements laid down by the Information Technology Act, 2000 whereby all the electronic records produced for the inspection of the court are also called 'documentary evidence'. Section 2(1)(t) of the Information Technology Act, 2000 provides for the definition of "electronic records" which 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.

The advancement and the impact of Information Technology on human beings has necessitated the need for admission of Electronic/electronic evidence in court proceedings. The only path to fulfill this need is to ensure that Electronic/electronic evidence is made admissible in Indian Courts and for the same Indian Parliament has enacted relevant laws.

Best Evidence Rule in regard to admissibility of Electronic evidence Law of Evidence mandates that the best evidence should be provided in the court to prove the fact in issue or relevant facts201. Primary evidence as provided in the Indian Evidence Act, 1872 is considered to be the 'best evidence' since it is the best available corroboration of the existence of a fact. This rule has its origins in common law and its application can be **traced back to the 18th Century. In Omychund v. Baker**[51], it was held by Lord Hardwicke that no evidence was admissible unless it was the best that the nature of the case will allow. McCormick on Evidence provides that where

[51] 1745)1 Atk 21: 26 ER 15

the evidences are material, the original writing must be produced unless it is shown to be unavailable for some reason other than the serious fault of the proponent[52].

The aforesaid rule came into existence at a time when copying of a document was done manually by some clerk and the rationale behind the rule was that unless the original is not produced before the court, the document cannot be relied upon as there would be significant chance of error or fraud in relying upon a copy. The draftsman of Indian Evidence Act, 1872 were also found to be in favour of the aforementioned rule and Section 60, 64 and 91 of the Indian Evidence Act exhibits the same. Section 60 of the act states that oral evidence must be direct meaning thereby that it must be stated by a person who has seen, heard, or perceived the fact by that particular sense, and in case of an opinion of an expert it must be stated by that expert who holds that opinion. Section 64 of the Act provides that documents must be proved by primary evidence except in some cases mentioned in Section 65 of the Act. Section 91 of the Act prohibits proving the contents of a written document other than by the document itself.

Two new sections i.e. Section 65-A and 65-B were introduced in the chapter relating to documentary evidence. Section 65-A states that the contents of electronic records may be admitted as evidence, if essentials mentioned in section 65-B are complied with. Section 65-B states that electronic records shall be construed as documents if the computer which generates those electronic records had been regularly in use and the computer had been working properly. It further states that all computer output shall be considered as being produced by the computer itself, whether it has been produced directly or indirectly or there has been any human intervention or not. This provision also provides that computer evidence shall not be treated as hearsay, if essential conditions specified above are truly complied with.[53]

Thus, after the amendments introduced in the Indian Evidence Act, 1872, electronic records have been made admissible as evidence without producing the original.

[52] Charles T. McCormick, "McCormick on Evidence", 4th Edition, West Publication House, p.230

[53] The term `hearsay' is used with reference to what is done or written as well as to what is spoken and in its legal sense, it denotes that kind of evidence which does not derive its value solely from the credit given to the witness himself, but which rests also, in part, on the veracity and competence of some other person. The word `hearsay' is used in various senses. Sometimes it means whatever a person is heard to say. Sometimes it means whatever a person declares on information given by someone else and sometimes it is treated as nearly synonymous with irrelevant. The sayings and doings of third person are, as a rule, irrelevant, so that no proof of them can be admitted. Every act done or spoken which is relevant on any ground must be proved by someone who saw it with his own eyes and heard it with his own ears.

3.2.5 Essential requirement for acceptance of Electronic Evidence

Section 65-A of the Indian Evidence Act, 1872, states that electronic evidence may be proved in accordance with Section 65-B. Hence, every piece of electronic evidence that has to be relied upon must be accompanied by a certificate as provided in Section 65-B. The section states that for admitting electronic evidence in a court of law without any further proof or production of original, a certificate should be given attesting the following.

i. 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 purpose of any activity regularly carried during that period by the person having lawful control over the use of the computer

ii. During the said period, information of the kind contained in the electronic record or from which the information so contained is derived was regularly fed into the computer during the ordinary course of the said activities

iii. Throughout the said period, the computer was operating properly or, if not, then with respect to any period in which it was not operating properly or was out of operation it must not be in a condition so as to affect the electronic record or the accuracy of its contents and-

The aforesaid certificate has to identify the electronic record contained in the statement and describe the manner in which it was produced and further provide the details of the device. Further, the said certificate has to be signed by a responsible

person occupying an official position in relation to the operation of the relevant

activities. The deponent must also wear to the best of his knowledge and belief.205

The certificate requirement which is provided in the Indian Evidence Act,

1872 is a replication of UK law. Section 69 of UK Police and Criminal Evidence

Act, 1984(now stands repealed by Youth Justice and Criminal Evidence Act206) states that electronic evidence shall be admissible in a court of law if the following two conditions are fulfilled:

(i) That there must be no reasonable ground for believing that the statement is inaccurate because of improper use of the computer.[54]

(ii) That the computer must have been operating properly at all material times or at least the part when it was not operating properly, it must not have affected the production of the documents or the accuracy of the contents.

In R v. Shephara209, a woman was accused of shoplifting from a clothing shop in London. When she was arrested she pleaded that she had purchased the item and had done away with the receipt. The prosecution relied on the shop's central computer system records. The legal question that arose before the House of Lords was whether this evidence should fulfill the requirement of Section 69 of the act. Lord Griffiths observed that if the prosecution wishes to rely upon a document produced by a computer, they must comply with Section 69 in all cases. However, the Indian Supreme Court in P.V. Anvar v. P. K. Basheer, clarified an essential difference and stated that the requirement to certification applies only to secondary electronic evidence.

The Hon'ble Supreme Court in State (NCT of Delhi) v. Navjot Sandhu[55] (well known as the Parliament Attack Case) convicted the accused under various provisions of the IPC and POTA, 2002. One of the most crucial piece of evidence relied upon by the prosecution against the accused was his call records. The Hon'ble Court held that cellular phone records are admissible in a court of law and they would be treated as secondary evidence as the primary evidence would be the call server maintained by the telecom operators thereby making it difficult to be brought before the court. However, the court went ahead and held that even if the requirements of section 65-B(4) of Indian Evidence Act, 1872 are not complied with, it would not be a bar to produce the secondary electronic evidence, if the evidence is otherwise admissible under the provisions of Sections 63 and 65 of the Indian Evidence Act, 1872.

[54] Section 69(1)(a), UK Police and Criminal Evidence Act,1984
[55] (2005) 11 SCC 600

CHAPTER 4

4. AUTHENTICATING ELECTRONIC EVIDENCE: 65B, INDIAN EVIDENCE ACT, 1872

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.

Ashwini Vaidialingam

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 relevancies and admissibility of electronic evidence, something that has been recognized by jurisdictions across the world[56].

In 2000, 65B was inserted into the Indian Evidence Act, 1872 ('Evidence Act')[57] 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.

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')[58] . 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.

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

[56] 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.

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

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

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.

4.1 UNDERSTANDING 65B: PRE-ANVAR

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.

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

(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 subsection (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[59]. 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.[60] 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.

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

[59] Indian Evidence Act, 1872, §65B(1).
[60] Indian Evidence Act, 1872, §65B(1).

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. Second, during that period of time, said information must have been regularly fed into the system in the ordinary course of said activities. 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. 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.

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.

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 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.[61] 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. 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

[61] 3 See infra Part II (B), III & IV

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" 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.

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.

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[62]. 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[63]. 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".

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

[62] Supra note 1; J. Hofman, Electronic Evidence in Criminal Cases, 19(3) SACJ 257, 258 (2006)
[63] 9 See infra Part V

demonstrates, the divergent attitudes taken by trial courts towards electronic evidence, has frustrated both these aspirations.

4.2 JUDICIAL HISTORY

The test for admissibility under 65B was considered for the first time in 2003 in State v. Mohd. Afzal ('Mohd. Afzal')[64], 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.[65] 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. They agreed with the prosecution that the certificate 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.

Two years later, this decision was affirmed in appeal by the Supreme Court in State **(NCT of Delhi) v. Navjot Sandhu ('Afsan Guru')**[66]. The Court examined and accepted as sufficient the oral testimony provided by the prosecution witnesses. 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

[64] State v. Mohd. Afzal, (2003) 107 DLT 385.
[65] Id., ¶266.
[66] 6 State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.

evidence to be given in the circumstances mentioned in the relevant provisions, namely, 63 and 65.

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,

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[67].

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.

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.

4.3 REINTERPRETING

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

[67] 1 Societe Des Products Nestle SA v. Essar Industries, (2006) 33 PTC 469 (Del)

admissibility of CDs containing said propaganda on the grounds that the requirements under 65B were not satisfied.[68] 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 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. 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. On this basis, it excludes the applicability of all provisions of the Evidence Act, except 65B.

This pure statutory interpretation is followed by an examination of its own previous decision in Afsan Guru. 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 generalia 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. 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[69].

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 before a statement under 65B can be made. The first of these relates to the method of authentication. The court states that under 65B(4), a certificate 'must' be produced. The obvious corollary is that in the absence of a certificate, the electronic record

[68] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
[69] See supra Part II (A).

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. 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. The Supreme Court reads it to mean that all of the conditions mentioned in subsection (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 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. 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[70]. While the nature of the

[70] Id., ¶14 (c).

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. What is truly unfortunate is that no part of the Supreme Court's decision acknowledges or attempts to explain the deviations made.

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)

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 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.[71] 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. 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.

[71] 9 Id., ¶23.

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**[72] 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.

4.4 LIMITING METHODS OF AUTHENTICATING ELECTRONIC EVIDENCE

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 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. In the absence of a certificate satisfying the Anvar conditions, the evidence was held to be inadmissible.

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.

[72] Ankur Chawla v. CBI, 2014 SCC OnLine Del 6461

[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.

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. 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. 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.

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[74]. 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. 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,

[74] Indian Evidence Act, 1872, §22.

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 .

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. This is unquestionably a question relating to the genuineness of the document.

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. 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. 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. **Starting with R.M. Malkani v. State of Maharashtra[75],** 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

[75] R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471, 23

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.

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

4.5 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. 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. 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' 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. Therefore, Anvar fails in its attempt at setting a higher threshold of authenticity/genuineness of electronic records.

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[76]. 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.

'The effect of the use of computers cannot be left undebated and the need for constructive criticism of the interface between computer industry and the judicial system is apparent for our system of justice to work. The gaps in the law caused by out of-date statutes should be noted and filled at the earliest opportunity by Parliament'

{Kelman and Sizer 1982 Foreword}

[76] See Indian Evidence Act, 1872, §65B(2).

The speed with which information and communication technologies developed over the past fifteen years has created a revolution in both business and individual practices throughout the world. Today more and more transactions take place on open telecommunication networks, such as the Internet, providing people more opportunities to enter online into contracts of all kinds[77]. The worldwide growth of electronic commerce and the developments in the computer and telecommunications sectors have deeply changed the dispatch and accessibility of information, goods, transactions and services. Besides its benefits, the proliferation of computers has also created a number of problems for the law. Many legal rules require the existence of paper records, of signed records, of original records. The law of evidence usually is based on paper records, although oral testimony and other kinds of physical objects have always been part of our courtrooms, too. With the advancement in the activities carried out by electronic means, it becomes imperative to consider that evidence of these activities be available to exhibit the legal rights flowing from them.

When we discuss about the word, cyber it includes computer, networks, data storage devices, cell phones, software, ATMs, internet etc. In nutshell, it includes everything which is somewhere related to computer, internet or somewhere related to technology. Developments in the area of information and communication technology have gone way beyond what the statute-makers could have visualized at the time of enactment of the statute. For instance, concepts, doctrines and gist of such things as documents, writing, systems of recording things etc. have become fundamentally changed or absolutely impractical. The advent of computer has, for example, brought with it totally new forms of record keeping in software - microfilms, microchips, diskettes, flash discs, pen drive etc. that are not covered by any means within the previous meaning of the word "document" which used to be a written matter on a surface. The very basic and simple division of documents into originals and copies has also become unrealistic with respect to the documents transmitted and stored through information and communication technology[78]. For instance, the information recorded or stored in the memory of a computer when printed out on paper, it is not easy to say that the information stored in the memory is a

[77] Mark D. Rasch. 'Criminal Law and the Internet' in the Internet and Business: A Lawyer's guide to the emerging legal issues, Computer Law Association, (last visited on 30 June, 2012).

[78] Andrew I. Chukwuemerie, 'Affidavit Evidence and Electronically Generated Materials in Nigerian Courts' SCRIPT-ed Volume 3 Issue 3 p.176-202 June 2006 (last visited on 11 Dec. 2013).

document or not. Nor is it easy to affirm that the print out is an original or a copy. It is also not easy to categorize an audio tape recording, a video tape recording, a text message or chat recorded on a mobile, an electronic mail on a computer screen, information contained in CDs, VCDs or such other things, as originals or copies. It brings with it many complex issues with regard to evidential aspect of electronic records, whether the erecords are relevant or not, admissible or not, to be treated as original or as hearsay evidence, authenticity of e-evidence in the absence of expert, when tampering can lead to inadmissibility of e-records etc.

These days, technology is playing a major role in everyday routine due to its ease and speed with which information travels to the other party. Emails and chats are the most commonly used electronic means to communicate any kind of information and information communicated through such kind of electronic means, if stored, can be used as evidence in legal suits whether civil or criminal. In civil trials, electronic evidences can be used to expose business and personal records, e.g. claims in case of breach of contract, divorce, harassment, defamation, policy claims, booking railway or air ticket, sale/ purchase of shares, buying or selling of goods etc. etc. In e-contracts, offer and acceptance may take place online, receipts may be created through computers, payment may be made online, hence, the electronic records are generated that may be useful in prosecuting or defending the suit. Whether it is opening a Demat account, purchase of insurance policy, withdrawal of money, transfer of money- everything can be done very easily and promptly with the help of electronic means of communications and every transaction, in the end, leaves behind its traces which can be used as evidences to prove or disprove a fact in case a dispute arises. Now the most important question is the relevancy and admissibility of these evidences. Different countries have difference laws to deal with the electronic evidences.

For the same reasons, there has been an increasing demand from businesses and users for new types of signatures as an effective alternate to the hand-written signature in the electronic environment ensuring integrity, confidentiality and authenticity of information and documents. However, in the hurry to adopt the technology as rapidly advancing as this, the international and municipal lawmakers of various countries have narrowed their focus to usage in evidence conditional on government or regulatory authorization of such records.

Information which has been processed or stored on computer is commonly and progressively a source of evidence in both criminal and civil proceedings[79]. The computerization of business, police and governmental records is already so widespread that many of the everyday transactions such as the purchase of groceries, the withdrawal of money from a bank account, online payments or the making of a telephone call commonly produce computerized data which is generally recorded and stored automatically without any human involvement.4 Such data may have been recorded with specific evidential uses in mind or it may accidentally get an evidential importance which was not imagined at the time of the recording. Test data regularly recorded by the producer of a quality controlled product, with a view to ensuring its specification, may afterward be found helpful in identifying whether the deficiency in product specification was the ground for the breach of contract or it was the malicious intention of party to avoid the contract. In the same way, sales data recorded on a computerized till roll in a department store may be helpful in proving whether the sale alleged by the accused has taken place or it is a case of shoplifting.

Information derived from or stored in computer systems, valuable it may be, can also create a number of evidential problems for the courts.6 It is imperative to understand the electronic evidence and the nature of electronic evidences. Electronically transmitted or stored information that is admitted as evidence at a trial or hearing is electronic evidence[80]. It may include electronic communications such as e-mails, text messages, chats, computer-generated data, computer-stored records, Electronic photographs, website content and social media postings etc. Distinct from any other kind of evidences, it is pretty easy to manipulate the electronic evidences, much easier for a computer expert who deals with them on regular basis. Therefore, extraordinary care and caution must be applied while dealing with such sensitive pieces of evidence[81]. Major threats to electronic evidence are from viruses, electromagnetic or mechanical damages. However, the legal regime should not visualize the internet and data (electronic) records in a negative manner. Keeping in mind the widespread use of ITC, the legal system must aim at facilitating the use of such technologies to best serve the society. The focus must be on weeding out the undesirable

[79] Diana Rowland and Elizabeth Mcdonald, 'Information Technology Law' (1997) p. 375 Cavendish Publishing House, London.

[80] Jonathan D. Frieden and Leigh M. Murray, "The Admissibility of Electronic Evidence under the Federal Rules of Evidence", XVII RICH. J.L. and TECH. 5 (2011

[81] Ishita Chattergee 'Challenges relating to enforcement and admissibility', (2012) 4

while simultaneously encouraging and facilitating the spread and use of technology. With specific reference to evidence, following are considerations to be borne in mind when legislating: the nature of the threshold that should apply to the admissibility of electronic evidence; the burden of proof on the proponent or opponent of the evidence, and the procedural requirements to ensure a proper examination of electronic evidence adduced before the court. The system so devised must be broad to encompass technologies past, present and future. The focus should be on drawing the balance between the sometimes conflicting goals of safeguarding and facilitating electronic transactions (be they commercial or personal) and encouraging technological development with an approach that encourages transparency and uniformity in the legal system.

The evidence to be admissible in court of law must meet certain established parameters. As a general rule, there are 3 requirements for evidence to be admissible in the court of law. These are.

I. Authentication
II. The best evidence rule
III. Exceptions to the hearsay rule If these requirements are not fulfilled, evidence so collected may not be admissible. Thus it becomes essential in case of Electronic evidences to comply with these established principles of Evidence law.

4.1.1 Doctrine of Functional Equivalence

Though according to the doctrine of functional equivalence for every online conduct there ought to be an offline equivalent, yet application of traditional jurisprudential concepts to conduct and activities in cyberspace poses novel and complex problems. Cyberspace is projected as a 'new universe' a parallel universe created and sustained by the world's computers and communications lines. That may be true, but cyberspace cannot be a space beyond law- a kind of legal hinterland where the reach of the national legal systems cannot extend and where greed, malice and treachery can reign supreme. The Final Report of the International Symposium on Freedom of Expression in the Information Society organized by the French National Commission for UNESCO in November 2002 reinforces this view. The Report observes that.

The internet has never been a space beyond the law: national laws apply to it. The offences committed on the internet reflect behaviors that are specific to social life, and which have already found carriers in the traditional media'[82].

4.1.2 Challenges of Electronic Evidence

The most challenging and daunting task which Electronic evidence poses for law enforcement lies in the nature of the electronic data which is latent in nature, can be viewed indirectly only after applying the proper procedure and the process of collecting data may change the data. Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence is latent. In its natural state, we cannot "see" what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence visible. Testimony may be required to explain the examination process and any process limitations. The nature of electronic evidence is such that it poses special challenges for its admissibility in court. To meet these challenges, it is essential to follow proper forensic procedures.

4.1.3 Original -Duplicate Distinction Non-existent

In Electronic environment there is no original or duplicate. Everything is original and everything is duplicate. This raises evidentiary problems. Electronic records challenge this very assumption since with respect to an electronic record everything is an original and everything is a duplicate.

4.5.1 UNCITRAL MODEL LAW OF ELECTRONIC COMMERCE

Articles 5 to 10 of UNCITRAL Model Law of Electronic Commerce deal with evidentiary value of e-records. These articles, for the sake of clear understanding, are provided hereunder.

[82] T. K. Viswanathan, 'Appreciating and evaluating electronic evidence'

4.5.2.1 Legal Recognition of Data Messages (Article 5)

Information shall not be denied legal effect, validity or enforce-ability solely on the grounds that it is in the form of a data message[83].

In other words, Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. It is intended to apply notwithstanding any statutory requirements for a "writing" or an original. That fundamental principle is intended to find general application and its scope should not be limited to evidence or other matters covered in chapter II. It should be noted, however, that such a principle is not intended to override any of the requirements contained in articles 6 to 10. By stating that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message", Article 5 merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. However, Article 5 should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein[84].

4.5.3 Incorporation by Reference (Article 5 bis)

'Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message[85].'

It is intended to provide guidance as to how legislation aimed at facilitating the use of electronic commerce might deal with the situation where certain terms and conditions, although not stated in full but merely referred to in a data message, might need to be recognized as having the same degree of legal effectiveness as if they had been fully stated in the text of that data message[86]. The expression 'incorporation by reference' is often used as a concise means of

[83] UNCITRAL Model Law on e-commerce.
[84] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996),
[85] As adopted by the Commission at its thirty-first session, in June 1998.
[86] Such recognition is acceptable under the laws of many States with respect to conventional paper communications, usually with some rules of law providing safeguards, for example, rules on consumer protection.

describing such situations which is often regarded as essential to widespread use of electronic data interchange (EDI), electronic mail, Electronic certificates and other forms of electronic commerce in an electronic environment. In electronic communications, practitioners should not have imposed upon them an obligation to overload their data messages with quantities of free text when they can take advantage of extrinsic sources of information, such as databases, code lists or glossaries, by making use of abbreviations, codes and other references to such information. Without the legal certainty, there might be a significant risk that the application of traditional tests for determining the enforceability of terms that seek to be incorporated by reference might be ineffective when applied to corresponding electronic commerce terms because of the differences between traditional and electronic commerce mechanisms.

While electronic commerce relies heavily on the mechanism of incorporation by reference, the accessibility of the full text of the information being referred to may be considerably improved by the use of electronic communications. For example, a message may have embedded in it uniform resource locators (URLs) which direct the reader to the referenced document. Such URLs can provide 'hypertext links' allowing the reader to use a pointing device (such as a mouse) to select a keyword associated with a URL[87]. One aim of article 5 bis is to facilitate incorporation by reference in an electronic context by removing the uncertainty prevailing in many jurisdictions as to whether the provisions dealing with traditional incorporation by reference are applicable to incorporation by reference in an electronic environment.

4.5.4 Writing (Article 6)

I. Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

II. Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

[87] Id

Enactment Guide to UNCITRAL Model Law provides:

Article 6 is intended to define the basic standard to be met by a data message in order to be considered as meeting a requirement (which may result from statute, regulation or judge-made law) that information be retained or presented "in writing" (or that the information be contained in a "document" or other paper-based instrument). It may be noted that article 6 is part of a set of three articles (articles 6, 7 and 8), which share the same structure and should be read together.

In the preparation of the Model Law, particular attention was paid to the functions traditionally performed by various kinds of 'writings' in a paper-based environment. For example, the following non-exhaustive list indicates reasons why national laws require the use of 'writings'.

(1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves.

(2) to help the parties be aware of the consequences of their entering into a contract

(3) to provide that a document would be legible by all

(4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction

(5) to allow for the reproduction of a document so that each party would hold a copy of the same data

(6) to allow for the authentication of data by means of a signature

(7) to provide that a document would be in a form acceptable to public authorities and courts

(8) to finalize the intent of the author of the 'writing' and provide a record of that intent

(9) to allow for the easy storage of data in a tangible form

(10) to facilitate control and subsequent audit for accounting, tax or regulatory purposes and

(11) to bring legal rights and obligations into existence in those cases where a writing' was required for validity purposes. However, in the preparation of the Model Law, it was found that it would be inappropriate to adopt an overly comprehensive notion of the functions performed by

writing. Existing requirements that data be presented in written form often combine the requirement of a 'writing' with concepts distinct from writing, such as signature and original.

Thus, when adopting a functional approach, attention should be given to the fact that the requirement of "writing" should be considered as the lowest layer in a hierarchy of form requirements, which provide distinct levels of reliability, traceability and unalterability with respect to paper documents. The requirement that data be presented in written form (which can be described as a "threshold requirement") should, thus, not be confused with more stringent requirements such as "signed writing", "signed original" or "authenticated legal act". For example, under certain national laws, a written document that is neither dated nor signed, and the author of which either is not identified in the written document or is identified by a mere letterhead, would be regarded as a 'writing' although it might be of little evidential weight in the absence of other evidence (e.g., testimony) regarding the authorship of the document. In addition, the notion of inalterability should not be considered as built into the concept of writing as an absolute requirement since'writing' in pencil might still be considered a 'writing' under certain existing legal definitions. Taking into account the way in which such issues as integrity of the data and protection against fraud are dealt with in a paper-based environment, a fraudulent document would nonetheless be regarded as a "writing". In general, notions such as "evidence" and "intent of the parties to bind themselves" are to be tied to the more general issues of reliability and authentication of the data and should not be included in the definition of a 'writing'.

4.5.6 Admissibility and Evidential Weight of Data Messages (Article 9)

'(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence.

(a) on the sole ground that it is a data message or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in

which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor'.

Enactment Guide to UNCITRAL Model Law with regard to Article 9 provides: The purpose of article 9 is to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value. With respect to admissibility, paragraph (1), establishing that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form, puts emphasis on the general principle stated in article 4 and is needed to make it expressly applicable to admissibility of evidence, an area in which particularly complex issues might arise in certain jurisdictions.

The term "best evidence" is a term understood in, and necessary for, certain common law jurisdictions. However, the notion of "best evidence" could raise a great deal of uncertainty in legal systems in which such a rule is unknown. States in which the term would be regarded as meaningless and potentially misleading may wish to enact the Model Law without the reference to the "best evidence" rule contained in paragraph (1). As regards the assessment of the evidential weight of a data message, paragraph (2) provides useful guidance as to how the evidential value of data messages should be assessed (e.g., depending on whether they were generated, stored or communicated in a reliable manner).

It may also be noted that paragraph (1) reinforces, in the context of contract formation, a principle already embodied in other articles of the Model Law, such as articles 5, 9 and 13, all of which establish the legal effectiveness of data messages.

4.5.7Retention of Data Messages (Article 10)

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied

(a) the information contained therein is accessible so as to be usable for subsequent reference and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

Article 10 establishes a set of alternative rules for existing requirements regarding the storage of information e.g., for accounting or tax purposes that may constitute obstacles to the development of modern trade.

Enactment Guide to UNCITRAL Model Law with regard to Article 10 provides: Paragraph (i) is intended to set out the conditions under which the obligation to store data messages that might exist under the applicable law would be met. Subparagraph (a) reproduces the conditions established under article 6 for a data message to satisfy a rule which prescribes the presentation of a "writing". Subparagraph (ii) emphasizes that the message does not need to be retained unaltered as long as the information stored accurately reflects the data message as it was sent. It would not be appropriate to require that information should be stored unaltered, since usually messages are decoded, compressed or converted in order to be stored.

4.5.8 Admissibility of Electronic Records

The UNCITRAL Model Law on Electronic Commerce (1996)19 deals with the admissibility and evidentiary weight of data messages in Article 9(1)[88].

[88] Article 9 (i) deal with admissibility while paragraph (ii) of the same article deals with evidential weight of the data messages.

The article mandates that in any legal proceeding, the rules of evidence should not apply to exclude a data message, either, solely because it is a data message (electronic format)21 or, if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form[89].

The Model law mandates that if there is a legal requirement of an original, this requirement will be met by a data message if it satisfies the two tests laid down in article 13.

The criteria for assessing integrity are also mentioned. Electronic signatures can also be used to ensure the integrity of messages or information[90]. The Model law states that information in the form of a data message shall be given due evidential weight, after considering the reliability of the manner in which the data message was generated, stored or communicated, reliability of the manner in which the integrity of the information was maintained, the manner in which the originator was identified, and any other relevant factor.

I. Writing

The Model law states that where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference. It also states that this applies whether the requirement is in the form of an obligation or whether the law simply provides consequences if it is not in writing. Finally, it states that this shall not apply in such cases where the government of each state feels that it should not apply.

II. ENGLISH LAW OF EVIDENCE

English law of evidence developed its basic common law rules and principles long before anyone could ever have envisaged the appearance of computer generated data; and those rules have not always proved adaptable to new kinds of evidence[91]. It is an irrefutable fact that the revolution in microelectronic technology resulting in advanced methods of capturing, storing, retrieving,

[89] Article 9 (1)(b)
[90] Art. 8(1)(a), (b).
[91] Supra n. 3

receiving and analysing information by computers - highlighted by Kelman and Sizer - has not been fully assimilated into the English law of evidence[92].

A party to a civil or criminal litigation in which computer evidence may be involved is likely to have at least three specific concerns regarding that evidence, namely: (1) will it be permissible to adduce that evidence at the trial or in other words, is such evidence legally admissible; (2) if so, how cogent will that evidence be; and (3) to what extent and by what methods may such evidence be open to challenge? Of these (1) and (3) raise specific questions of law while it is more difficult to deal with (2) as the cogency of computer evidence may vary from near-conclusiveness to total ineffectiveness, depending on the evidence itself and on the circumstances of the case.31 However, there are certain procedure specified to avoid doubts or objections being raised as to the cogency or integrity of the information stored in them, though not having the backing of law. Courts may take account of commercially accepted „best practices" while evaluating the cogency of the evidence. Concern (1) cannot always be separated from concern (2) as failure to adopt procedures for safeguarding the accuracy and integrity of computerized records may result in a court or judge refusing to recognize the authenticity or inadmissibility of data derived from them.

Common law rule was subject to a variety of common law and statutory exceptions and these too were often complex and technical in nature, some of them ill-considered and subject to frequent amendment. For example, the Criminal Evidence Act, 1965, designed to admit hearsay in trade and business records, was passed as an interim measure, but few could have foreseen that the broader provisions set out in sections 68-72 of Police and Criminal Evidence Act, 1984 relating to documentary hearsay by which it was replaced, would in turn be replaced only four years later by sections 23-28 of the Criminal Justice Act 1988 provisions which unfortunately contained serious drafting errors. Sections 23-28 of the 1988 Act have now been repealed. In criminal cases, the meaning of hearsay and the circumstances in which it is admissible are now governed by Chapter 2 of part 11 of the Criminal Justice Act 2003. Civil Evidence Act 1995deals with the evidentiary value of electronic records with regard to civil matters while Criminal Justice Act 2003 deal with regard to criminal matters. The complexity of the legislation

[92] Solomon E. Salako, Computer Printout as Admissible Evidence A Critical Legal Study of Section 24 of The Criminal Justice Act 1988'

dealing with the admissibility of computer generated evidence has led Courts into different directions, resulting in a somewhat confusing case law. The apparent confusion stems from the qualification given to computer-generated evidence: does it constitute hearsay or real evidence.

III. Evidential Aspect in Criminal Cases

a. Rules of Admissibility

In criminal proceedings, the English Law of evidence remains characterized by complexity and excessive technicality. There is no concept of "free appreciation of evidence". It will not necessarily suffice to show that a given item of evidence is relevant to some disputed issue in the case. Relevance is clearly important as no court will waste time listening to a case manifestly irrelevant[93]. General rule for an evidence to be admissible is that the document must be original and not a copy. Apart from being original, evidence must be direct not hearsay except in the cases where rules of exclusion apply.

b. The Hearsay Rule

The rule against hearsay has always been surrounded by an aura of mystery and has been treated with excessive reverence by many English judges. Traditionally the English courts have been reluctant to allow any development in the exceptions to this exclusionary rule, regarding hearsay evidence as being so dangerous that even where it appears to be of a high probative caliber it should be excluded at all costs[94]. The hearsay rule is expressed as 'Express an implied assertions of persons other than the witness who is testifying, and assertions in documents produced to the court when the witness is testifying, are inadmissible as evidence of the truth of that which was asserted. As far as computer evidence is concerned, the most troublesome rule by far is the hearsay rule. This rule might better be known as the rule against second-hand evidence. it ordinarily requires facts in issue to be proved by the oral testimony of persons who have first-hand (i.e. personal) knowledge of those facts.40 It is not ordinarily permissible to prove such facts by the testimony of some other person to whom the facts have been narrated by the original witness nor is that witness's written account acceptable in place of his or her oral testimony.

[93] Supra n. 3 at p.376.
[94] R. A. Clark, 'The Changing Face Of The Rule Against Hearsay In English Law'.

Cross-examination of witnesses is considered to be a vital ingredient in the forensic search for truth, but one cannot cross-examine a document[95].

The hearsay rule was designed to exclude unreliable gossip and rumour but unfortunately it is not always so discriminating. The danger of reliable evidence being excluded as a result of the hearsay rule is illustrated by the notorious decision of the House of Lords in Myers v. Director of Public Prosecution.

The House of Lords decision in Myers v DPP[96]. demonstrated graphically how what appeared to be very cogent documentary evidence could be rendered inadmissible by strict adherence to the hearsay rule. In this case the defendant had been charged with various counts involving the theft of cars. His alleged modus operandi was to buy a wrecked car and then steal a car in good condition, as nearly as possible identical to the wrecked car. He would then disguise the stolen car as the wrecked car including the transfer of number plates, engine number and chassis number. The stolen car was then sold together with the log book of the wrecked car. It was not possible, however, to transfer the block number from one car to another since this was indelibly stamped on the engine. The prosecution wished to put in evidence microfilms of record cards kept by workers at the Longbridge Austin Car Factory on which had been recorded the engine number, chassis number and block number of each vehicle as it was being assembled. If admissible these records would have been almost incontrovertible evidence that the log books did not belong to the cars and that the cars were stolen. The House of Lords held that these records were inadmissible because they had not been brought to court by a witness who had been responsible for compiling the records and who could testify as to the accuracy of the records.

The consequence of the Myers case was that it was left to Parliament to extend the exceptions to the hearsay rule in criminal cases by making admissible certain types of documentary hearsay.43 To plug the gap through which the accused was exonerated, the Criminal Evidence Act 1965 was enacted. The Act provides

(1) In any criminal proceedings where direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, on production of

[95] Id.
[96] [1965] 1 AC 1001.

the document, be admissible in evidence of that fact if- (a) the document is, or forms part of, a record relating to any trade or business and compiled, in the course of that trade or business, from information supplied (whether directly or indirectly) by persons who have, or may reasonably be supposed to have personal knowledge of the matters dealt with in the information they supply; and (b) the person who supplied the information recorded in the statement in question is dead, or beyond the seas, or unfit by reason of his bodily or mental condition to attend as a witness, as cannot with reasonable diligence be identified or found, or cannot reasonably be expected (having regard to the time which elapsed since he supplied the information and to all the circumstances) to have any recollection of the matter dealt with in the information he supplied[97].

After Myres, court again stumbled to the erroneous conclusion that information stored on computers must necessarily be a form of hearsay. In Pettigrew45, the court of Appeal held that a trial Judge had been wrong to admit in evidence an automatically produced computer printout from the Bank of England, which tended to prove that bank notes found in the accused‟s possession came from a batch which had been stolen in burglary with which he was charged.46 The Court of Appeal considered that since they were being asked to rely on the accuracy of the printout, and since no witness could claim first-hand information it contained, the content of the printout must be hearsay[98]. This provoked a very influential article by Professor J.C. Smith:

JC Smith, 'The Admissibility of Statements by Computer

1981 Criminal Law Review 337

Where information is recorded by mechanical means without the intervention of a human mind, the record made by the machine is admissible in evidence, provided, of course, it is accepted that the machine is reliable. An elementary example is a maximum and minimum thermometer. These records two items of information in the course of 24 hours and there is no doubt that a witness could give evidence of the reading he took from it if that was relevant to the issue before the court. A Fortiori, the instrument itself could be produced, if it were possible to do so while it

[97] Supra n. 30
[98] Id.

still bore the relevant readings. It would not be necessary to call a professor of physics to prove how a thermometer works because that is surely such a matter of common knowledge as to be judicially noticed. The same is true of a camera which photographs an event or a tape- recorder which records a conversation, where the event or conversation is in issue or is relevant to the issue before the court. A radar speedometer, similarly, makes a record of an event- the speed of a passing vehicle and is not different in legal principle from thermometer. The physics is more complicated and less comprehensible to the layman but we are all so completely convinced by our scientific colleagues that it works that the matter is again judicially noticed.

The computer differs from these other instruments only in that it can perform a variety of functions instead of only one. For that reason, it is necessary to have evidence - such as that which was admitted in Pettigrew - to establish the nature of the operations which the computer has been programmed to perform. It performs those operations just as mechanically as the thermometer or the camera. Of course, the programmer may make a mistake but so may be the person who, for example, devises the scale on the thermometer. This consideration goes weight rather than admissibility. In any event it certainly has nothing to do with the hearsay rule.

The information produced by the Bank of England's computer seems to be exactly the same in principle as that produced by a camera, a tape recorder, a radar speedometer or the radar set in The Statute of Liberty.49 When it discards a note, it records that fact. If a movie camera could photograph the rejected notes as they were ejected from the machine, the film would be admissible to prove the number of the rejected notes. The computer has a different and more complex method of recording the same information; but there is no difference in principle. Hearsay invariably relates to the information which has passed through a human mind. This information never did so.

The logic of Professor Smith's argument was subsequently accepted by the court of Appeal, and in R. v. Wood, the Lord Chief Justice set out to classify the different kinds of computer evidence that might come before the courts. Admission of Computer recordings is now well established by cases such as **Castle v. Cross50and R. v. Spiby**[99].In the former case, the Divisional Court held that a printout produced by a Lion Intoximeter breathe analysis machine stating that the motorist

[99] (1990) 91 Cr. App R 186

had failed to provide a sufficient specimen for analysis constituted real evidence rather than the hearsay and in the latter case the court of Appeal similarly categorized a printout produced by a hotel computer showing detail of telephone calls made by hotel guests. The calls had been automatically recorded by the computer in order that guests could be charged for the same.

c. Admissibility of E-records

Computer-related evidence falls into two clear categories. Each consists of information output by a computer, either as a result of some operation it has performed or as a hard copy of data stored in some permanent form (e.g. on magnetic disk). The first category is where the computer is used as a compact filing cabinet in which are stored records of information provided to it by human beings. These records might be almost anything - observations of the weather, the serial numbers of cheques, notes of a meeting - but their essential characteristic for the purposes of admissibility is that they originate in an observation by a human. The second category consists of records generated directly by a computer, whether that machine stores the record or another[100] . Information stored on or produced by computers may thus contain admissible or inadmissible hearsay or in other cases, it may constitute real evidence. The crucial thing to look for is the reproduction of factual information keyed in by human agency.55 This will be hearsay if tendered as evidence of those facts (if the court is asked to rely upon the information being correct) and the same will be true of material which is derived, albeit in the processed form from such information. Unless the operator can testify, at first hand, as to the accuracy of the input (as was done in R. v. Wood), the output of the computer will then be hearsay. Computerised bank records concerning customers‟ accounts represent typical examples of such evidence. Assuming that the computer printout is being tendered as a true record of the relevant transactions, it will be hearsay except insofar as it shows automatic transactions (direct debits etc.) performed by the computer itself without direct human intervention or automatically monitored customer transactions, such as withdrawals from ATMs.

d. Evidential Aspect in Civil Cases

The civil courts in England and Wales have in the past faced problems caused by lack of adequate provision for the admissibility of computer evidence. The most widely publicized

[100] Id.

difficulties were those connected with collection of the notorious community charge (orpoll tax) in the early 1990s[101]. The poll tax legislation made the magistrates' courts responsible for the judicial enforcement of unpaid demands for this tax, and local authorities throughout the land relied on their computerized records in order to identify and sue defaulters. As magistrates‟ court would accordingly be presented with computer printouts showing the defendant D owed so many pounds in unpaid poll tax; but was such evidence admissible In R v. Coventry Justice, ex p Bullard, the applicants obtained orders from the Divisional Court, quashing liability orders imposed by magistrates on the basis of computer evidence adduced by the local authority. The problem faced by the local authority was that most recognised exceptions to the hearsay rule were at that time inapplicable in civil proceedings heard in magistrates‟ courts.

In R v. Coventry Justice, ex p Bullard (1992) 95 Cr App R 175, Mann LJ stated that

The decision in Myres led to a statutory abrogation of the hearsay rule in the Criminal justice Act 1965 and there were later abrogations in the Civil Evidence Act 1968 and in the Police and Criminal Evidence Act 1984. None of these abrogation is available in civil proceedings in magistrates‟ courts, where, subject to the Evidence Act 1938 and to its own established common law exceptions, the hearsay rule remains fully applicable.

We know nothing of the operation of the computer which produced the printout. However, it must be the case that the outputs are of or are derived from information implanted by a human. They are thus hearsay and inadmissible as evidence of either the amounts which the applicants are liable to pay or of the amounts which are unpaid.

e. Civil Evidence Act 1995

As a result of reforms introduced by the Civil Evidence Act 1995, admissibility problems of the Coventry Justices kind will no longer be capable of troubling the civil courts or tribunals. The hearsay rule is, for most Practical purposes, abolished insofar as it applies to civil proceedings. The introductory words of the Act states- An Act to provide for the admissibility of hearsay evidence, the proof of certain documentary evidence and the admissibility and proof of

[101] Supra n. 3 at p.390.

official actuarial tables in civil proceedings; and for connected purposes, itself suggests that the Act was passed for the admissibility of hearsay evidence.

4.6 US LAW OF EVIDENCE

Most information is now communicated, generated, or stored electronically[102]. As Chief United States Magistrate Judge Grimm of the United States District Court for the District of Maryland acknowledged in Lorraine v. Markel American Insurance Company[103], because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try'.75 The prevalence of electronic evidence has required no substantial changes to the Federal Rules of Evidence. The seminal decision addressing the admissibility of electronic evidence is Judge Grimm's 51-page opinion in Lorraine v. Markel American Insurance Company, which reads as a comprehensive guide to the admission of electronic evidence.76 In Lorraine, Judge Grimm describes a decision model for addressing the admission of electronic evidence, which, unsurprisingly, is nearly identical to the one many proponents apply to the admission of more traditional forms of evidence. The Lorraine model suggests that the proponent of electronic evidence focus first on relevance, asking whether the electronic evidence has any tendency to make some fact that is of consequence to the litigation more or less probable than it would be otherwise[104] . Second, the proponent should address authenticity, asking if he can present evidence demonstrating that the electronic evidence is what it purports to be. Third, the proponent must address any hearsay concerns associated with the electronic evidence, asking if it is a statement by the declarant, other than one made by the declarant while testifying at the trial or hearing, offered for the truth of the matter asserted, and, if the electronic information is hearsay, whether an exclusion or exception to the hearsay rule applies. Fourth, the proponent must address the application of the original documents rule. Fifth, and finally, the proponent should consider "whether the probative value of the electronic evidence is substantially outweighed by the danger of unfair prejudice", confusion, or waste of time. Careful consideration of these traditional evidentiary principles will permit a proponent to successfully

[102] 'Electronic Discovery in Litigation', INFOLOGY.
[103] Jonathan L. Moore, 'Moore on Upgrading the Federal Rules of Evidence to Accommodate ESI', LEGAL INFORMATICS BLOG (June 11, 2010, 9:04 PM)
[104] Id. at 540 (citing Fed. R. Evid. 401 which will be discussed later in this chapter).

admit electronic evidence. The court is referring to rules in the Federal Rules of Evidence; the full interpretation by the court reads.

Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI relevant as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it authentic as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being as offered as evidence an original or duplicate under the original writing rule, or if not, is there admissible secondary evidence to prove the content of ESI (Rule 1001-1008) and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.

4.6.1 Federal Rule of Evidence

There are hundreds of cases dealing with this topic in the United States and they are based on a variety of state laws. As there is no uniformity in the wording and requirements provided for in such statutes, there are often conflicting decisions which can create some confusion as to the admissibility of computer-generated evidence. Although there exists no nation-wide comprehensive law on the admissibility of electronic evidence, the Federal Rules of Evidence provide the requirements for the authentication of documentary evidence, a prerequisite step for the admission of such evidence. These rules apply to proceedings in United States courts. These rules should be construed so as to administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination.

4.6.2 Relevancy of Evidence

There are certain rules under Federal Rule of Evidence dealing with the evidentiary value of electronic evidence. Rules 401 and 402 of the Federal Rules of Evidence address this fundamental question of “logical relevance”. Rule 401 provides for the definition of the

relevance evidence. Rule 402 provides relevant evidence is admissible and irrelevant evidence is inadmissible. Rule 403 provides for the reasons to exclude relevant evidence.

A. Test for Relevant Evidence (Rule 401)

Evidence is relevant if

a) It has any tendency to make a fact more or less probable than it would be without the evidence and

b) The fact is of consequence in determining the action.

Problems of relevancy call for an answer to the question whether an item of evidence, when tested by the processes of legal reasoning possesses sufficient probative value to justify receiving it in evidence.84 Thus, assessment of the probative value of evidence that a person purchased a revolver shortly prior to a fatal shooting with which he is charged is a matter of analysis and reasoning. Relevancy is not an inherent characteristic of any item of evidence but exists only as a relation between an item of evidence and a matter properly provable in the case.86 If the evidence makes a fact more or less probable, it is relevant. The rule uses the phrase, fact that is of consequence to the determination of the action ‘ to describe the kind of fact to which proof may properly be directed.

B. General Admissibility of Relevant Evidence (Rule 402)

- Relevant evidence is admissible unless any of the following provides otherwise: • the United States Constitution
- a federal statute
- these rules or other rules prescribed by the Supreme Court. Irrelevant evidence is not admissible.

The provisions that all relevant evidence is admissible, with certain exceptions, and that evidence which is not relevant is not admissible are a presupposition involved in the very conception of a rational system of evidence Not all relevant evidence is admissible. The exclusion of relevant evidence occurs in a variety of situations and may be called for by these rules, by the Rules of

Civil and Criminal Procedure, by Bankruptcy Rules, by Act of Congress, or by constitutional considerations.

4.6.3 Analogy for Electronic Evidence

Keeping in mind the Rule 401, electronic evidence will also be relevant if makes a fact more or less probable and evidence for such fact may be adduced. Rule 402 also seems equally applicable to electronic evidence according to which irrelevant evidence is not admissible as well as when otherwise provided by the United States Constitution or a federal statute these rules or other rules prescribed by the Supreme Court. Rule 403 makes electronic evidence, even if logically relevant, irrelevant if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.

A court is most likely to invoke Rule 403 to exclude otherwise relevant electronic evidence where such evidence: (1) 'contain{s} offensive or highly derogatory language that may provoke an emotional response. (2) consists of computer animations or simulations where 'there is a substantial risk that the jury may mistake them for the actual events [at issue] in the litigation 93 (3) consists 'of summaries of voluminous electronic writings, recordings or photographs under Rule 1006;"94 or (4) is potentially unreliable or inaccurate.

4.6.4 Authenticity of Evidence

Before being admitted, evidence must be authenticated - that is, the proponent of the evidence must make a showing sufficient to support a finding that the evidence is what it purports to be.96 Authenticity is often the central battleground for determining admissibility of electronic evidence due to the common perception that electronic record may be readily altered to appear to be something they are not[105]. Judge Grimm also noted in Lorraine that "Counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation".98 The proponent of electronic

[105] Keiko L. Sugisaka, 'Admissibility of E-Evidence in Minnesota, New Problems or Evidence as Usual?'35 WM. Mitchell L. Rev. 1453, 1459 (2009).

evidence also has to swim against the tide of a judiciary that is highly skeptical of such evidence.99 Perhaps nowhere is such skepticism better articulated than in a decade-old decision from the United States District Court for the Southern District of Texas addressing the admissibility of information discovered on the Internet

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any website from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules.

The Southern District of Texas's early distrust of electronic evidence has been shared and discussed with equal force by Federal Courts across the country.101 However, some courts seem less willing to dismiss electronic evidence based on the mere fact that such evidence is susceptible to alteration[106] . Indeed, some courts will admit, for example, e-mails, after a threshold showing of authenticity and then leave the determination of whether the e-mails were altered for the jury.

A. Authenticating or Identifying Evidence (Rule 901)

a. IN GENERAL. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

[106] United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) (The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents and copies of those documents.

b. EXAMPLES. The following are examples only-not a complete list-of evidence that satisfies the requirement:

1. Testimony of a Witness with Knowledge.

Testimony that an item is what it is claimed to be.

2. Non-expert Opinion About Handwriting.

A non-expert‟s opinion that handwriting is genuine, based on a familiarity with it that was not acquired for the current litigation.3. Comparison by an Expert Witness or the Trier of Fact.

A comparison with an authenticated specimen by an expert witness or the trier of fact.

4.6.7 Authentication of E-mails and Text Messages

There is no form of ESI more ubiquitous than e-mail, and it is the category of ESI. In modern litigation, it is rare when a case does not involve some communication by e-mail or text message. Such a communication is easily authenticated if the proponent of the communication can secure the admission of the author or sender of the communication that he drafted or sent the communication. Additionally, a recipient, or non-recipient with knowledge that the communication was sent, may authenticate an e-mail or text message. Also, a witness with knowledge of how the responsible Internet service providers or wireless telephone carriers sent and received an e-mail or text message, and how such messages are stored and retrieved, may authenticate such messages. The threshold determination for authentication will often vary with the piece of evidence and the court the evidence is before.

CHAPTER-5

5. CONCLUSION AND SUGGESTIONS

With the advancements in computer technology, telecommunication and information technology, the use of computer networks has gained considerable popularity in the recent past. Computer networks serve as channels for electronic trading across the globe. Business communities as well as individuals are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. It is easier to store, retrieve and speedier to communicate. People are aware of these advantages but they are reluctant to conduct business or conclude business transactions in the electronic form due to lack of legal framework .

In the WTO Work Programme on Electronic Commerce, electronic commerce means the production, distribution, marketing, sale or delivery of goods and services by electronic means. Broadly defined, electronic commerce encompasses all kinds of commercial transactions that are concluded over an electronic medium or network. Essentially, the internet and e-commerce covers three main types of transactions, i.e. business-to-consumer (B2C), business-to-business (B2B), and business-to-government (B2G). For every commercial transaction, there must be contract, oral or in writing, to make it legally enforceable, so is it with regard to e-commerce, for which the transactions are done through e-contract.

The power of internet to reach the world carries with it a variety of legal issues, such as validity of e-contract, how to form contracts, authenticity of e-contract, evidentiary value of e-record, jurisdiction and alternative dispute resolution which are briefly discussed in chapter 1. Authorities seeking to apply their laws in traditional ways or to expand legal control over international links faced many challenges due to the global nature of internet. Due to the apprehension and distrust of the electronic medium in the mind of businesses and consumers, the United Nations provided a Model Law designed to afford certainty and security for all parties involved in electronic data transactions that was ultimately finalized in 1996 and provided legal recognition to e-commerce taking place online. As India is signatory to it has to revise its laws as per the said Model Law. Keeping in view the urgent need to bring suitable amendments in the existing laws to facilitate e-commerce, Information Technology Bill was introduced in the Parliament which was passed by both the Houses of Parliament and received the assent of

President on 9th June, 2000. Legal framework for e-commerce has been provided by the IT Act 2000, which makes India only the twelfth country in the world which has such a comprehensive legislation for e-commerce. This Act also effects consequential amendments in the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Books Evidence Act, 1891 and the RBI Act 1934 to bring them in line with the requirements of Electronic transactions. England has enacted Electronic Communications Act 2000 and the Electronic Signature Regulations Act 2002 to provide legal enforceability to Electronic transactions. In US, the Uniform Electronic Transactions Act (UETA) and the Uniform Commercial Information Transactions Act (UCITA) deal with the electronic transaction. Electronic Signatures in Global and National Commerce Act (E-sign) is another federal legislation providing federal recognition to the UETA. Chapter 1 throws light briefly on these legislations. Various issues discussed in subsequent chapters are also introduced in chapter 1.

Two principal hurdles which stand in the way of facilitating ecommerce are the requirements as to writing and signature for legal recognition. At present many legal provisions assume the existence of paper based records and records that bear signatures. The law of evidence is traditionally based upon paper based records and oral testimony. Since ecommerce eliminate the need for paper-based transactions, hence to facilitate e-commerce, the need for legal changes had become an urgent necessity and the IT Act 2000 has done some suitable changes to facilitate e-commerce.

Chapter 2 of the thesis discusses various issues related to contract formation. First issue discussed is whether the electronic contracts have legal validity or not. There was no traditional law denying validity to electronic transaction, however, its validity and enforceability was doubtful in the absence of any clear provision providing validity. Section 4 of the IT Act has provided legal recognition to electronic records equating it with the written documents and section 5 has provided legal recognition to Electronic signatures.1 At present, all legal systems in the world have provided legal recognition to electronic commerce.

E-contracts can be formed, generally, either through the medium of email or website. We often come across these e-contracts in our everyday life but are unaware of the legal complexities connected to it. Contracts entered through e-mail are somewhat similar to sending letters to each other though the time taken to send or receive it is very minimal. Sometimes, it

may bounce back or doesn't even reach to the other party. Web-wrap agreement is web based agreement which requires assent of the party by way of clicking the "I agree" or "I confirm" link. Web based agreement is similar to standard form contract whose terms and conditions are determined in advance and the party has to either accept it or reject it entirely. When it comes to legality/enforceability of such e-contracts entered between two or more parties, we need to look into basic provisions of laws regarding the contracts which are given in The Indian Contract Act 1872 unless the IT Act 2000 specifically provides contrary.

One of the issues discussed in chapter 2 is whether computer-generated agreements should be enforceable as legally binding contracts or not. Efforts are made to draw an analogy between the formation of electronic contract and traditional contract. There is certainly nothing about the subject matter of computer-generated agreements under any law which should render them unenforceable but the laws prevalent doesn't even lay down any express provisions when it comes to formation of such contracts and the difficulties arise only because of the legal doctrine of contract law which is based on an idealized model of communication between natural persons. Though the IT Act provides for some provisions with respect to the e-commerce but these provisions are restricted to the legality of the e-commerce and the security of such a transaction but the Act doesn't lay down any specific provision with respect to the formation of such contracts.

The Indian Contract Act 1872 is the basic law encompassing all rules dealing with the formation of contract. This law deals with the issue when contract takes place between two natural persons. With the advancement of internet, it is felt that the Indian Contract Act lags behind rapidly developing technology. As the IT Act is also silent about formation of contract, we have to look towards the Indian Contract Act to decide the legal issues involving internet. Indian judiciary has also not got much opportunity to determine law on e-contract.

First issue relating to contract formation is whether web advertisement2 is to be treated as shop display making it as invitation to offer or should it be treated as an offer. English Law is based on common law and The Indian Contract Act is also based on English Law. By drawing an analogy with Carlill v. Carbolic Smoke Ball Co. Ltd. case, web advertisements can be equated with the invitation to offer unless it clearly indicates the web advertiser's intention to be bound upon acceptance. Web advertisements will be invitations to offer unless the language used on

website indicates the intention of the seller to sell turning the invitation to treat into an offer. Hence, the fact is to be decided on case by case basis considering all the facts including the language used on the website. In US case of Leftowitz v. Great Minneapolis Surplus Stores, it was held that advertising a fur stole under the concept of „first come first serve basis" constitute an offer as the language of the advertisement makes clear the intention of the seller to sell the goods on first come basis indicating the acceptance by the first comers. The basic thought behind limiting the alleged offer to invitation to offer is that a merchant can never know how many might be interested in the purchase and therefore it won't be fair for the merchant to supply inn case of lack of supply. In case of online sale through fully automated software, it is quite possible to have a count on the quantity that is offered for sale and once it is sold, the system will show the product as out of stock. However, to avoid any kind of technical mishap, „terms and conditions" clause of the websites provides ample liberty to the seller to cancel the contract and absolve seller from any kind of legal liability in case breach of contract takes place on ground of certain contingency like lack of supply, out of stock etc.

In line with the common law principle, section 4 of the Indian Contract Act provides that offer is complete when it comes into the knowledge of the offered and the communication of an acceptance is complete as against the proposer- when it is put in a course of transmission to him so as to be out of the power of the acceptor and against the acceptor- when it comes to the knowledge of the proposer. With regard to communication of offer or acceptance online, section 12 compels that the communication is complete on the receipt of acknowledgement by the originator which impliedly results into a conflicting situation than that is prescribed in the Indian Contract Act concluding that communication of offer or acceptance will not be complete unless acknowledgement is received by the sender. US law doesn't warrant for the requirement of acknowledgement while English law requires for it. Indian Law now has conflict in law regarding communication of offer and acceptance in traditional and online contract.

With regard to communication of acceptance, postal and receipt rules still apply according to the analogy drawn in case of online contracts as well. As per traditional law, postal rule applies for communication done through non-instantaneous means of communication and receipt rule applies where instantaneous means of communication such as phone, telex etc. is used. By Entores Ltd v Miles Far East Corporation case, the contract is complete in case of

instantaneous means of communication only when the acceptance is received by the offered, hence, the receipt rule applies. Contracts entered through websites, chat, video conferencing etc. are instantaneous means of communication as telephone and telex is, hence, receipt rule applies to them. E-mail is treated at par with the simple letter issued through post; hence, postal rule applies to it. By virtue of the postal rule as envisaged in Adams v. Lindsall case, a complete contract comes into existence when the properly stamped and addressed letter is put in the course of transmission so as to be out of the power of the acceptor and it is immaterial whether that letter reaches to the offered or not. However there is big difference between letter sent through post and an e-mail sent via internet. Email communication is almost instantaneous in comparison to communication via post. Email messages split into various packets and sent via different routes. There is also possibility that e-mail not reaching in totality. As analogy is drawn between emails and letter sent via post, e-mails are covered under non instantaneous means of communications, however, application of postal rule is doubtful due to nearly instantaneous nature of communication. Section 13 of the IT Act provides the time of receipt of acceptance (i) when it reaches the designated information system or (ii) information system of the address (if not designated) or when it is retrieved by the addressee (if sent to a system other than designated). The IT Act has not specifically mentioned any difference as to instantaneous or no instantaneous means of communication. Hence, section 13 applies equally to both means of communication. By deducing meaning of section 13, it can be very clearly concluded that receipt is not complete at the time of dispatch, so dispatch rule can't apply. Receipt happens not at the time when it is received by the addressee but when it enters the information system of the addressee, so „receipt rule" can also not be applied in strict sense. However, the analogy is drawn more in favour of „receipt rule. English courts still apply the traditional methods of determining the time of communication of acceptance: dispatch rule for non-instantaneous means of communications and receipt rule for instantaneous means of communication. While United States has adopted only receipt rule to determine the time of communication of acceptance whatever the means of communication is. In Morrison v. Thoelke, Florida District Court of United States has reiterated the applicability of the receipt rule stating that „this decision to apply the mailbox rule is limited to any prospective application to circumstances involving the mails and doesn't purport to determine the rule possibly applicable to cases involving other modern means of communication.

Meeting of mind or knowledge is an essential requirement for contract formation in traditional way. A binding contract comes into existence only when it is assented by the offered that implies the knowledge of the offer and meeting of mind. There can be no acceptance of the offer without meeting of mind. In **Stover v. Manchester City Council, UK court** has laid down that an offer is an expression of willingness to contract on specified terms, made with the intention that it is to be binding once accepted by the person to whom it is addressed. Regulation 9 of Electronic Commerce (EC Directive) Regulation 2002 have also impliedly accepted the formation of contract through electronic agent but is silent as to the requirement of meeting of mind". In the case of Lalmal Shukla v. Gauri dutt, Indian court has also held that in order to constitute a contract there must be an acceptance of the offer and there can be no acceptance unless there is knowledge (meeting of mind) of the offer. However, with the introduction of electronic agent which is attributable to its originator, communication is done automatically by the software even without the knowledge of the originator. Hence, the concept of „meeting of mind" is not relevant in case of electronic transactions. In US, the UETA (section 14) has expressly recognized that an electronic agent may operate autonomously and contemplated contracts formed through/by the interaction of electronic agents as formed by the individuals. UCITA also contains provisions supporting the ability of electronic agents to make binding contracts. Keeping in mind the mushrooming growth of online trading with the help of electronic agent, there is dire need that specific provision is to be incorporated in the IT Act to override the requirement of „meeting of mind" as specified by the Indian Contract Act.

In India, CPC is the law to deal with the jurisdictional issues which applies „cause of action" or consequence " rule to decide the jurisdictional issue. US apply the „minimum contact" test and „purposeful availment" test to assume jurisdiction over a foreign national and England applies „most real and substantial connection to the action" test and „justice" rule for the same. In International Shoe Co. v Washington, 5US court held that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he must have certain minimum contacts with it such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice. The **Court in Zippo Manufacturing Company v Zippo Dot Com,** Inc. also came to the same conclusion holding that „no matter where parties may fall on the spectrum, they should recognize that engaging in commercial

activity over the internet may spawn liability in foreign jurisdictions if that activity consists of something more than simple posting of information. In England, Lord Keith in **Rockware Glass Ltd v Mac Shannon** laid down that the appropriate forum will be the country with which the action has the most real and substantial connection. **By Spiliada Maritime Corpn. v Cansulex Ltd. case**, the Court laid down connecting factors "and these will include not only factors affecting convenience or expense (such as availability of witnesses), but also other factors such as the law governing the relevant transaction…and the place where the parties respectively reside or carry on business". Need is to devise a uniform and coherent law on jurisdiction to ensure batter and safe legal environment for the business community.

In order that the transition from the traditional to the Electronic form of commerce is made with minimum discomfort, it is critical to ensure that governments adopt a cautious, velvet-glove kind of approach to policy development in respect of e-commerce. The resulting product must be transparent and completely integrated with the traditional legal system, so that both can coexist efficiently, until such time as the transition is complete. In order to achieve this harmonization, while at the same time retain the best interests of the consumers and businessmen alike, policy makers should respect the unique nature of the medium and understand that widespread competition and increased consumer participation in choices are the defining features of the Electronic age that is newly upon us.

6.1 SUGGESTIONS

1. Due to the section 12 of the IT Act 2000, acknowledgement is binding to complete the communication. Impliedly, in case of contract, no offer or acceptance will be treated as sent unless acknowledgement is received by the person concerned. Due to the acknowledgement factor, time of communication of offer and acceptance also gets changed to the time of receipt of acknowledgement' creating a very contradictory situation in contrast to traditional rules provided under the Contract Act. Hence, the need is to clearly incorporate a provision specifying the time when the communication of offer or acceptance will be completed. Author feels that Requirement of, Acknowledgement should not be binding.

2. Section 4 of the Contract Act provides that the communication of offer is complete when it comes into the knowledge of the offered. On close examination of sections 12 and 13 of the IT Act, it becomes clear that the test of knowledge on the part of offered as provided under section 4 of the Contract Act for finding whether communication of an offer is complete are inapplicable to electronic Communications. The addressee may use an automated process for sending acknowledgement which means, in a given situation, the addressee may not be aware of the electronic record of which acknowledgement of receipt has been sent. It means that the knowledge element necessary for determining the time for communication of acceptance in postal communications is irrelevant in case of electronic communications. As Sections 12 and 13 don't deal with the term knowledge, it is suggested that, as it is contrary to the Contract Act, it should have been clearly mentioned in the IT Act.

3. Determining the time of contract formation is essential since it identifies the moment of transfer of ownership and risk, among others. With regard to the rule of acceptance, need is to specially incorporate a provision specifying that only receipt rule is to apply whether the means of communication is instantaneous like website, chat etc. or non-instantaneous like email, unless otherwise agreed by the parties.

4. In case of malfunctioning of the information system or the file is not intelligible or usable; IT Act is silent about it. Author feels that the e-record should be treated as not received by the addressee.

5. Both UCITA and UETA address the issue of mistake after the contract has been formed. In an automated transaction, a consumer is not bound if the mistakes were caused by an electronic error. An electronic error' is defined as "an error in an electronic message created by a consumer using an information processing system if a reasonable method to detect and correct or avoid the error was not provided. Both uniform laws allow the consumer to avoid the effect of mistake by notifying the other party promptly on learning of the error and by taking reasonable steps that conform to the other party's reasonable instructions, to return to the other person, or to destroy the consideration received, if any, as a result of the erroneous electronic record. Under The Indian Contract Act, agreement is void if both parties are under mistake of fact. Mistake of law as in force

in India is no ground to avoid a contract. In case of online contract, it is quite a possibility that the other party residing in other country may not be having knowledge as to law in force in India. Hence, the need is to make a clear provision in The IT Act to clarify the position as to mistake of law.

REFERENCE

• Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa reported as AIR 1987 SC 1454

• See,Principles of Statutory Interpretation, 9th Edition by Justice G.P. Singh - Chapter V, Synopsis IV at pages 318 & 319

• Union of India and Anr. V. G.M. Kokil and Ors. [(1984) SCR196]

• Chandavarkar Sita Ratna Rao v. Ashalata S. Guram [(1986)3SCR866]

• ANVAR P.V. V. P.K. BASHEER AND OTHERS [MANU/SC/0834/2014]

• Sanjay Singh Ramrao Chavan v. Dattatray Gulabrao Phalke [MANU/SC/0040/2015]

• Ankur Chawla v. CBI [MANU/DE/2923/2014]

• Abdul Rahaman Kunji v. The State of West Bengal [MANU/WB/0828/2014]

• Jagdeo Singh v. The State and Ors. [MANU/DE/0376/2015] 2015 CRI L.J. 3976 S.C.

• State of Madhya Pradesh Vs. Madanlal 2015 CRI L.J. 4186 S.C.

• Jogendra Yadav & Oths Vs. State of Bihar AIR 2015 (NOC) 1226 (Bom)

• Animal and birds Charitable Trust & others Vs. Municipal Corporation of Greater Mumbai and others. AIR 2015 (NOC) 1132 (Bombay)

• Bangana Co-operative Housing Society Ltd. Mumbai Vs. Mrs. Vasanti Gajanan Nerulkar