Summary of second workshop on the Criminal topic

"Admissibility of Electronic Record, Video Recording, Computer Outputs"

INTRODUCTION

The present generation is living in the electronic world. Due to invention of technology the electronic communication and electronic writings have emerged as foundation of today's world. New generation is using one or other form of electronic device for communication in daily life. So also most of the individuals, private sector, government and non governmental organization are carrying out their function paperless. Not surprisingly, various forms of electronic evidence (i.e. e-evidence) is increasingly being used in both civil and criminal litigation. As Court continue to grapple with this new electronic frontier, it is important to stress that electronic evidence is subject to the same rules of evidence as paper document. However, the unique nature of e-evidence, as well as the ease with which it can be manipulated or falsified, creates hurdles to admissibility not faced with other evidence. Court of law relies on oral as well as documentary evidence. For instance, when information recorded or stored in a memory of a computer is printed out on paper, it is not easy to say that the version in the memory is a documentary evidence. Nor is it easy to assert that the printout is an original or a copy. Also, even if such things (audio, tape recording, a video tape recording, electronic mail on computer screen) when presented as evidence, and such things as electronically transmitted mandates in commercial transaction can be regarded as document.

The proliferation of computer, the social influence of information technology and the ability to store information in digital form have all required Indian Law to be amended to include provisions on the appreciation of digital evidence. In 2000 Parliament enacted the Information Technology Act, 2000, which amended the existing Indian Statute such as Indian Evidence Act, Indian Penal Code and the Bankers Book Evidence Act etc to allow for the admissibility of digital evidence which recognizes transactions that are carried out through electronic data interchange and other means of electronic communication.

We are living in the information age. The frontiers between different paper formats (text, map, photograph) and traditional analog electronic formats (sound recording, film), are becoming increasingly blurred because digital technology can combine all the above formats in a single record. Those are two of the reasons why organizations are moving towards automating their information systems and creating more electronic documents. Other reasons are the speedier access to the information, the facility to share it worldwide, and the decreasing cost of storing the information electronically.

What is an Electronic Record?

An electronic record is information recorded by a computer that is produced or received in the initiation, conduct or completion of an agency or individual activity. For example electronic record includes: e-mail messages, word-processed documents, electronic spreadsheets, digital images and databases.

Electronic media is used for storing information in different formats (text, image, sound), just like "paper" is a medium for storing information in different formats (text, map, photograph). Electronic Record is the recorded information on an electronic medium, regardless of physical form or characteristics, which requires an electronic system for retrieving and reading the information. There is only one criteria which makes a record, an electronic one. An electronic record contains machine-readable information, as opposed to a paper file which contains human-readable information. Machine-readable records cannot be read without the proper hardware and software. A coding process of the information (converting the data into an electronic signal) makes the record machine-readable.

Once an electronic document has been printed, the print-out is not an electronic record, since the information is now in human-readable form.

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 microfilm or computer generated micro-fiche.

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

Section 4 related with the legal recognition of electronic records.

If any information or matter is rendered or made available in an electronic form, and accessible so as to be usable for a subsequent reference, shall be deemed to have satisfied the requirement of the law which provides that information or any other matter shall be in writing or in the typewritten form.

Section 5 related with the legal recognition of digital signatures.

Section 6 related with the use of electronic records and digital signatures in Government and its agencies.

Section 7 related with the retention of electronic records.

If any law provides that documents, records or information are required to be retained for any specific period, then, that requirement shall be deemed to have been satisfied if the same is retained in electronic form.

The Information Technology Act, 2000 was amended to allow for admissibility of digital evidence. The electronic record is any probative information stored or transmitted in digital form that a party to a Court case may use at trial. Before accepting digital evidence it is vital that the determination of its relevance veracity and authenticity be ascertained by the Court and to establish if the fact is hearsay or copy is preferred to the original. Digital evidence is “information of probative value that is stored or transmitted in binary form.” 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. The E-evidence can be found in e-mails, digital 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, digital video or audio files. Digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available.

Computer Output

Computer output means data generated by a computer. This includes data produced at a software level, such as the result of a calculation, or at a physical level, such as a printed document. A basic example of software output is a calculator program that produces the result of a mathematical operation. A more complex example is the results produced by a search engine, which compares keywords to millions of pages in its Web page index.

Devices that produce physical output from the computer are creatively called output devices. The most commonly used output device is the computer's Monitor, which displays data on a screen. Devices such as the printer and computer speakers are some other common output devices.

Any information that has been processed by and sent out from a computer or similar device is considered output. A simple

example of output is anything you view on your computer monitor. That data is then printed onto a piece of paper; both are forms of output.

Examples of output on a computer

- **Digitized Speech:**- Digitized speech is anything spoken that has been converted from an analog to a binary signal to be used for playback at a later time
- **Hard copy** is anything that has been printed on paper. Hard copies allow data to be read without the need of a computer and are often required when someone needs to sign a document.
- **Soft copy**:- A soft copy is a copy of text stored on the computer and only accessible through the computer. The most common method of displaying a soft copy is through a computer monitor or other display.

Admissibility Of Electronic Evidence

Electronic Evidence proof and Admissibility :-

It is world of e-banking, e-business, e-court. This is a paperless job without loss of ink and time. It saves our valuable time and makes transaction of court, business and Banking business easier. The advancement of technology has advantages and disadvantages too. Some of the experts are using their skill for illegal gains. Such as hacking data, fetching, phishing and collecting personal information. Such information is used for development of

computer programmes used for withdrawing money from others bank account. These are known as cyber offences in general. We have been studying the Evidence Act, which is enacted keeping in view all the evidence, which is full of papers based record and oral testimony. Internet goes from PC to PC, PC to mobile and through server of the system. So what can be best evidence is a question. The answer is specified in a new amendment to evidence Act, in section 65(A) and 65(B) of Evidence Act.

Section 65-B is very important section. It provides admissibility of electronics records.

The definition of evidence has been amended to include electronic record. The definition of documentary evidence has been amended to include all documents including electronic record produced for inspection by the Court. New section 65-A and 65-B are introduced to the Evidence Act under the second schedule to the Information Technology Act. Section 65-A provides that the contents of electronic record may be proved in accordance with provisions of section 65-B. Section 65-B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic, is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the condition set out in section 65-B are satisfied. The conditions specified in section 65-B(2) are:

1] Firstly the computer output containing the information should have been produced by the computer during the period over which the computer was used regularly to store or

process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of the computer.

2] The second requirement is that it must be shown that during the said period the information of the kind contained in electronic record or of the kind from which information contained is derived was 'regularly fed into the computer in the ordinary course of said activity'.

3] The third requirement is that during material part of the said period, the computer was operating properly and that even if it was not operating properly for sometime that break did not affect either the record or the accuracy of its contents.

4] The fourth requirement is that the information contained in the record should be a reproduction or derived from the information fed into the computer in the ordinary course of the said activity.

Under section 65-B(4) the certificate which identifies the electronic record containing the statement and describes the manner in which it was produced giving the particulars of the device involved in the production of that record and deals with the conditions mentioned in Section 65-B(2) and is signed by a person occupying a responsible official position in relation to the operation of relevant device, “shall be the evidence of any matter stated in the certificate.”

Section 65-B(1) states that if any information contained in an electronic record produced from a computer (known as computer output) has been copied on to a optical or magnetic media,

then such electronic record that has been copied 'shall be deemed to be also a document' subject to conditions set out in section 65-B(2) being satisfied.

In the proceeding where computer out put is desired to be produced in evidence, a certificate by a person responsible for the operation of the computer system or the management of related activities shall be the evidence of matter stated in the certificate, stated to be true to the best of knowledge and belief of the person certifying his certificate. The certificate may give following details;

a) Identification of the electronic record and description of manner of production.

b) Particulars of device used in production and

c) details indicating compliance of condition in para 2 above.

For the purpose of this section;

a) the information shall be taken as supplied to the computers, if supplied in appropriate form, whether directly or by other appropriate equipment.

b) even if the information is supplied to the computer by a computer otherwise in the course of those activities, information is duly supplied to that computer in the course of activities carried out by official with a view to process and store, the information shall be deemed to have been duly supplied.

c) out put shall be deemed to be production by the computer, even if the same is directly or by other appropriate equipment like printer. So, if we refer above mentioned definitions in the light of the provisions incorporated u/s 65-A & 65-B of evidence Act;

Electronic Evidence is one another type of documentary evidence which is, if duly proved in the manner provided in sec 65-B, can be considered as strong evidence.

Let us take an example of publisher of child pornography. He may have e-mail I.D., of the domain eg. Yahoo.com. which locates abroad. Then, if it happens that pornography pictures seen in the school of children in France, then we have to revolve around the world to hunt the culprit. The school authority may lodge complaint with French police. The French police will contact the domain authority which has flouted the pornography picture on other site. Then they will take the server in India through which the pornography picture were published. Therefore the server in India, will take the I.P. address of the originator of India. (I.P.address means Internet protocol address, it is different for every different computer). Subsequently, the Indian cyber police will come in picture. They will have to collect the data about the person on whose I.P. address, the pornography pictures are published. The said person may be living in any part of India. Internet service provider will give the physical address of Internet protocol. Police will search his physical address and trap him. The first thing, cyber police will do is that they will seize the hard disk and take prints out from his computer in presence of panchas. In this case, what will be the evidence, is a question before court. An example is that the police officer has taken some hard copies from the computer of accused itself. The condition embodied in section 65-B is that the outputs shows have been produced by the computer during the period which

the computer was in regular use. Whether panch can be believed for obtaining hard copies and hard disk copy from the computer?

The panchas can tell perfectly which copy was obtained from which computer. Certainly it can only corroborate that each and only if prosecution can establish through reliable evidence that this is personal computer of accused without access to others. This could be corroborated with the evidence of scientific officer of Forensic Department who will tell whether it was containing picture. It is to be noted that it is not necessary that every witness would tell that computer was in regular service and was operated by the accused. The service provider will give the evidence with log in and log out details that a particular pornography picture was sent to a particular domain address through the I.P. address of the accused. It is to be noted that every computer has a distinct I.P. address. Similarly, the domain of his like G-mail, yahoo-mail etc. will give the details about the transaction in their server with system generated report. That both the reports can be compliance of section 65-B(2) of Evidence Act.

There are seldom eye witnesses in the cyber offence seeing the offender committing the offence. The evidence come through the proprietor of cyber cafe, cctv camera footing, service provider's record and Internet browsing record to Internet domain and ultimately hard disk which may contain data. This all change of evidence can only establish the guilt of the accused. The cyber cafe will give hard copy from its computer. Service provider will give hard copy with log in and log out details. Domain Administrator will also

give hard copy of its inter transaction to their domain. Everyone of them has to establish that system from which they have given this data is regularly in use. They have exclusive and legal control over the system and its use in ordinary course of their activities. They have to certify that there was no interruption and their system was operating properly. Then only the positive copy of Electronic Record will be read in evidence. Besides this, a seized Hard disk, data containing device will be examined by the expert and will have only corroborative value to the first hand information given by the above witnesses.

When a statement had to be produced in evidence under this section, it should be accompanied by a certificate which should identify the electronic record containing the statement and describe the manner in which it was produced, give the particulars of the device involved in the production of the electronic record showing that the same was produced by a computer and showing compliance with the conditions of sub-section (2) of this section. The statement should be signed by a person occupying a responsible official position in relation to the operation or management of the relevant activities. Such statement shall be evidence of the matter stated in the certificate. It should be sufficient for this purpose that the statement is made to the best of knowledge and belief of the person making it [Sec. 65-B(4)].

The audio C.D. was marked by the Court as an exhibit with the condition that when it was displayed, an opportunity would

be given to the wife for cross examining the husband. **(G. Shyamlal Rajini V. M.S. Tamizhnathan. AIR 2008 NOC 476 (Mad.)**

On the point of recording of evidence through video conference in the case of **Amitabh Bagchi Vs. Ena Bagchi (AIR 2005 Cal. 11,** the Court held that the physical presence of a person in Court may not be required for the purpose of adducing evidence and the same can be done through medium like video conferencing. Section 65-A and 65-B provide provisions for electronic records and admissibility of electronic records and that definition of electronic record includes video conferencing.

In the case of **State of Maharashtra Vs. Dr. Praful B. Desai A.I.R. 2003 SC 2053** the Hon'ble 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 the 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 the case of **Bodala Murali Krishna Vs. Smt. Bodala Prathima 2007(2) Ald 72,** the Court held that...the amendments carried to the Evidence Act by introduction of Section 65-A and 65-B are in relation to the electronic record. Section 67-A and 73-A were introduced as regards proof and verification of digital signatures. As

regards presumption to be drawn about such records, Section 85-A and 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 digital signatures, as admissible pieces of evidence.

In the case **Dharmbir Vs. C.B.I. Delhi high court decided on 11/3/2008** it is held that when Section 65-B talks of an electronic record produced by computer referred to as the computer output, it would also include hard disk in which information was stored or was earlier stored or continuous to be stored. It distinguished as there being two levels of an electronic record. One is the hard disk which once used itself becomes electronic record in relation to the information regarding the changes the hard disk has been subject to and which information is retrievable from the hard disk by using a software program. The other level of electro record is the active accessible information recorded in the hard disk 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 disk which contains no information but was once used for recording information can also be copied by producing a cloned had or a mirror image.

The case of **State (NCT of Delhi) Vs. Navjot Sandhu AIR 2005 SC 3820** deals with the proof and admissibility of mobile telephone call records. While considering the appeal against the accused for attacking Parliament, a submission was made on behalf

of the accused that no reliance could be placed on the mobile telephone call records, because the prosecution had failed to produce the relevant certificate under section 65-B(4) of the Evidence Act. The Supreme Court concluded that a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records.

In the case of **Jagjit Singh Vs. State of Haryana SC decided on 11/12/2006 Writ Petition No.287/06,** the Hon'ble Supreme Court considered the digital 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 digital evidence and the conclusions reached by him.

In the case of **Twentieth Century Fox Film Corporation Vs. NRI Film Production Associates (P) Lt. AIR 2003 Kant 148** certain conditions have been laid down for video recording of evidence:

Before a witness 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.

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.

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 of 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.

The recent judgment of the Hon'ble Supreme Court delivered in **Anvar P.V. Vs. P.K. Basheer and others,** the Hon'ble 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. The legal interpretation by the Court of the following sections 22A, 45A, 59, 65-A and 65-B of the Evidence Act has confirmed that the stored data in CD/DVD/Pen Drive is not admissible without a certificate u/s 65-B(4) of Evidence Act and further clarified that in absence of such a certificate, the oral evidence to prove existence of such electronic evidence and the expert view under section 45-A of the Evidence Act cannot be availed to prove authenticity thereof.

The Hon'ble Supreme Court has held that Section 65-A being a 'not obstante clause' would override the general law on secondary evidence under section 63 and 65 of the Evidence Act. Section 63 and section 65 of the Evidence Act have no application to the secondary evidence of the electronic evidence and same shall be wholly governed by the Section 65A and 65B of the Evidence Act.

The original recording in Digital Voice Recorders/mobile phones need to be preserved as they may get destroyed, in such a case the issuance of certificate under section 65-B(4) of the Evidence

Act cannot be given. Therefore, such CD/DVD is inadmissible and cannot be exhibited as evidence, the oral testimony or expert opinion is also barred and the recording/data in the CD/DVD's do not serve any purpose for the conviction.

New provisions for electronic records

The Information Technology Act amended section 59 of the Evidence Act to exclude electronic records from the probative force of oral evidence in the same manner as it excluded documents. This is the reapplication 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:

Once electronic evidence is properly adduced according to section 65B of the Evidence Act, along with the certificate of sub section (4), the other party may challenge the genuineness of the original electronic record. If the original electronic record is challenged, section 22A of the Evidence Act permits oral evidence as to its genuineness only. Note that section 22A disqualifies oral evidence as to the contents of the electronic record, only the genuineness of the record may be discussed. In this regard, relevant oral evidence as to the genuineness of the record can be offered by the Examiner of Electronic Evidence, an expert witness under section 45A of the Evidence Act who is appointed under section 79A of the IT Act.

When electronically stored information is offered as evidence, the following tests need to be affirmed for it to be admissible:

(i) is the information relevant;

(ii) is it authentic;

(iii) is it hearsay;

(iv) is it original or, if it is a duplicate, is there admissible secondary evidence to support it; and

(v) does its probative value survive the test of unfair prejudice?

Presumptions

A fact which is relevant and admissible need not be construed as a proven fact. The judge must appreciate the fact in order to conclude that it is a proven fact. The exception to this general rule is the existence of certain facts specified in the Evidence Act that can be presumed by the court.

To bridge the widening gap between law and technology, Parliament enacted the Information Technology Act, 2000 ("IT Act") by which the Indian Evidence Act has been amended to introduce various presumptions regarding digital evidence and electronic records. Said amended provisions are as follows;

Sec. 81A related with the presumption as to Gazettes in electronic forms.

Sec. 85A Presumption as to electronic agreements.

The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of

the parties was so concluded by affixing the digital signature of the parties.

Sec. 85B related with the presumption as to electronic record and digital signatures. –

(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that

(a) The secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) Except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Sec.85C related with the presumption as to Digital Signature Certificates.

Sec. 88A. Presumption as to electronic messages.

The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for

transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation : For the purposes of this section, the expressions “addressee” and “originator” shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub section (1) of section 2 of the Information Technology Act, 2000.”

In the case of **Kolkata High Court (Appellete Side) Abdul Rahaman Kunji vs The State Of West Bengal on 14 November, 2014**

It is observed that under Section 88A of the Evidence Act the Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed in the computer for transmission. However, the Court cannot draw any presumption about the person who sent the message. The term 'originator' has been defined in the Information and Technology Act, 2000 under Section 2(za) as a person who sends, generates, stores or transmits any electronic message; or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary. Thus on analysing Section 88A of the Evidence Act and the relevant provisions of the Information and Technology Act, it is apparent that the Court may presume the veracity of the message fed into the computer for transmission by the originator through his mail server to an addressee, that is, the person who is intended by the originator to receive the electronic record and does not include any

intermediary. However, this is a rebuttable presumption. Besides, no presumption can be drawn about the person who has sent such a message.

Sec. 90A. Presumption as to electronic records five years old.

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

Explanation- Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This Explanation applies also to section 81A.

Mobile Phone Data

The active mobile phone has two components i.e. the mobile instrument and the SIM card. Every mobile phone instrument has a unique identification number, namely, Instrument Manufactured Equipment Identity, for short, IMEI number. Such SIM card could be provided by the service providers either with cash card

or post paid card to the subscriber and once this SIM card is activated the number is generated which is commonly known as mobile number. The mobile service is operated through a main server computer called mobile switching center which handles and records each and every movement of an active mobile phone like day and time of the call, duration of the call, calling and the called number, location of the subscriber during active call and the unique IMEI number of the instrument used by the subscriber during an active call. This mobile switching center manages all this through various sub-systems or sub-stations and finally with the help of telephone towers. These towers are actually Base Trans-receiver Stations also known as BTS. Such BTS covers a set of cells each of them identified by a unique cell ID. A mobile continuously selects a cell and exchanges data and signaling traffic with the corresponding BTC. Therefore, through a cell ID the location of the active mobile instrument can be approximated.

Satellite Sketch

Now-a-days Courts may rely upon the satellite sketches to find out the location of the accused and spot of the incidence. In case of **Ms. V.S. Lad and Sons Vs. State of Karnataka reported in 2009 Cri. L.J. 3760**, it is held by Hon'ble Karnataka High Court that criminal action can be initiated against the accused alongwith order of seizure on the basis of report of Lokayukta and Satellite sketch relied on in side report. The encroachment carried out by petitioner on the Forest Area was revealed by super imposition of leased out

area on satellite map on the basis of the satellite emergency obtained from the Karnataka State Remote Sensing Application Center.

E-mail Data

Now-a-days we are sending the messages on e-mail for saving the time. Sometimes such transaction is required to be proved. The Hon'ble Calcutta High Court in the case of **Abdul Rehaman v. The State of West Bengal [MANU/WB/0828/2014]** held that an e-mail down loaded and printed from an e-mail account of a person can be proved as per section 65B and 88A of the Evidence Act. The testimony of a witness who has carried out the procedure of down loading and printing is sufficient to prove the communication. Thus, the only options to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence. Thus, in the case of CD, DVD, Memory Card etc. containing secondary evidence, the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

Video Recording

Now-a-days persons are very aware. They are having the smart phones. Many times they used to record the scene of offences. Now a days there is facility of Skype as well as video conferencing. Therefore for saving the time and money we can use this facility to record the evidence. The admissibility of the secondary electronic evidence has to be adjudged within the parameters of Section 65B of Evidence Act and the proposition of the law settled in the recent

judgment of the Apex Court and various other High Courts as discussed above. The proposition is clear and explicit that if the secondary electronic evidence is without a certificate u/s 65B of Evidence Act, it is not admissible and any opinion of the forensic expert and the deposition of the witness in the court of law cannot be looked into by the court. However, there are few gaps which are still unresolved as what would be the fate of the secondary electronic evidence seized from the accused wherein, the certificate u/s 65B of Evidence Act cannot be taken and the accused cannot be made witness against himself as it would be violative of the Article 19 of the Constitution of India. Recently in **Suvarna Rahul Musale Vs. Rahul Prabhakar Musale (2015 (2) Mh.L.J. 801)** the Hon'ble Bomay High Court in para 8 to 10 observed as follows;

"8. It is to be noted that our legislature has wisely taken note of this fact and accordingly has made the changes in the Evidence Act by amending Section 65 and thereby section 65A, 65B are inserted on the point of recording of evidence relating to electronic record and admissibility of electronic record. When the legislature has expanded the scope of term 'Evidence' acknowledging advance technology and scientific methods used by people in their day-to-day activities, it is the duty of the Judicial officers to put life to those letters of law by interpreting them effectively.

An Attitudinal change in Judges is required. We need to train ourselves to understand the pulse of the new generation who is avidly techno savvy. Though it is difficult for the Judges, especially who are in their middle age, to accept and digest the entry of new language and methods of evidence in the established judicial system, it is high time for us to change our mind set and see whether this new technology can help us to increase the speed

and also we have to take into account the convenience of the parties as our judicial system is necessarily litigant centric.

The presence of the person can be obtained physically so also virtually. What is important is that a person should be seen and be heard and vice versa. These are the methods of distant communication, which is possible by virtual measures and micro-speakers. Therefore, it is not necessary for the Judge to insist for the physical presence of the witness when it is not possible especially in the circumstances of this case, a virtual presence can be secured which is very much legal and for this purpose, it is not necessary for the Judge himself to give time but such evidence can be recorded by appointing Commissioner.

Conclusion

The admissibility of the secondary electronic evidence has to be adjudged within the parameters of Section 65B of Evidence Act and the proposition of the law settled in the recent judgment of the Apex Court and various other High Courts as discussed above. The proposition is clear and explicit that if the secondary electronic evidence is without a certificate u/s 65B of Evidence Act, it is not admissible and any opinion of the forensic expert and the deposition of the witness in the court of law cannot be looked into by the court. However, there are few gaps which are still unresolved as what would be the fate of the secondary electronic evidence seized from the accused wherein, the certificate u/s 65B of Evidence Act cannot

be taken and the accused cannot be made witness against himself as it would be violative of the Article 19 of the Constitution of India.

Paper prepared by Core Committee Group 'A'

(Smt. K.B.Agrawal)
Dist.Judge-1 & Addl.Sessions Judge, Jalgaon

(A.K.Patani)
Dist.Judge-4& Addl.Sessions Judge, Jalgaon

(S.S.Ghorpade)
Civil Judge, S.D., Jalgaon.

(B.D.Pawar)
3rd Jt. Civil Judge, S.D., Jalgaon.