ADMISSIBILITY AND PROOF OF ELECTRONIC RECORDS

"Law must be conscious of the speed of change in society and accordingly adapt"

A. SARAVANA KUMAR. B.A. B.L.,
REGISTRAR (I.T) / DISTRICT JUDGE,
TAMIL NADU STATE JUDICIARY.

Synopsis

1. **Electronic Record Defined Under IT Act**
2. **Other Provisions relating to electronic record**
3. **Computer, Computer System and Computer Network**
4. **Forms of Digital evidence or records**
5. **Computer output and output devices**
    - **5.1 CPU**
    - **5.2 Display Monitor (CRT/LCD/TFT etc.) screens of Mobile Phones, if switched on**
    - **5.3 Smart Cards, Dongles and biometric scanners etc**
    - **5.4 Digital Cameras**
    - **5.5 Smart Phones**
    - **5.6 Hard Disc Drives**
    - **5.7 Local Area Network (LAN) Card or Network Interface Card (NIC)**
    - **5.8 Modems, Routers, Hubs and Switches**
    - **5.9 Servers**
    - **5.10 Network cables and connectors**
    - **5.11 Printers**
    - **5.12 Scanners**
    - **5.13 Copier**
    - **5.14 CD & DVD Drives**
    - **5.15 Digital Watches**
    - **5.16 Fax machine**
    - **5.17 Global Positioning System (GPS)**
    - **5.18 Keyboard & Mouse**
6. **Admissibility of electronic record or electronic document**
7. **Requirement of Section 65-B of Indian Evidence Act**
8. **Proving various kinds of electronic records**
    - **8.1 Proof of identity of mobile telephone**
    - **8.2 Compact Disc**
    - **8.3 Tapping Of Phone Calls**
    - **8.4 Proof of tape recorded conversation**
    - **8.5 Proof of Call Data Record**
    - **8.6 Proof of CCTV Footage**
    - **8.7 Body Worn Cameras**
    - **8.8 Proof of Email**
    - **8.9 Proof of Hard Disc**
    - **8.10 Admissibility of Satellite Sketch**
    - **8.11 ATM**
    - **8.12 Proof of Whatsapp messages**
    - **8.13 Emoji**
    - **8.14 Memory Cards**
    - **8.15 Proof of Copy of computer generated statement of account**
9. **Others**
    - **9.1 Presumption of electronic records**
    - **9.2 YouTube and Liability of Intermediary**
    - **9.3 Altering computer programme or source is an infringement of copy right**
    - **9.4 Rights of the accused and digital records**

At the swipe of everyone's finger a tech-savvy world exists. The virtual world is not a real world. But it creates several opportunities for the commission of cyber crimes and also creates several forms of evidences to deny or uphold one's civil or other rights. The admissibility of electronic evidence gains momentum, both in civil and criminal matters, with the steady rise in the dependency of electronic form of communications. The biggest operational challenge to the courts is to decide authenticity, veracity, genuineness and reliability of the electronic records. Apart from statutory provisions, individual judges must have some basic knowledge of computer operation.

A computer can be a tool for the commission of an offence and it can be a repository of electronic evidence. Realising the importance of computer knowledge to Judges, the Hon'ble Supreme Court in the case of **Vijendra Kumar Verma v/s Public Service Commission, Uttarakhand & Ors**. 2011 (1) SCC 150 has observed that the Indian judiciary is taking steps to apply e-governance for efficient management of courts. In the near future, all the courts in the country will be computerized. In that respect, the new judges who are being appointed are expected to have basic knowledge of the computer operation. It will be unfair to overlook basic knowledge of computer operation to be an essential condition for being a judge in view of the recent development being adopted. Therefore, the Supreme Court is of the considered opinion that requirement of having basic knowledge of computer operation should not be diluted.

Electronic records are relevant to prove any facts. In **Shafhi Mohammad v/s State of Himachal Pradesh** 2018 AIR(SC) 714 , the Hon'ble Supreme Court has held that it will be wrong to deny to the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved. Though such devices are susceptible to tampering, no exhaustive rule could be laid down by which the admission of such evidence may be judged. Electronic evidence was relevant to establish facts. Scientific and electronic evidence can be a great help to an investigating agency.

In electronic evidence jurisprudence, it must be bear in mind that possession of electronic evidence is one thing and proof of the same is another thing.

1. ELECTRONIC RECORD DEFINED UNDER IT ACT:

Electronic records are placed at par with other forms of record. In ordinary common parlance, an electronic record is information recorded by a computer which is produced or received in initiation, conduct or completion of an agency or individual activity. For example, electronic record includes, email messages, word processed

documents, electronic spreadsheets, digital images and data bases. However, the term "electronic record" is defined in Section 2(t) of the Information Technology Act, 2000 as follows:

> *"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."*

In paper documents we use ink for inputs. Likewise, in digital world, any data is fed into the computer system in **'**binary' format. The word **'meta data'** means data that provides crucial information about other data. In other words, it is data about data. However, speaking legally, expression "data" is defined in Section 2(o) of the Information Technology Act as follows:

> *"Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."*

Therefore, it is clear that as per the Information Technology Act - 2000, 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.

Two separate and special provisions deal with electronic evidence. Section 59 says that all facts, except the contents of documents or electronic records, may be proved by oral evidence. It is based on the fundamental principle as best evidence rule. Section 65-A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65-B. Thus, Section 65-A provides for a special procedure for proving of contents of electronic record. In furtherance thereof, Section 65-B provides for the procedure.

2. Other Provisions relating to electronic record:

The other relevant provisions provided in the Information Technology Act in respect of electronic records are as under:

i. Section 4 relates to the legal recognition of electronic records. It states that if any information or matter is rendered or made available in an electronic form, and

accessible so as to be unusable for a subsequent reference, shall be deemed to have satisfied the requirements of law which provides that information or any other matter shall be in writing or in the typewritten form.

ii. Section 5 relates to the legal recognition of digital signatures.

iii. Section 6 relates to the use of electronic records and digital signatures in Government and its agencies.

iv. Section 7 related with retention of electronic records. It states that if any law provides that documents, records, or information are required to be retained by for any specific period, then, that requirement shall be deemed to have been satisfied if the same is retained in electronic form.

Moreover, digital evidence is information of probative value that is stored or transmitted in binary form. Digital evidence is not only limited to that found on computers but may also extend to include evidence of digital device such as telecommunication or electronic multimedia devices. While so, it is appropriate to understand what is computer, computer system and computer network.

3. <u>Computer, Computer System and Computer Network:</u>

The I.T. Act defines computer in clause (i) of Section 2(1) of the Act. According to the definition, 'computer' means any electronic, magnetic, optical or other high speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. 'Computer system' is defined in clause (1) of Section 2(1) of I.T. Act, as to mean a device or collection of devices, including input and output support devices which are programmable, capable of being used in conjunction with external files which contain computer programmes, electronic instructions, data storage and retrieval and communication control. The I.T. Act also defines 'computer network' in clause (j) of Section 2(1) of the Act, which reads as under:

> *(j) Computer network means the interconnection of one or more computer through- (i) the use of satellite, microwave, terrestrial line or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.*

While interpreting Section 2(1) of the IT Act, in **Syed Asifuddin V/S State of Andhra Pradesh** 2006 (1) ALD Cri 96: 2005 CriLJ 4314 it has been observed in Para 12 that a reading of clauses (i), (j) and (1) of Section 2(1) of the I.T. Act would show that any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

Computers work through source code. It is the source of a computer. It contains declaration, instructions, functions, loops and other statements which act as instruction for the program on how to function. While dealing with Computer source code, it has been stated in **Syed Asifuddin v/s State of Andhra Pradesh** 2006 (1) ALD Cri 96: 2005 CriLJ 4314, in Para 13 that a computer has to be appropriately instructed so as to make it work as per its specifications. The instructions issued to the computer consists of a series of OS and is in different permutations and combinations. This machine language can be in different forms in different manner, which is called computer language. The communicator as well as the computer understand "a language" and mutually respond with each other. When specified or particular instructions are given, having regarded to the capacity of the computer it performs certain specified functions. The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. Known as source code in computer parlance, the programme written in whatever computer language by the person who assembled the programme are not seen by the users. A source code is thus a programme as written by the programmer. Every computer functions as a separate programme and thus a separate source code.

It has been further observed in Para 14 of the above judgment that computer source code or just source or code may be defined as a series of statements written in some human readable computer programming language constituting several text files but the source code may be printed in a book or recorded on a tape without a file system, and this source code is a piece of computer software. The same is used to produce object code. But a programme to be run by interpreter is not carried out on object code but on source code and then converted again. [Diane Rowland and Elizabeth Macdonald: Information Technology Law; Canandish Publishing Limited; (1997). p. 17] Thus, source code is always closely guarded by the computer companies, which develop different function specific computer programmes capable of handling various types of functions depending on the need. The law as we presently see is developing in

the direction of recognizing a copyright in the source code developed by a programmer. If source code is copied, it would certainly violate copyright of developer.

4. Forms of Digital evidence or records:

Digital evidence can be found in emails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programmes, spreadsheets, internet browser histories databases, contents of computer memory, computer backups, computer print out, global positioning system tracks, logs from hotel's electronic door locks, digital video or audio files. In this context, it is also better to understand what is computer output and output devices.

5. Computer output and output devices:

Computer output means data generated by a computer. This includes data produced at software level. Devices that produced physical output from the computer are creatively called output devices. Any information that has been processed by and sent out from a computer or similar device is considered as output. At this juncture, it is better to understand certain important devices and its uses.

5.1 CPU:

The device itself may be evidence of component theft, counterfeiting etc. The device contains digital devices with all the files and folders stored including deleted files and information, which may not be seen normally. Cyber Forensic is used to image, retrieve and analyze the data.

5.2 Display Monitor (CRT/LCD/TFT etc.) screens of Mobile Phones, if switched on:

All the graphics and files that are open and visible on the screen in switched on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs and through description in seizure memo.

5.3 Smart Cards, Dongles and biometric scanners etc:

The device itself, along with the identification/authentication information of the card and the user, level of access, configurations and permissions.

5.4 Digital Cameras:

The device can be looked for images, videos, sounds, removable cartridges, time & date stamps.

5.5 Smart Phones:

Much information can be obtained from these devices like address book, appointment calendars/information, documents, emails, phone book, messages (text & voice), emails passwords etc.

5.6 Hard Disc Drives:

The basic storage location of any computer is HDD. The HDD can be both internal and as well as external. Internal HDD is integrated into the computer system. External HDD can be attached though USB portals and includes like pen drive or flash drive. It is generally referred to as secondary storage of the computer system. The primary being the Random Access Memory (RAM).

5.7 Local Area Network (LAN) Card or Network Interface Card (NIC):

The device itself and also MAC (Media Access Control) address can be obtained.

5.8 Modems, Routers, Hubs and Switches:

In routers, configuration files contain information related to IP addresses etc.

5.9 Servers:

Information like last logins, mails exchanged, contents downloaded, pages accessed etc. can be obtained.

5.10 Network cables and connectors:

Network cables are used to trace back to their respective computers. Connectors help in identifying the types of devices that are connected to the computers.

5.11 Printers:

The device has data like number of prints last printed and some maintain usage logs, time & date information. If attached to a network, they may store network identity information. In addition, it can also be examined for figure prints.

5.12 Scanners:

The device itself, having the capability to scan, may help to prove illegal activity.

5.13 Copiers:

Copies may contain some documents both physical and electronic, user usage logos, time and data stamps.

5.14 CD & DVD Drives:

These devices store files/data in which evidence can be found.

5.15 Digital Watches:

Some latest digital watches contain information like address book, notes, appointment calendars, phone numbers, emails etc.

5.16 Fax machine:

These devices contain some documents, phone numbers, send/receive logs, film cartridges that can be considered.

5.17 Global Positioning System (GPS):

The device may provide travel logs, home location, previous destinations, way point coordinators, way point name etc.

5.18 Keyboard & Mouse:

These devices can be examined for fingerprints.

6. Admissibility of electronic record or electronic document:

The word 'admissible' means the evidence which can be admitted in court and taken on record. The concept of admissibility is completely different from concept of relevancy and probative value of the evidence adduced. Section 65 B makes electronic evidence admissible, it does not dispense with the relevancy and probative value. In **State of Uttar Pradesh Vs. Raj Narain** (1975)4 SCC 428, it has been held that facts should not be received in evidence unless they are both relevancy and admissible. The Apex Court in **State of Bihar Vs Sri Radha Krishna Singh** 1983 AIR 684 has further held that admissibility of document is one thing and its probative value is quite another thing – these two aspects cannot be combined. In **Arjun Panditrao Khotkar** (2020 (5) CTC 200) the Hon'ble Supreme Court has observed that Section 65 differentiates between existence, condition and contents of a document. Whereas existence goes to '*admissibility*' of a document '*contents*' of a document are to be proved after a document becomes admissible in evidence. Section 22-A of the Evidence Act provides that if the genuineness of the electronic record produced is questioned, the oral evidence would be admissible as to the contents of the electronic records. However, the Hon'ble Madras High Court reiterated the same in **Santhoshkumar Vs State rep. by Inspector of Police Perundurai Police Station** 2021(2) MLJ (Crl) 225 wherein it has been held that oral evidence cannot take the place of section 65-B (4) certificate. Further Section 4 of IT Act also provides that if a document in electronic form is (a) rendered or made available in an electronic form and (b) accessible so as to be usable for a subsequent reference, then it would be sufficient compliance. Moreover, the electronic evidence is made admissible by the amendment of section 92 of Information Technology Act-2000 in the Indian Evidence Act. Section 3(2) of Indian Evidence Act states that evidence includes all documents including electronic records produced for the inspection of the court. Such documents are called as documentary evidence. As stated supra, the word 'electronic records' is defined under section 2(t) of Information Technology Act. It has

been held in **Thana Singh Vs Central Bureau of Narcotics (2013)2 SCC 590)** that a digital charge sheet was held to be a document and it can be accepted as electronic record. Hon'ble Supreme Court has directed to supply of charge sheet in electronic form additionally.

7. Requirement of Section 65-B of Indian Evidence Act :-

Primary evidence means when the document itself is produced for the inspection of the Court . In **Anvar P V V/S P K Basheer And Others** 2014 LawSuit(SC)783 in Para 24 it is clarified that primary evidence of electronic record was not covered under Sections 65A and 65B of the Evidence Act.

The expression "document" is defined in Section 3 of the Evidence Act to mean any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.

In Anvar PV (stated supra), it is observed in Para 14 that any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B. Section 65B deals with the admissibility of the electronic record. The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer. It may be noted that the Section starts with a non-obstante clause. Thus, notwithstanding anything contained in the Evidence 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 a document only if the conditions mentioned under sub- Section (2) are satisfied, without further proof or production of the original. The very admissibility of such a document, i.e., electronic record which is called as computer output, depends on the satisfaction of the four conditions under Section 65B(2). Following are the specified conditions under Section 65B(2) of the Evidence Act :

i. The electronic record containing the information should have been produced by the computer during the period over which the same was regularly used to store or process information for the purpose of any activity regularly carried on over that period by the person having lawful control over the use of that computer.

ii. The information of the kind contained in electronic record or of the kind from which the information is derived was regularly fed into the computer in the ordinary course of the said activity.

iii. During the material part of the said period, the computer was operating properly and that even if it was not operating properly for some time, the break or breaks had not affected either the record or the accuracy of its contents; and

iv. The information contained in the record should be a reproduction or derivation from the information fed into the computer in the ordinary course of the said activity.

Under Section 65B (4) of the Evidence Act, if it is desired to give a statement in any proceedings pertaining to an electronic record, it is permissible provided the following conditions are satisfied:

a. There must be a certificate which identifies the electronic record containing the statement;

b. The certificate must describe the manner in which the electronic record was produced;

c. The certificate must furnish the particulars of the device involved in the production of that record;

d. The certificate must deal with the applicable conditions mentioned under Section 65B(2) of the Evidence Act; and

e. The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device.

It is further clarified in Anvar PV (stated above) that the person need only to state in the certificate that the same is to the best of his knowledge and belief. Most importantly, such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), Video Compact Disc (VCD), pen drive, etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence. All these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic record sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

In **Arjun Panditroa Khotkar Vs Kailsh Kushanrao Goraytyal** 2020(5) CTC 200 : 2020(7)SCC 1**,** the Hon'ble Supreme Court has held as follows :

> *"The applicability of procedural requirement under Section 65-B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded. In such case, procedure under the said sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in the absence of certificate under Section 65-B(4) of the Evidence Act, which party producing cannot possibly secure. Thus, requirement of certificate under Section 65- B(4) is not always mandatory.*
>
> *Accordingly, we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section 65-B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by the court wherever interest of justice so justifies*."

Next important position of law to be bear in mind is that only if the electronic record is duly produced in terms of Section 65B of the Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort can be made to Section 45A – opinion of examiner of electronic evidence.

The above said position has been well explained in **Arjun Panditroa Khotkar Vs Kailsh Kushanrao Goraytyal** 2020(5)CTC 200 : 2020(7)SCC 1, wherein the Hon'ble Supreme Court has held in Paras 21 to 23 that Sections 65A and 65B of the Evidence Act is proof of information contained in electronic records. The marginal note to Section 65A indicates that "special provisions" as to evidence relating to electronic records are laid down in this provision. The marginal note to Section 65B then refers to

"admissibility of electronic records". Section 65B(1) opens with a non-obstante clause, and makes it clear that any information that is 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 a document, and shall be admissible in any proceedings without further proof of production of the original, as evidence of the contents of the original or of any facts stated therein of which direct evidence would be admissible. The deeming fiction is for the reason that "document" as defined by Section 3 of the Evidence Act does not include electronic records. Section 65B(2) then refers to the conditions that must be satisfied in respect of a computer output, and states that the test for being included in conditions 65B(2(a) to 65(2(d)) is that the computer be regularly used to store or process information for purposes of activities regularly carried on in the period in question. The conditions mentioned in sub-sections 2(a) to 2(d) must be satisfied cumulatively. Under Sub-section (4), a certificate is to be produced that identifies the electronic record containing the statement and describes the manner in which it is produced, or gives particulars of the device involved in the production of the electronic record to show that the electronic record was produced by a computer, by either a person occupying a responsible official position in relation to the operation of the relevant device; or a person who is in the management of "relevant activities" – whichever is appropriate. What is also of importance is that it shall be sufficient for such matter to be stated to the "best of the knowledge and belief of the person stating it"

It has been held in **Anvar P V v/s P K Basheer And Others** 2014 LawSuit(SC)783 at Para 14 that the Evidence Act does not contemplate or permit the proof of an electronic record by oral evidence if requirements under Section 65B of the Evidence Act are not complied with, as the law now stands in India. It has been further reiterated **in Ravinder Singh VS State of Punjab 2022(7) SCC 581** that the certificate under Section 65B(4) of the Evidence Act is mandatory to produce electronic evidence and that the oral evidence in the place of such certificate cannot possibly suffice.

However, interestingly, while deciding the question as to who is to give certificate under section 65-B of the Evidence Act, in **Shafhi Mohammad v/s State of Himachal Pradesh** 2018 AIR(SC) 714 at Para 11 it has been held that the applicability of procedural requirement under Section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded. In such case, procedure under the said Sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving,

such document is kept out of consideration by the court in absence of certificate under Section 65B(4) of the Evidence Act, which party producing cannot possibly secure. Thus, requirement of certificate under Section 65B(h) is not always mandatory. Accordingly, we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section 65B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies.

However, regarding the interpretation of section 65-B of the Indian Evidence Act, a Bench of Three judges made reference to the Honb'le Larger Bench of the Supreme Court in the case of Arjun Panditrao Khotkar Vs Kailash Kushanrao Gorantyal (Civil Appeal No. 20825-20826 dated 14 July, 2020) wherein the Hon'ble Supreme Court (Four Judges Bench) has **overruled the judgment rendered in Shafhi Mohammad's case** and upheld the law down in the PV Anvar case.

As held in Arjun Panditroa Khotkar (*stated supra*), only if the electronic record is duly produced in terms of Section 65-B of the Evidence Act, would the question arise as to the genuineness thereof and in that situation, resort can be made to Section 45-A opinion of Examiner of Electronic Evidence.

It is also pertinent to bear in mind that non-production of certificate at an earlier stage is not fatal, it is a curable defect. The Hon'ble Supereme Court, in **Union of India & Ors v/s CDR Ravindra Vs Desai** (2018 Law Suit(SC) 358) has held as follow :

> *"We are in agreement with the aforesaid findings. Learned counsel for the appellants rightly argued that non-production of the certificate under Section 65-B of the Indian Evidence Act, 1872 on an earlier occasion was a curable defect which stood cured".*

8. **Proving various kinds of electronic records:**

There are various forms of electronic records. Let us consider some of the important electronic records often produced before the court of law and how it can be proved.

8.1 Proof of identity of mobile telephone:

There is no point of doubt that the mobile phone is a computer. Often it is a moot question as to whether how to prove the identity of mobile phone. Before knowing it we may now consider in brief the technological aspects of a cell phone and how it works.

In **Syed Asifuddin v/s State of Andhra Pradesh** 2006 (1) ALD Cri 96: 2005 CriLJ 4314, at Para 15,16,17,18,and 19 the working of cell technology is explained in detail as follows:

> *Alexander Graham Bell invented telephone in 1876. This enabled two persons at two different destinations to communicate with each other through a network of wires and transmitters. In this, the sound signals are converted into electrical impulses and again re-converted into sound signals after reaching the destination. The radio communication was invented by Nikolai Tesla in 1880, which was formerly presented by Guglielmo Marconi in 1894. A combination of telephone technology and radio technology resulted in radio telephone, which became very popular as technology advanced. Two persons can communicate with each other through radio telephone without there being any intervention of network of wires and other infrastructure. The radio signals travel through atmosphere medium and remain uninterrupted as long as the frequency at which radio signals travel is not disturbed. The science realized that the radio telephone communication required heavy equipment by way of powerful transmitter and that it can facilitate only 25 people to use the system. The problem was solved by communication technology by dividing a large area like a city into small cells and any two persons connected to a cell system - at a time receive 800 frequencies and crores of people can simultaneously communicate with each other at the same time. That is the reason why the term 'cell mobile phone or cell phone.*
>
> *In the cell technology, a person using a phone in one cell of the division will be plugged to the central transmitter, which will receive the signals and then divert the signals to the other phone to which the same are intended. When the person moves from one cell to other cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower when the telephone user moves from one division to another. [How Cell Phones Work? See website - http://electronics, howstuffworks.com. Much of the information on technological aspects of Cell Phones is taken from this. Cell phone, it looks the database and diverts the call to that cell phone by picking up*

frequency pair that is used by the receiver cell phone.] Another advantage in a cell phone compared with radio phone is that when the radio phone is used, one person can talk at a time as both the persons can communicate simultaneously and also receive sound signals simultaneously.

All cell phone service providers like Tata Indicom and Reliance India Mobile have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider. To understand how the cell phone works, we need to know certain terms in cell phone parlance. System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing. If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range. When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring. When MTSO gets a call intended to one.

The essential functions in the use of cell phone, which are performed by the MTSO, is the central antenna/central transmitter and other transmitters in other areas well coordinated with the cell phone functions in a fraction of a second. All this is made possible only by a computer, which simultaneously receives, analyses and distributes data by way of sending and receiving radio/electrical signals.

So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the

phone. It is a combination of several computer chips programmed to convert analog to digital (Analog - Anything analogous to something else).

Analog computer - A computing machine so designed and constructed as to provide information in terms of physical quantities analogous to those in which the problems are formulated.

Digital - 1. Of, pertaining to, or like the fingers or digits 2. Digitate. 3. Showing information, such as numerals, by means of electronics: digital watches.

Digital computer - An electronic computing machine which receives problems and processes the answers in numerical form, especially one using the binary system. (See "The New International Webster's Comprehensive Dictionary of the English Language", Encyclopeadic Edition, 2003 edn., pp. 52 and 358).] and digital to analog conversion and translation of the outgoing audio signals and incoming signals. This is a micro processor similar to the one generally used in the compact disk of a Desktop computer. Without the circuit board, cell phone instrument cannot function.

Such being the functionality of a cell phone, the question is whether a cell phone is a computer? In **Syed Asifuddin** (stated supra) it is held that it is not possible to accept the submission that a cell phone is not a computer. Even by the very definition of the computer and computer network as defined in IT Act, a cell phone is a computer which is programmed to do among others the function of receiving digital audio signals, convert it into analog audio signal and also send analog audio signals in a digital form externally by wireless technology.

As to burden of proof, in the case of **Arun Maruthi Wahchaure Vs State of Maharastra,** Crl Appeal No. 1291 of 2012 dated 19.3.2015, at page 13, it has been laid down that whenever the identity of mobile number is questioned, it is the duty of the investigation agency to prove the IMEI number of the mobile instrument number. Therefore, it is clear that identity of the mobile number can be proved by proving IMEI number.

8.2 <u>COMPACT DISC:</u>

A compact disc is a portable storage medium that can be used to record, store and play back audio, video and other data in digital form. It is available in many formats like CD-ROM, CD-I (inter active), CD-RW (re writable), CD-R (Recordable), Photo CD, and Video CD etc.,

In **Shamsher singh Verma v/s State of Haryana** Criminal Appeal No. 1525 OF 2015 dated 24 November, 2015 : 2015 Law Suit(SC) 1145 it is made it very clear that the definition of 'document' in Evidence Act includes the compact disc and it is also a document. Therefore, in **Balasaheb Gurling Todkar and Ors vs. State of Maharashtra and Ors** (2015 Law Suit(Bom) 1060, it has been held that in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.,

A case on the point is **K K Velusamy v/s N Palanisamy**, SC, 2011 LawSuit (SC)271) wherein the appellant involved in that case wanted to cross-examine the witnesses with reference to the admissions made during some conversations, recorded on a compact disc (an electronic record). While deciding the same, the Supreme Court has observed as follow at Para 7:

> *"The amended definition of "evidence" in section 3 of the Evidence Act, 1872 read with the definition of "electronic record" in section 2(t) of the Information Technology Act 2000, includes a compact disc containing an electronic record of a conversation. Section 8 of Evidence Act provides that the conduct of any party, or of any agent to any party, to any suit, in reference to such suit, or in reference to any fact in issue therein or relevant thereto, is relevant, if such conduct influences or is influenced by any fact in issue or relevant fact, and whether it was previous or subsequent thereto. In R.M Malkani vs. State of Maharastra - AIR 1973 SC 157, this 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. The SC 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".*

Another interesting question arose as to when and how the admissibility of CD can be questioned before the Court of law. The question is answered in **Sonu @ Amar v/s State Of Haryana,** 2017 Law Suit(SC)704 at page 27 which run as follows:

> *"Ordinarily an objection to the admissibility of evidence should be taken when it is tendered and not subsequently. The objections as to admissibility of documents in evidence may be classified into two classes: (i) an objection that the document which is sought to be proved is itself inadmissible in evidence; and (ii) where the objection does not dispute the admissibility of the document in evidence but is directed towards the mode of proof alleging the same to be irregular or insufficient. In the first case, merely because a document has been marked as 'an exhibit', an objection as to its admissibility is not excluded and is available to be raised even at a later stage or even in appeal or revision. In the latter case, the objection should be taken before the evidence is tendered and once the document has been admitted in evidence and marked as an exhibit, the objection that it should not have been admitted in evidence or that the mode adopted for proving the document is irregular cannot be allowed to be raised at any stage subsequent to the marking of the document as an exhibit. The later proposition is a rule of fair play. The crucial test is whether an objection, if taken at the appropriate point of time, would have enabled the party tendering the evidence to cure the defect and resort to such mode of proof as would be regular. The omission to object becomes fatal because by his failure the party entitled to object allows the party tendering the evidence to act on an assumption that the opposite party is not serious about the mode of proof. On the other hand, a prompt objection does not prejudice the party tendering the evidence, for two reasons: firstly, it enables the Court to apply its mind and pronounce its decision on the question of admissibility then and there; and secondly, in the event of finding of the Court on the mode of proof sought to be adopted going against the party tendering the evidence, the opportunity of seeking indulgence of the Court for permitting a regular mode or method of proof and thereby removing the objection raised by the opposite party, is available to the party leading the evidence. Such practice and procedure is fair to both the parties. Out of the two types of objections, referred to*

hereinabove, in the later case, failure to raise a prompt and timely objection amounts to waiver of the necessity for insisting on formal proof of a document, the document itself which is sought to be proved being admissible in evidence. In the first case, acquiescence would be no bar to raising the objection in superior Court.

It is nobody's case that CDRs which are a form of electronic record are not inherently admissible in evidence. The objection is that they were marked before the Trial Court without a certificate as required by Section 65B (4). It is clear from the judgments referred to supra that an objection relating to the mode or method of proof has to be raised at the time of marking of the document as an exhibit and not later. The crucial test, as affirmed by this Court, is whether the defect could have been cured at the stage of marking the document. Applying this test to the present case, if an objection was taken to the CDRs being marked without a certificate, the Court could have given the prosecution an opportunity to rectify the deficiency. It is also clear from the above judgments that objections regarding admissibility of documents which are per se inadmissible can be taken even at the appellate stage. Admissibility of a document which is inherently inadmissible is an issue which can be taken up at the appellate stage because it is a fundamental issue. The mode or method of proof is procedural and objections, if not taken at the trial, cannot be permitted at the appellate stage. If the objections to the mode of proof are permitted to be taken at the appellate stage by a party, the other side does not have an opportunity of rectifying the deficiencies. The learned Senior Counsel for the State referred to statements under Section 161 of the Cr. P.C. 1973 as an example of documents falling under the said category of inherently inadmissible evidence. CDRs do not fall in the said category of documents. We are satisfied that an objection that CDRs are unreliable due to violation of the procedure prescribed in Section 65 B (4) cannot be permitted to be raised at this stage as the objection relates to the mode or method of proof."

Therefore, an objection as to the admissibility of CD must be taken at the time of marking it cannot be raised at the appellate stage.

So far as authentication of CD is concerned, it needs to be noted that comparison of hash values of original data and the data copied on CD is an important means of authentication. The importance of comparison of hash value of a source data and CD was underlined by Punjab and Haryana High Court in the case of **Ram Kishan Fauji son of Shri Dharam Pal Vs State of Haryana** (SCC Online P&H 5058) that if the CD cannot stand the test of authenticity by its comparison with its hash value with the source, then the transcript of what has been obtained through its audio footage or what it purports to capture cannot be taken as of value.

In **Shamsher singh Verma v/s State of Haryana** Criminal Appeal No. 1525 OF 2015 dated 24 November, 2015: 2015 Law Suit (SC) 1145, it has been held that if the accused wishes to rely on some part of CD, which the prosecution does not admit, then the accused can insist on playing the contents of the said CD/DVD in the court and can also insist for sending it to the forensic laboratory for further analysis.

However, preserving the integrity of CD is the main issue faced by the Courts. A valuable piece of evidence may be vanished if it is not properly preserved. CD must be stored or packaged in Faraday Bags or Static bags to preserve the integrity of the information contained therein. Faraday bags are a type of Faraday cage made of flexible metallic fabric. They are used to block remote wiping, alternation of wireless devices recovered in criminal investigations and to protect against data theft.

8.3 TAPPING OF PHONE CALLS:

A voice print is a visual recording of voice. It mainly depends on the position of "formants". These are concentrates of sound energy at a given frequency. It is stated that their position in the "frequency domain" is unique to each speaker. Voice prints resemble finger prints, in that each person has a distinctive voice with characteristic features dictated by vocal cavities and articulates. (87th Report of the Law Commission dated 29th August, 1980).

Nowadays, courts are spending much time as to the admissibility, proof, evidentiary value of call records and conversations in mobile phone or telephone. The court has to make a striking balance between privacy of an individual and larger public interest in detecting the crime. Because, in **People's Union of Civil Liberties ... vs Union Of India (Uoi) And Anr.** AIR 1997 SC 568, at Para 19, it has been held that the right to privacy-by itself-has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case.

But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". Conversations on the telephone are often of an intimate and confidential character. Telephone-conversation is a part of modern man's life. It is considered so important that more and more people are carrying mobile telephone instruments in their pockets. Telephone conversation is an important facet of a man's private life. Right to privacy would certainly include telephone-conversation in the privacy of one's home or office. Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law. Hence it is clear that telephone tapping is permitted only under procedure established by law.

While so, the next question arises as to what are the procedure involved in Interception of phone calls and how it can be recorded. In **Peoples union for civil liberties V/S Union of India**, (cited supra), at Para 28, 29, 30 it has been laid as follows;

> *"Section 5(2) of the Act permits the interception of messages in accordance with the provisions of the said Section. "Occurrence of any public emergency" or "in the interest of public safety" are the sine qua non for the application of the provisions of Section 5(2) of the Act. Unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers under the said Section. Public emergency would mean the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action. The expression "public safety" means the state or condition of freedom from danger or risk for the people at large. When either of these two conditions are not in existence, the Central Government or a State Government or the authorised officer cannot resort to telephone tapping even though there is satisfaction that it is necessary or expedient so to do in the interests of sovereignty and integrity of India etc. In other words, even if the Central Government is satisfied that it is necessary or expedient so to do in the interest of the sovereignty and integrity of India or the security of the State or friendly relations with sovereign States or public order or for preventing incitement to the commission of an offence, it cannot intercept the messages or resort to telephone tapping unless a public emergency has occurred or the interest of public safety or the existence of the interest of public safety requires.*

Neither the occurrence of public emergency nor the interest of public safety are secretive conditions or situations. Either of the situations would be apparent to a reasonable person. The first step under Section 5(2) of the Act, therefore, is the occurrence of any public emergency of the existence of a public-safety interest. Thereafter the competent authority under Section 5(2) of the Act is empowered to pass an order of interception after recording its satisfaction that it is necessary or expedient so to do in the interest of (i) sovereignty and integrity of India, (ii) the security of the State, (iii) friendly relations with foreign States, (iv) public order or (v) for preventing incitement to the commission of an offence. When any of the five situations mentioned above to the satisfaction of the competent authority require then the said authority may pass the order for interception of messages by recording reasons in writing for doing so. The above analysis of Section 5(2) of the Act shows that so far the power to intercept messages/conversations is concerned the Section clearly lays-down the situations/conditions under which it can be exercised. But the substantive law as laid down in Section 5(2) of the Act must have procedural backing so that the exercise of power is fair and reasonable. It is therefore, ordered and directed as under:

1. An order for telephone-tapping in terms of Section 5(2) of the Act shall not be issued except by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. In an urgent case the power may be delegated to an officer of the Home Department of the Government of India and the State Governments not below the rank of Joint Secretary. Copy of the order shall be sent to the Review Committee concerned within one week of the passing of the order.

2. The order shall require the person to whom it is addressed to intercept in the course of their transmission by means a public telecommunication system, such communications as are described in the order. The order may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the order.

3. The matters to be taken into account in considering whether an order is necessary under Section 5(2) of the Act shall include whether the information which is considered necessary to acquire could reasonably be acquired by other means.

4. The interception required under Section 5(2) of the Act shall be the interception of such communications as are sent to or from one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications to or from, from one particular person specified or described in the order or one particular set of premises specified or described in the order.

5. the order under Section 5(2) of the Act shall, unless renewed, cease to have effect at the end of the period of two months from the date of issue. The authority which issued the order may, at. any time before the end of two month period renew the order if it considers that it is necessary to continue the order in terms of Section 5(2) of the Act. The total period for the operation of the order shall not exceed six months.

6. The authority which issued the order shall maintain the following records:
(a) The intercepted communications,

(b) The extent to which the material is disclosed,

(c) The number of persons and their identity to whom any of the material is disclosed.

(d) The extent to which the material is copied and

(e) The number of copies made of any of the material.

7. The use of the intercepted material shall be limited to the minimum that is necessary in terms of Section 5(2) of the Act.

8. Each copy made of any of the intercepted material shall be destroyed as soon as its retention is no longer necessary in terms of Section 5(2) of the Act.

9. There shall be a Review Committee consisting of Cabinet Secretary, the Law Secretary and the Secretary, Telecommunication at the level of the Central Government. The Review Committee at the State level shall consist of Chief Secretary, Law Secretary and another member, other than the Home Secretary, appointed by the State Government.

(a) The Committee shall on its own, within two months of the passing of the order by the authority concerned, investigate whether there is or has been a relevant order under Section 5(2) of the Act. Where there is or has been an order whether there has been any contravention of the provisions of Section 5(2) of the Act.

(b) If on an investigation the Committee concludes that there has been a contravention of the provisions of Section 5(2) of the Act, it shall set aside the order under scrutiny of the Committee. It shall further direct the destruction of the copies of the intercepted material.

(c) If on investigation, the Committee comes to the conclusion that there has been no contravention of the provisions of Section 5(2) of the Act, it shall record the finding to that effect.

The above are the position with regard to the tapping of telephones.

8.4 <u>Proof of tape recorded conversation:</u>

However, often the tape recorded conversations are produced to prove any matter or fact before the court. So far as the proof of the same is concerned, in **R.M. Malkani vs State Of Maharashtra** (1973 AIR 157, 1973 SCR (2) 417), at page 23, it has been held that tape recorded conversation is admissible provided first the conversation is relevant to the matters in issue; secondly, there is identification of the voice and. thirdly, the accuracy of the tape recorded conversation is proved by eliminating the possibility of erasing the tape record. A contemporaneous tape record of a relevant conversation is a relevant fact and is admissible under section 8 of the Evidence Act. It is res gestae. It is also comparable to a photograph of a relevant incident. The tape recorded conversation is therefore a relevant fact and is admissible under section 7 of the Evidence Act.

In **Ram Singh Vs. Col Ram Singh** 1986 AIR(SC)3, the Hon'ble Supreme Court has laid down the following conditions for admissibility of Telephonic conversations as evidence;

(a) The voice of the person alleged to be speaking must be duly identified by the maker of the record or by others who knew it.

(b) Accuracy of what was actually recorded had to be proved by the maker of the record and satisfactory evidence, direct or circumstances had to be there so as to rule out possibilities of tampering with the record.

(c) The subject matter recorded had to be shown to be relevant according to rules of relevancy found in the evidence Act." (Ephes ours) Thus, so far as this Court is concerned the conditions for admissibility of a tape recorded statement may be stated as follows:

1. The voice of the speaker must be duly identified by the maker of the record or by others who recognise his voice. In other words, it manifestly follows as a logical corollary that the first condition for the admissibility of such a statement is to identify the voice of the speaker. Where the voice has been denied by the maker it will require very strict proof to determine whether or not it was really the voice of the speaker.

2. The accuracy of the tape recorded statement has to be proved by the maker of the record by satisfactory evidence - direct or circumstantial.

3. Every possibility of tampering with or erasure of a part of a tape recorded statement must be ruled out otherwise it may render the said statement out of context and, therefore, inadmissible.

4. The statement must be relevant according to the rules of Evidence Act.

5. The recorded cassette must be carefully sealed and kept in safe or official custody.

6. The voice of the speaker should be clearly audible and not lost or distorted by other sounds or disturbances.

While deciding the evidentiary value of tape recorded conversation, in **Yusufalli Esmail Nagree v. State of Maharashtra** [1967] 3 S.C.R. 720 it has been reiterated that if a statement is relevant, an accurate tape record of the statement is also relevant and admissible. The time and place and accuracy of the recording must be proved by a competent witness and the voices must be properly identified. One of the features of magnetic tape recording is the ability to erase and re-use the recording medium. Because of this facility of erasure and re-use, the evidence must be received with caution. The court must be satisfied beyond reasonable doubt that the record has not been tampered with. The tape was not sealed and was kept in the custody of Mahajan. The absence of sealing naturally gives rise to the argument that the recording medium might have been tempered with before it was replayed. In **N. Sri Rama Reddy, etc. v. V.V.Giri** [1971] 1 S.C.R at page 399, it is further observed as follows:

"Having due regard to the decisions referred to above, it is clear that a previous statement, made by a person and recorded on tape, can be used not only to corroborate the evidence given by the witness in Court but also to contradict the evidence given before the Court, as well as to test the veracity of the witness and also to impeach his impartiality.

8.5 <u>Proof of Call Data Record:</u>

A Call Data Record is a detailed record of SMS and calls that are sent and received by a subscriber of a service provider. The main benefits we can reap from Call Detail Record are identifying the suspect's day location , night location, handset details, maximum contact number, date, time , tower location at the time of occurrence of the offence, coordinates of his movement etc., It can also be disseminate the details regarding call duration, connection status, source number, destination number, accurate identification of telephone exchange, unique sequence number identifying the record, the route by which the call entered the exchange, the route by which the call left the exchange.

Regarding the proof and admissibility of mobile phone call records, it needs to be proved by producing certificate under Section 65-B of Evidence Act. In **Bala Saheb Gurling Todkari Vs. State of Maharastra** (2015 SCC Online Bom 3360) it has been held in Para 36 that absence of certificate would render the CDR inadmissible in law. Being inadmissible it cannot be considered. However, in **State of NCT of Delhi Vs**

Navjot Sadhu AIR 2005 SC 3820, the accused side raised a submission that no reliance can be placed on the mobile phone call records , because the prosecution has failed to produce the relevant certificate under section 65-B of the Evidence Act, The Supreme Court has concluded that a cross examination of the competent witness acquainted with the functioning of the computer during the relevant point of time and the manner in which the printouts of the call records were taken was sufficient to prove the call records.

In **Sonu Vs State of Haryana** (2017)8 SCC 517 it has been held in Para 32 by the Supreme Court that an objection that CDRs are unreliable due to violation of procedure prescribed in section 65-B (4) cannot be permitted to be raised at the appellate stage as the objection relates to the mode or method of proof. In **Union of India Vs. Ravindra Desai,** the Hon'ble Supreme Court has also held in Para 22 that non production of the certificate under Section 65-B on an earlier occasion was a curable defect. Similarly, in the case of State of Karnataka Vs M.R. Hiremath reported in 2019 (7) SCC 515 it has been held that the non-production of a certificate under Section 65-B of the Indian Evidence Act at a prior stage is a curable defect.

8.6 <u>Proof of CCTV Footage:</u>

Walter Bruch is considered to be the inventor of the CCTV Camera. There are 3 types of CCTV. Firstly, Standalone which is self contained camera having inbuilt memory device. Secondly, Wired, which has a wire to connect a camera and to a recorder. Thirdly, IP which uses Wi-Fi to communicate with recorder or uses the cloud storage facility whereby the footage can be viewed from anywhere with an internet connection. CCTV camera has a CCD Sensor (Charge Coupled Device) which converts lights into an electronic signal and which is then converted into a video signal recorded or displayed in screen. CCTV works by camera or cameras taking constant sequence of images that are then transmitted by cable or wirelessly to the recording device and then on to the display monitor, which enables the individual to see the sequence of images as video footage. In criminal trial, the evidence of CCTV footage assumes very much importance. It helps to prove the presence of the accused in the scene of crime. It is equal to ocular evidence. Though CCTV footage is the best evidence, the mode and manner of proof is always a challenge.

As held in **TOMASO BRUNO & ANR V/S STATE OF U P** 2015 Law suits (SC) 54, CCTV footage is a strong piece of evidence. In **K .RAMAJAYAM @ APPU V/S INSPECTOR OF POLICE** 2016 Law suits(Mad)136 at Para 31, the Hon'ble Madras High Court has observed that it is axiomatic that CCTV footage does not suffer ills and human fragilities, and they are indubitably superior to human testimony of facts.

One has to understand the science of CCTV Recordings in the light of the Information and Technology Act, 2000, for the purpose of its optimum usage as evidence in the Court of Law. Gone are the days when Hindustan Photo Films produced film rolls for loading in the camera and on the click of the button the image gets imprinted on the film. The imprint is called the negative, which is the primary evidence, and the positive developed there from is considered as the secondary evidence. That technique has now become defunct. Today, the physical images captured by the camera is converted by a computer software into information, capable of being stored as data in electronic form and the stored data is electronic record. It has been further observed in Para 32 that the images captured by the cameras were transferred to a Digital Video Recorder (DVR), which is a rectangular box, through wires. DVR has a computer programmed circuit to receive the images from the four cameras and convert them into electronic form in binary and store them in the hard disk. The software is so programmed that it can not only receive and store, but also play back the images on a screen, be it a monitor, Television screen, or Cinema Screen. The information so stored are not tangible information for the Court to inspect and see with its naked eyes. The DVR is an electronic record within the meaning of Section 2(t) of the Information Technology Act, 2000, as it stores data in electronic form and is also capable of output.

Regarding the procedure to be followed to ascertain the integrity of CCTV footage, the Bombay High Court has given certain directions in the case of **Vaijinath Vs State of Maharastra** 2019 SCC Online Bom 1357**.** A CCTV footage must also be proved by producing a certification under section 65-B of the Evidence Act.

8.7 <u>Body worn Cameras:</u>

States of America and the United Kingdom. Body-worn cameras act as deterrent against anti-social behaviour and is also a tool to collect the evidence. It was submitted that new technological device for collection of evidence are order of the day. He also referred to the Field Officers' Handbook by the Narcotics Control Bureau, Ministry of Home Affairs, Government of India. Reference was also made to Section 54-A of the Cr.P.C. providing for videography of the identification process and proviso to Section 164(1) Cr.P.C. providing for audio video recording of confession or statement under the said provision. (At page 2, **SHAFHI MOHAMMAD V/S STATE OF HIMACHAL PRADESH** 2018 AIR(SC) 714)

8.8 <u>Proof of Email:</u>

Email is the most often produced in a court of law. Generally, email is not sent directly from the sender to the receiver but it uses a *'store and forward method'*. Because if the user is not online, then the email may get lost and hence internet service provider

store the mail, till the recipient is on online and retrieves it. A computer dedicated to the transfer of email is called a mail server. Microsoft Exchange, Gmail, yahoo mail are some of the known examples. Every email service provider has its own dedicated email server which transfers email from the sender, firstly the destination address is verified. If the destination address also belongs to the same email service provider then the mail server directly sends it to the recipient's mail box. However, if the recipient's email service provider is different than the sender's email server, it will first find the recipient's email server and would send it to that email server. The receiver's email server then pushes the email to the recipient.

Such being the working of email system, In **Smt bharathi V Rao Vs. Sri Pramod G. Rao,** MANU/KA/3242/2013, it has been held that email comes under the definition of electronic record under section 2(t) of IT Act and is admissible in evidence. In **Abdul Rahman Kunji vs. The State of West Bengal** 2016 CrLJ 1159 it has been further held that an email downloaded and printed from the email account of the person can be proved by virtue of section 65-B r/w 88A of Evidence Act. The testimony of the witness to carry out such a procedure to download and print the same is sufficient to prove the electronic communication. It is further held in **Babu Ram Aggarwal & Anr v/s Krishan Kumar Bhatnagar & ors.** 2013 Law Suit (Delhi 422 at Para 19) that as per Section 65B of the The Indian Evidence Act, 1872, for such emails to be proved, it has to be proved/established that the computer during the relevant period was in the lawful control of the person proving the email; that information was regularly fed into the computer in the ordinary course of the activities; that the computer was operating properly and the contents printed on paper are derived from the information fed into the computer in the ordinary course of activities and a certificate identifying the electronic record has to be proved.

Section 88-A of the Evidence Act provides for a presumption about electronic messages. It is necessary to understand that the presumption merely states that the message received by the addressee is the same, which was fed into the originator's computer for transmission. As held by Madras High Court, in **S. Karunakaran Vs Srileka** 2019 SCC Online Mad 1402, the court shall not make any presumption as to the person by whom such message was sent. Therefore, it is clear that mere filing of email does not give raise a presumption that it is sent by the originator. Similarly, the High Court of Punjab and Haryana, in **Nidhi Kakka vs Munish Kakkar** 2011 SCC On line P&H 2599 has held in Para 6 that the correctness and exact reproduction in print out version of the mail could still be issues in the cross examination and the court will have to consider whether the text could have been altered or morphed.

8.9 <u>Proof of Hard Disc:</u>

Hard disc is a magnetic storage medium for a computer. It is a non-volatile storage device. Non volatile refers to storage devices that maintain stored data when turned off. The word 'data' includes not only the active memory of the computer, but even the subcutaneous memory like Hard Disc. Hard Disc is not merely a physical object, but a document within the meaning of Section 3 of the Evidence Act. Explaining the position of law, about hard disc, mirror image and subcutaneous memory, the Delhi High Court in the case of **Dharambir; Jagdish Chandra; Ajay Khanna; Anand Mohan Sharan Vs Central Bureau of Investigation** (48 (2008) DLT 289), at Para 8.9 and 8.10 it has been observed as follows:

> *"Given the wide definition of the words 'document' and 'evidence' in the amended Section 3 the EA, read with Sections 2(o) and (t) IT Act, there can be no doubt that an electronic record is a document. The further conclusion is that the hard discs are themselves documents. A hard disc is an electronic device used for storing information, once a blank hard disc is written upon it is subject to a change and to that extent it becomes an electronic record. Even if the hard disc is restored to its original position of a blank hard disc by erasing what was recorded on it, it would still retain information which indicates that some text or file in any form was recorded on it at one time and subsequently removed. By use of software programmes it is possible to find out the precise time when such changes occurred in the hard disc. To that extent even a blank hard disc which has once been used in any manner, for any purpose will contain some information and will therefore be an electronic record. This is of course peculiar to electronic devices like hard discs. Therefore, when Section 65B EA 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. There are 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 programme. 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.

8.10 Admissibility of Satellite Sketch:

It is also be noted that satellite sketches to find out the location of the accused and spot of the incident can be admitted. In **V.S. Lad and Sons vs. State of Karnataka** 2009 Crl. LJ 3760, the state of Karnataka relied on super imposition of leased out area on satellite map on the basis of satellite emergency obtained by Karnataka State Remote Sensing Application Centre to initiate action against the accused to show encroachment of forest land. The court has accepted it as a evidence and refused quash the FIR.

8.11 ATM:

In a case reported in 2005 AIR Knt. HCR 9, it was held that Automated Teller Machines was held to be not a computer by itself nor it is a computer terminal.

8.12 Proof of Whatsapp messages:

Whatsapp message is legal evidence under law. The IT Act recognizes the electronic evidence as proof in court. The messages sent through whatsapp messaging app are valid legal evidence under law and the blue tick over the messaging is a valid proof that the recipient read it. Mobile whatsapp and facebook chat are taken as evidence proof in the court of law. In **Suo moto writ petition (C) No. 2/2020, dated 10.7.2020** the Hon'ble Supreme Court has allowed to serve summons, notices through instant messaging services such as whatsapp, Telegram, signal.

Since mobile phone is computer the print out taken is a computer output, it requires certificate under section 65-B of the Evidence Act. However, in **Aryan Shah Rukh Khan Vs Union of India** ADPS BAIL APPLICATION NO 2571 of 2021 dated 20.10.2021, it has been held that such a certificate is not necessary in the stage of investigation.

8.13 Emoji:

Emojis are used to convey something funny or laughable. Considering whether sending of emoji would attract criminal liability, the Hon'ble High Court, Madras, in Linga Bhaskar and other vs. The State (2018 - 4-LW. 175) has held as follows:

"It is admitted that the emoji are posted to convey numerous feelings. It is stated that emoji is used when something is funny or laughable. In the present context, the petitioners and respondents are members of whatsapp group . . . When it is accepted that an emoji is sent to express ones feeling about something, it cannot be treated as an overt act on others. It is a comment to ridicule or to show one's disproval in a given context.

The allegation is about the posting of an emoji in a whatsapp group shared by the group of persons. The posting of emoji is to express one's feeling. it is an act that may offend the second respondent but that is not an act attracting section 4 of TN PWH Act, 1998.

8.14 <u>Memory Cards :</u>

Normally memory cards are the integral parts of every digital device. In P. **Gopalakrishnan Vs. State of Kerala** (2020) 9 SCC 161, it is held that contents of memory card would be a matter and it would be treated as a substance. Hence it can be treated as document.

8.15 <u>Proof of Copy of computer generated statement of account :</u>

Often it happens that the parties are producing computer generated account statements in order prove their money claims. The question arises as to whether certificate under section 65-B of Evidence Act is necessary to prove the transaction. When a similar question arose in **M/s. IOCEE Exports Ltd., Chennai Vs. Mr. Moosa Ahmed (Deceased)**, the Hon'ble Madras High Court has held in Para 11 that the statement of accounts Ex.P.32 is not accompanied by a certificate certified by a person who is in charge of the operation of the relevant activities as per Section 65B of the Indian Evidence Act. Therefore, merely on the basis of some transactions and on the basis of Ex.P.32, the suit claim cannot be countenanced. In the absence of any proof with regard to the statement of accounts and any corresponding entries in the ledger and day book, the plaintiff cannot recover the entire suit amount from the defendants, merely on the basis of inadmissible document Ex.P.32.

9. Others :

9.1 Presumption of electronic records:

Section 81-A of Indian Evidence Act deals about presumption as to genuineness of electronic records. It says that genuineness of the electronic record shall be presumed in respect of official gazette or purporting to be electronic records directed by any law to kept by any person if such record is kept substantially in the form required by law and is produced from proper custody.

9.2 YouTube and Liability of Intermediary:

It is further held that the basic function of the YouTube website permits users to "upload" and view video clips free of charge. Before uploading a video to YouTube, a user must register and create an account with the website. The registration process requires the user to accept YouTube's Terms of Use agreement, which provides, inter alia, that the user "will not submit material that is copyrighted ... unless [he is] the owner of such rights or ha[s] permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein." When the registration process is complete, the user can sign in to his account, select a video to upload from the user's personal computer, mobile phone, or other device and instruct the YouTube system to upload the video by clicking on a virtual upload "button." The same is the procedure in Google Website. Thus, if the actual knowledge to the intermediary is proved, then intermediary cannot escape its liability. (at Para 87, **Google India Private Limited V/S Visaka Industries Limited And 2 Others**, 2016 Law Suit (Hyd) 548)

9.3 Altering computer programme or source is an infringement of copy right:

Therefore, reading Section 2(o), (ffc) and Sections 13 and 14 together, it becomes clear that a computer programme is by very definition original literary work and, therefore, the law protects such copyright. Under Section 63 of the Copyright Act, any infringement of the copyright in a computer programme/source code is punishable. Therefore, prima facie, if a person alters computer programme of another person or another computer company, the same would be infringement of the copyright.

9.4 Rights of the accused and digital records:

Once we deal about proof of electronic records, it is equally important that opportunity must be given to disprove it. Needless to say, right to fair trial is a fundamental right and valuable right to an accused. In **Manu sharma Vs State NCT of Delhi** (2010)6 SCC 1**,** it has been observed in Para 220 that the right of the accused with regard to disclosure of document is a limited right but it is codified and is the foundation

of a fair investigation and trial. On such matters, the accused cannot claim an indefeasible legal right to claim every document of the police file or even the portion which are permitted to be excluded from the document annexed to the report under Section 173(2) as per order of the court. It has been further held that right of the accused to claim documents stemmed from the sections 207, 243 and 91 CrpC. Therefore, when the prosecution proposes to rely upon the tap recorded conversation, accused is entitled to get copies of the same. In a case, the court has to proceed on the basis that the CBI proposes to rely upon the 19 CDs containing 768 calls in addition to the document listed by it in the annexure to the charge sheet. Therefore, each of the accused is entitled to be provided with copies of the 19 CDs containing the 768 calls. (**Dharambir; Jagdish Chandra; Ajay Khanna; Anand Mohan Sharan V/S Central Bureau Of Investigation** 148 (2008) DLT 289). Regarding the right of the accused to get copies and fair trial, the Supreme Court in **P. Gopalakrishnan Vs. State of Kerala 2019** SCC online SC 1532 has held that it is cardinal that a person tried for serious offence should be furnished with all the material and evidence in advance, on which the prosecution proposed to rely against him during the trial. Any other view would not only impinge upon the salutary mandate contained in the 1973 code, but also the right of the accused of a fair trial enshrined in Article 21 of the Constitution of India.

****