International Journal of Pure and Applied Mathematics
Volume 120 No. 5 2018, 1317-1328
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

TYPES OF ELECTRONIC DEVICES AND THEIR RELIABILITY

[1]DINESHWARI C.P, [2]Dr.A.SREELATHA

[1]Student, BA,BL,(hons), Final Year, saveetha school of law, saveetha university, Saveetha institute of medical and technical sciences, Chennai, Tamilnadu, India

[2]Professor, Saveetha School Of Law, Saveetha University, Saveetha institute of medical and technical sciences, Chennai, Tamilnadu, India

[2]annamanenisreelatha.ssl@saveetha.com

ABSTRACT:

Electronic evidence in criminal and civil proceedings, no doubt is always seem to be problematic. A Mindful emergence of new technologies has raised legitimate concerns about its accuracy and authenticity. Although the formal conditions to the admissibility of electronic evidence have been removed,1 the increasing complexity and sophistication of rapidly developing technology necessitates a shift from concerns about exclusion and admissibility subject to overly - technical requirements towards a more precise focus on issues relevant to establishing authenticity and suitable weight for the evidence which it generates. In Anvar v. P. K. Basheer.2, the Supreme Court noted that "there is a revolution in the way that evidence is produced before the court". When electronically stored information was treated as a document in India before 2000, secondary evidence of these electronic "documents" was adduced through printed reproductions or transcripts, and the authenticity was certified. When the creation and storage of electronic information grew more complex, the law had to change more substantially.

Keywords: Reliability, Electronic Evidence Email,technology,criminal activity.

INTRODUCTION:

The last twenty - five years have witnessed rapid developments in technology resulting in significant changes to the physical nature of computers, networked - technology, communications and a range of applications. Many of the features of modern communications

technology such as low cost, ease of use and the potential of anonymity and pseudonymous activity make new technologies an appealing medium for committing and facilitating criminal activity too. The point of the paper is to contemplate the idea of types of electronic evidence and their reliability.

OBJECTIVES:

1. To examine the witness
2. To analyse on the types of evidence
3. To study on realablity
4. To prove electronic evidence is an evidence

HYPOTHESIS:

NULL HYPOTHESIS: In the many cases the electronic evidence is not admissible in court

ALTERNATIVE HYPOTHESIS: In the court is admissible in realting to facts and circumstances and satisfied sec 65A and 65B of IPC.

RESEARCH METHODOLOGY:

The research methodology used in the project is the non-emprical type of research. The source from where the data has been collected are the secondary sources .The secondary sources are used for referring the case law and collecting the material .material is also collected from print and electronic media like various search engines and internet databases .from the collected material and information research proposes to critically analyze the topic of the study and tries to teach the core aspects of study.

THE INDIAN EVIDENCE ACT, 1872:

The involvement of technology in criminal activity also means an abundance of evidence. Data in the course of transmission or stored in some form of storage media are now valuable sources of evidence in criminal and civil proceedings. New technological capabilities, a range of applications and a modern global communications system with a growth in network - based crimes have produced many new forms of electronic evidence. Many of the earlier held assumptions that a computer is just like a “compact filing cabinet”3 or that computer documents

are just like the paper equivalent no longer hold true.4 Increasingly courts are being presented with evidence that includes more than the obvious computer printouts. Electronic evidence can originate from a variety of sources, in different file formats and application systems, across a number of jurisdictions.

The Electronic evidence can originate from a variety of sources, in different file formats and application systems, across a number of jurisdictions. These days, the admissibility of electronic evidence in any jurisdiction is increasingly more common: comments in social media, video recordings, instant messaging, certified emails, etc. But this wide variety of sources of digital evidence must have access to the judicial process through some of the legally prescribed means of proof. For clarifying this topic, in this article we will answer the following questions : what is electronic evidence and how admissible it is in court?

The definition of electronic evidence and its admissibility for a judge in court The emergence and popularization of digital communication (instant messaging, social networks, certified email, etc.) has not only provoked a revolution in the way that we relate to our personal and work life, but also in the legal environment and especially in the field of computer law. We no longer understand how to relate to each other without technology. Digital media evolves everyday and floods our daily life. Faced with this massive use of electronic instruments, the legal environment is enjoying LegalTech solutions that are redesigning the sector, as it faces unknown conflicts due to the increase of new electronic evidence.

What is electronic evidence?

We define electronic evidence as all information with probative value that is included in an electronic media or is transmitted by said media.

For this, we distinguish two basic types of electronic evidence:

1. Data stored in computer systems or devices.

2. Information transmitted electronically through communication networks.

What are the steps for collecting and using electronic evidence?

In any jurisdiction, collecting and using electronic evidence has the following steps, as explained by the Judge Joaquín Delgado Martín in his article "The value of digital evidence" (in Spanish):

• Obtaining the information.

The parties must access the information in a lawful manner, without violating the fundamental rights.

• Incorporating data to the process.

In order to incorporate the data into the process, it should meet some requirements: relevance, necessity, legality and procedural admissibility.

• Value of the incorporated data.

Lastly, if the above requirements on obtaining and incorporating data are met, the electronic evidence will be subject to assessment by a judge or court.

PROCEDURAL POSITION OF THE PARTIES:

In making an assessment, the judge should keep in mind the position of each party related to the electronic evidence provided, especially if the opposing party rejects (contests) its validity.

• If no objection is made, meaning that the validity of the electronic evidence is not questioned, the judge will have to consider it as authentic and accurate, and will evaluate it together along with the rest of the evidence.

• If there is an objection, then the arguments that argue for its rejection and those that show the evidence and expert opinions to prove its validity are both relevant for the judge.

Thus, in practice, the party seeking the validity of electronic evidence must provide all evidence possible to strengthen the evidence provided, usually with a computer expert who proves the authority and non-manipulation of have produced many new forms of electronic evidence. Many of the earlier held assumptions that a computer is just like a "compact filing cabinet"3 or that computer documents are just like the paper equivalent no longer hold true.4 Increasingly courts are being presented with evidence that includes more than the obvious computer printouts. Electronic evidence can originate from a variety of sources, in different file formats and

application systems, across a number of jurisdictions. Sources of such evidenceSuch electronic data can often serve to disprove claims and defeat cases as it contains uncensored personal information the parties assumed were off limits due to their seemingly private nature. To the contrary, however, the courts have taken the view that where the evidence contained in such sources of electronic data is relevant to the matters at issue in the action, preservation and production of the evidence should be ordered subject to principles of proportionality' imposed by Ontario's Rules of Civil Procedure9 .10 As a result, in many recent Canadian decisions, photographs of parties that had been posted to their Facebook profiles were admitted as relevant documents subject to production.11

To illustrate the point that few areas of our daily lives are immune from the effects of new media, consider the story of a Quebec woman who lost her insurance benefits because of the photos posted on a popular social networking site. The woman was on long-term sick benefits for a year and a half after she was diagnosed with major depression. Her insurance company, Manulife, cut off her benefits after seeing photos posted on Facebook of the woman having a good time at a Chippendales bar show, at her birthday party and on holiday. Electronic evidence in criminal and civil proceedings, no doubt is always seem to be problematic. A Mindful emergence of new technologies has raised legitimate concerns about its accuracy and authenticity. Although the formal conditions to the admissibility of electronic evidence have been removed,1 the increasing complexity and sophistication of rapidly developing technology necessitates a shift from concerns about exclusion and admissibility subject to overly - technical requirements towards a more precise focus on issues relevant to establishing authenticity and suitable weight for the evidence which it generates. In Anvar v. P. K. Basheer.2, the Supreme Court noted that “there is a revolution in the way that evidence is produced before the court”. When electronically stored information was treated as a document in India before 2000, secondary evidence of these electronic “documents” was adduced through printed reproductions or transcripts, and the authenticity was certified. The expansion of PCs and the impact of data innovation on society as entire, combined with the capacity to store and hoard data in computerized frame have all required alterations in Indian law, to fuse the arrangements on the energy about advanced proof. The Information Technology Act, 2000 and its revision depends on the United Nations Commission on International Trade Law (UNCITRAL) demonstrate Law on Electronic Commerce. The Information Technology (IT) Act 2000, was changed to take into

account the suitability of computerized prove. A correction to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 gives the administrative system to exchanges in electronic world. Advanced confirmation or electronic proof is any probative data put away or transmitted in computerized frame that a gathering to a court case may use at trial. Before tolerating computerized confirm it is fundamental that the assurance of its importance, veracity and realness be determined by the court and to build up if the truth of the matter is prattle or a duplicate is liked to the first. Advanced Evidence is "data of probative esteem that is put away or transmitted in double frame". Proof isn't just restricted to that found on PCs yet may likewise stretch out to incorporate confirmation on advanced gadgets, for example, media transmission or electronic sight and sound gadgets. The e-EVIDENCE can be found in messages, advanced photos, ATM exchange logs, word preparing, reports, text chronicles, records spared from bookkeeping programs, spreadsheets, web program accounts databases, Contents of PC memory, Computer reinforcements, Computer printouts, Global Positioning System tracks, Logs from an inn's electronic entryway locks, Digital video or sound documents. Advanced Evidence has a tendency to be more voluminous, more hard to demolish, effectively adjusted, effortlessly copied, possibly more expressive and all the more promptly accessible. PC criminology is a branch of criminological science relating to legitimate proof found in PCs and computerized stockpiling mediums. PC crime scene investigation is otherwise called computerized criminology. The objective of PC criminology is to clarify the present condition of an advanced relic. The term advanced antiquity can include: A PC framework stockpiling medium (hard circle or CD-ROM) an electronic archive (e.g. an email message or JPEG picture) or even a grouping of parcels moving over a PC arrange. The meaning of 'confirm' has been changed to incorporate electronic records. The meaning of 'narrative proof' has been changed to incorporate all reports, including electronic records delivered for examination by the court. Area 3 of the Evidence Act, 1872 characterizes confirm as under: "Confirmation" - Evidence implies and incorporates:- 1) all announcements which the court allows or requires to be made before it by witnesses, in connection to issues of reality under request; such articulations are called oral proof; 2) all reports including electronic records created for the assessment of the court. Such records are called narrative confirmation. The term 'electronic records' has been given an indistinguishable significance from that alloted to it under the IT Act. IT Act accommodates "information, record or information produced, picture or sound put away, got or

sent in an electronic frame or microfilm or PC created microfiche". The meaning of 'affirmation' (Section 17 of the Evidence Act) has been changed to incorporate an announcement in oral, narrative or electronic frame which recommends a deduction to any reality at issue or of pertinence. New Section 22-A has been embedded into Evidence Act, to accommodate the pertinence of oral proof with respect to the substance of electronic records. It gives that oral affirmations in regards to the substance of electronic records are not important unless the validity of the electronic records delivered is being referred to. The meaning of 'prove' has been revised to incorporate electronic records. The meaning of 'narrative confirmation' has been revised to incorporate all reports, including electronic records delivered for investigation by the court. New segments 65-An and 65-B are acquainted with the Evidence Act, under the Second Schedule to the IT Act. Area 65-A gives that the substance of electronic records might be demonstrated as per the arrangements of Section 65-B. Area 65-B gives that despite anything contained in the Evidence Act, any data contained in an electronic, is considered to be a record and is permissible in confirm without additional confirmation of the first's generation, given that the conditions set out in Section 65-B are fulfilled. The conditions indicated in Section 65-B (2) are:

1. Firstly, the PC yield containing the data ought to have been delivered by the PC amid the period over which the PC was utilized frequently to store or process data with the end goal of any exercises consistently carried on finished that period by the individual having legitimate control over the utilization of the PC.

2. The second prerequisite is that it must be demonstrated that amid the said period the data of the kind contained in electronic record or of the kind from which the data contained is inferred was 'routinely encouraged into the PC in the standard course of the said movement'.

3. A third necessity is that amid the material piece of the said period, the PC was working legitimately and that regardless of whether it was not working appropriately for quite a while that break did not influence either the record or the exactness of its substance.

4. The fourth prerequisite is that the data contained in the record ought to be a generation or got from the data bolstered into the PC in the standard course of the said movement.

Under Section 65-B(4) the authentication which recognizes the electronic record containing the announcement and portrays the way in which it was delivered giving the particulars of the gadget

associated with the creation of that record and manages the conditions specified in Section 65-B(2) and is marked by a man possessing a capable authority position in connection to the task of the applicable gadget 'might be proof of any issue expressed in the testament'.

Segment 65-B(1) states that if any data contained in an electronic record created from a PC (known as PC yield) has been duplicated on to an optical or attractive media, at that point such electronic record that has been replicated 'should be considered to be additionally a report' subject to conditions set out in Section 65-B(2) being fulfilled. Both in connection to the data and additionally the PC being referred to such archive 'might be acceptable in any procedures when additional verification or creation of the first as confirmation of any substance of the first or of any reality expressed in that of which coordinate proof would be allowable.'

ELECTRONIC EVIDENCE - CASE LAW'S:

- ✓ **Amitabh Bagchi Vs. Ena Bagchi**[1] [Sections 65-An and 65-B of Evidence Act, 1872 were analyzed. The court held that the physical nearness of individual in Court may not be required for reason for illustrating proof and the same should be possible through medium like video conferencing. Areas 65-Aand 65-B give arrangements to confirmations identifying with electronic records and suitability of electronic records, and that meaning of electronic records incorporates video conferencing.
- ✓ **State of Maharashtra versus Dr Praful B Desai**[2] The question included whether a witness can be analyzed by methods for a video conference. The Supreme Court watched that video conferencing is a progression of science and innovation which grants seeing, hearing and conversing with somebody who isn't physically present with an indistinguishable office and simplicity from on the off chance that they were physically present. The lawful necessity for the nearness of the witness does not mean real physical nearness. The court permitted the examination of an observer through video conferencing and inferred that there is no motivation behind why the examination of an observer by video conferencing ought not be a fundamental piece of electronic proof.

[1] AIR 2005 Cal 11
[2] AIR 2003 SC 2053

- ✓ **BODALA MURALI KRISHNA VS. SMT. BODALA PRATHIMA**[3] The court held that, "… the alterations conveyed to the Evidence Act by presentation of Sections 65-A and 65-B are in connection to the electronic record. Areas 67-A and 73-A were presented as respects confirmation and check of computerized marks. As respects assumption to be drawn about such records, Sections 85-A, 85-B, 85-C, 88-A and 90-A were included. These arrangements are eluded just to exhibit that the accentuation, at display, is to perceive the electronic records and advanced marks, as allowable bits of confirmation."
- ✓ **DHARAMBIR Vs. Focal BUREAU OF INVESTIGATION**[4] The court touched base at the conclusion that when Section 65-B discusses an electronic record delivered by a PC alluded to as the PC yield) it would likewise incorporate a hard circle in which data was put away or was before put away or keeps on being put away. It recognized as there being two levels of an electronic record. One is simply the hard plate which once utilized turns into an electronic record in connection to the data with respect to the progressions the hard circle has been liable to and which data is retrievable from the hard circle by utilizing a product program. The other level of electronic record is the dynamic open data recorded in the hard plate as a content document, or sound record or a video record and so on. Such data that is open can be changed over or replicated all things considered to another attractive or electronic gadget like a CD, pen drive and so on.

CONCLUSION:

Is there is a need to further amend or to legislate a separate law of evidence to deal with the issue of interpretation and a Businesses not only depend on computers to record their business activities but are now required to produce those records (to the extent they are relevant) in electronic form. Parties seeking to avoid the sting of their electronic words or deeds often seek to discredit the electronic evidence being relied upon by their opponents principally by attacking the authenticity of the evidence. Good record keeping practices coupled with the help of computer forensic experts can help to refute these objections to the use of electronic evidence. Demission of digital source as evidence in court a part from the law already existed.

[3] 2007 (2) ALD 72
[4] 148 (2008) DLT 289

REFERENCE:

[1]. Dr. B.N. Mani Tripathi, Jurisprudence (All. Law Agency, 17th ed, 2006).

[2]. C.K Takwani, Lectures on Administrative Law (Eastern Book Co., 2nd ed, 1994).

[3]. The Indian evidence Act, 1872, Section 3.

[4]. The Information Technology Act, 2000 (Act No. 21 of 2000)

[5]. Vepa P Sarthi, Law of Evidence, (Eastern Book Co. 6th ed , 2006)

[6]. Nayan Joshi, Electronic Evidence, (Kamal Publishers, New Delhi 2016)

[7]. R.V. Kelkar's, Criminal Procedure ((Eastern Book Co. 5th ed , 2008)

8. *Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier. ISBN 0-12-13104-4.*

10...*Various (2009). Eoghan Casey, ed. Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 0-12-374267-6. Retrieved 2 September 2010.*

"'The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice""Legal Aspects of Digital Forensics""State v. Schroeder, 613 NW 2d 911 - Wis: Court of Appeals 2000"

11.. *"US v. Bonallo". Court of Appeals, 9th Circuit. 1988. Retrieved 1 September 2010.*

12. *Zupanec, Donald (1981-01-01). "Admissibility of Computerized Private Business Records". American law reports. alr 4th. cases and annotations. 7. pp. 16–19.*

13. *Pollitt, MM. "Report on digital evidence". CiteSeerX 10.1.1.80.1663.*

14. *"ACPO Good Practice Guide for Digital Evidence" (PDF). Retrieved 26 April 2016.*

15.."Federal Rules of Evidence #702". *Retrieved 23 August 2010*

16'Alorie Gilbert, *Newsmaker: Fixing the Sorry State of Software*, CNETNews, Oct. 9, 2002 (interviewing William Guttman, Director, CyLabSustainable Computing Consortium, Carnegie Mellon University), athttp://news.com.com/2008-1082-961370.html.

17."Software" as used in this article includes traditional softwareinstruction sets, as well as those found in firmware, and hardware.

18... Florida v. Bjorkland, No. 2004 CT 014406 SC (Sarasota County, 2005).

19.. Coca-Cola Bottling Co. v. Coca-Cola Co., 107 F.R.D. 288 (D. Del.1985).

20. See Fed. R. Civ. P. 45, Committee Notes, 1991 Amendment *Subdivision(a)* ("Fourth, *Paragraph (a)(1)* authorizes the issuance of subpoena to compel a non-party to produce evidence independent of any deposition."); *cf*. Fed. R. Civ. P. 26(c)(7) (court *may* grant protective order to limit disclosure of trade secrets, but is not required to do so.

21. Dr.Lakshmi T and Rajeshkumar S 2018, "*In Vitro Evaluation of Anticariogenic Activity of Acacia Catechu against Selected Microbes*", International Research Journal of Multidisciplinary Science & Technology, Volume No. 3 , Issue No. 3, P.No 20-25.

22. Trishala A , Lakshmi T and Rajeshkumar S 2018," *Physicochemical profile of Acacia catechu bark extract –An In vitro study*", International Research Journal of Multidisciplinary Science & Technology, Volume No. 3 , Issue No. 4, P.No 26-30.