Cyber adjudication, collection & admissibility of electronic evidence

The definition of 'evidence' has been amended to include electronic records (Section 3(a) of the Evidence Act). Evidence can be in oral or documentary form. The definition of 'documentary evidence' has been amended to include all documents, including electronic records produced for inspection by the court. The term 'electronic records' has been given the same meaning as that assigned to it under the IT Act, which provides for "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated micro fiche".

New Sections 65A and 65B were introduced to the Evidence Act under the Second Schedule to the IT Act, 2000.

Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B. Section 65B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record (ie, the contents of a document or communication printed on paper that has been stored, recorded and copied in optical or magnetic media produced by a computer ('computer output')), is deemed to be a document and is admissible in evidence without further proof of the original's production, provided that the conditions set out in Section 65B(2) to (5) are satisfied.

Conditions for the admissibility of electronic evidence

Before a computer output is admissible in evidence, the following conditions as set out in Section 65(B)(2) must be fulfilled:

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Section 65B(4) further provides that in order to satisfy the conditions set out above, a certificate of authenticity signed by a person occupying a responsible official position is required. Such certificate will be evidence of any matter stated in the certificate.

The certificate must:

- identify the electronic record containing the statement;
- describe the manner in which it was produced; and
- give such particulars of any device involved In the production of the electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer.

The certificate must also deal with any of the matters to which the conditions for admissibility relate.

Amitabh Bagchi v. Ena Bagchi (AIR 2005 Cal 11)

- Sec 65A & 65B were analyzed in the case. It was held to be inclusive of includes video conferencing.
- Physical presence of a person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing.

State of Maharashtra v. Dr. Praful B. Desai (AIR 2003 SC 2053)

It was held that, examination of witness through video conferencing is allowed and is regarded as an essential part of electronic evidence.

Jagjit Singh v. State of Haryana (2006) 11 SCC 1

Issue in the present matter was regarding the appreciation of digital evidence in the form of interview transcripts from television channels. It was held 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 of the persons taking action.

Presumptions Regarding Electronic Evidence

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. The Evidence

Act has been amended to introduce various presumptions regarding digital evidence.

Gazettes in electronic form

Under the provisions of Section 8lA of the Evidence Act, the court presumes the genuineness of electronic records purporting to be from the Official Gazette or any legally governed electronic record, provided that the electronic record is kept substantially in the form required by law and is produced from proper custody.

Electronic agreements

Section 84A of the Evidence Act provides for the presumption that a contract has been concluded where the parties' digital signatures are affixed to an electronic record that purports to be an agreement.

Secure electronic records and digital signatures

Section 85B of the Evidence Act provides that where a security procedure has been applied to an electronic record at a specific time, the record is deemed to be a secure electronic record from such time until the time of verification. Unless the contrary is proved, the court is to presume that a secure electronic record has not been altered since obtaining secure status. The provisions relating to a secure digital signature are set out in Section 15 of the IT Act. A secure digital

signature is a digital signature which, by application of a security procedure agreed by the parties at the time that it was affixed, is:

- unique to the subscriber affixing it;
- capable of identifying such subscriber; and
- created by a means under the exclusive control of the subscriber and linked to the electronic record to which it relates in such a manner that if the electronic record as altered, the digital signature would be invalidated.

It is presumed that by affixing a secure digital signature the subscriber intends to sign or approve the electronic record. In respect of digital signature certificates (Section 8Se of the Evidence Act), it is presumed that the information listed in the certificate is correct, with the exception of information specified as subscriber information that was not verified when the subscriber accepted the certificate.

Electronic messages

Under the provisions of Section 88A, it is presumed that an electronic message forwarded by a sender through an electronic mail server to an addressee corresponds with the message fed into the sender's computer for transmission. However, there is no presumption regarding the person who sent the message. This provision presumes only the authenticity of the electronic message and not the sender of the message.

Five-year old electronic records

The provisions of Section 90A of the Evidence Act make it clear that where an electronic record is produced from custody which the court considers to be proper and purports to be or is proved to be five years old, it may be presumed that the digital signature affixed to the document was affixed by the signatory or a person authorized on behalf of the signatory. An electronic record can be said to be in proper custody if it is in its natural place and under the care of the person under whom it would naturally be. At the same time, custody is not considered improper if the record is proved to have had a legitimate origin or the circumstances of the particular case are such as to render the origin probable. The same rule also applies to evidence presented in the form of an electronic copy of the Official Gazette.