Jamshed al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 1, March 2016, pp. 148~150

Reliability of Electronic Evidence

Jamshed

Assistant Professor, Campus Law Centre, University of Delhi

***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

I. 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 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. Sources of such evidence include seized computer hard - drives and back - up media, real -time email messages, chat - room logs, ISP records, web pages, digital network traffic, local and virtual databases, digital directories, wireless devices and memory cards. With technology rapidly evolving, "unique file formats" across various storage media are in the "hundreds of thousand making it impossible to be familiar with every variation of every kind of digital evidence"[5] This evidence can take the form of data digitally stored as text files, graphics files, sounds, motion pictures, databases, temporary files, cache files, deleted files, and computer data generated on the storage device by the operating system or application program.[6] A simple file can contain incriminating information and have associated properties useful for investigations such as details about when a file was created, on which computer and by whom.[7]

In a networked environment, sources of evidence include server logs, the contents of devices connected to the network and the records of traffic activity.[8] Different crimes involving computers result in different types of evidence. Cyber stalkers often use electronic mail communications to harass their victims; computer hackers may leave evidence of their activities in network logs files; and cases involving pornographic material the most likely

[1] The Indian Evidence Act, 1872.

[2] AIR 2015 SC 180.

[3] C Reed, The Admissibility and Authentication of Computer Evidence: A Confusion of Issues, 2, (*5th BILETA, 2005)* ***available at*** http://www.bileta.ac.uk/90papers/reed.html.

[4] P Sommer, Digital Footprints: Assessing Computer Evidence, 2 (CSRC, London School of Economics and Political Science) ***available at*** https://www.google.co.in/webhp?hl=en-IN#hl=en IN&q=P+Sommer%2C+Digital+Footprints: +Assessing+Computer+Evidence.

[5] E Casey, Digital Evidence and Computer Crime, 231, (Elsevier Academic Press CA, 2nd edn, 2004).

[6] R v Porter (Ross Warwick) (2006) EWCA Crim 560.

[7] Supra Note 5.

[8] S. Mason, Sources of Digital Evidence: Disclosure, Discovery and Admissibility, 1, 12, (LexisNexis Butterworth's London, 1st edn, 2007).

source of evidence are digitized images found on computers or other storage media.[9]

The special characteristics of electronic evidence also raise concerns about the accuracy and authenticity of the evidence. This is primarily due to the intangible and transient nature of data, especially in a networked environment where such evidence can be created, stored, copied and transmitted with relative ease. It can also be modified or tampered without signs of obvious distortions, thereby rendering the process of investigation and recording of evidence extremely vulnerable to claims of errors, accidental alteration, prejudicial interference or fabrication.[10]

Electronic evidence can also be easily changed because of the processes involved in collecting it as evidence.[11] Errors can be introduced during examination and interpretation of the evidence or the examination tools being used can contain malicious software or viruses that can cause them to represent the data incorrectly.[12] Shutting down a system for example may necessarily destroy all process - related data. The process of opening a file or printing is not always neutral and its source and integrity is not always easy to prove. Given the volatility of the data, a failure to follow crime - scene protocols and proper procedures for handling computer evidence may render such evidence unusable or vulnerable to defence claims of errors or prejudicial distortions.[13] Therefore technical obsolescence is a major problem maintaining access to digital records over the long - term involves interdependent strategies for preservation in the short to medium term based on safeguarding storage media, content and documentation, and computer software and hardware; and strategies for long - term preservation to address the issues of software and hardware obsolescence.[14]

The main obvious issue in reading data relates to what can be seen. Electronic evidence is, by its very nature, binary patterns in magnetic, optical or electronic form all of which need to be translated and interpreted for the court - "Evidence of these crimes is neither physical nor human, but, if it exists, is little more than electronic impulses and programming codes. If someone opened a digital storage device, they would see no letters, numbers, or pictures on it". Most computers and operating systems now function in a networked environment, using products (notebook computers, mobile phones, PDAs, etc) and using various applications (e-mailing, instant / text messaging, 'blogging', chat -rooms) that run over networks (the Internet, wireless and cellular networking). For investigators the challenges involve a greater variety of evidence that may be found anywhere on the global communications network:

"The nature of this structure means that almost everything anybody does on a device that is connected to a network is capable of being distributed and duplicated with ease. As a result, the same item of digital data can reside almost anywhere.[15] However, when dealing with network - based evidence, investigators face a number of unpredictable challenges.

Data on networked systems are dynamic and volatile, making it difficult to take a snapshot of a network at any given instant. Unlike a single computer, it is rarely feasible to shut a network down because digital investigators often have a responsibility to secure evidence with minimal disruption to business operations that rely on the network. Besides, shutting down a network will result in the destruction of most of the digital evidence it contains. Also, given the diversity of network technologies and components, it is often necessary to apply best evidence collection techniques in unfamiliar contexts.

In what is referred to as the "identity" problem, investigators face a number of challenges when dealing with TCP/IP addresses as evidence. For example, IP headers only contain information about computers, not people, and as a result, it is difficult to prove that a specific individual created a given packet. However, such information certainly is beneficial as an investigative lead and the source IP address can be used to get closer to the origin of the crime which may help identify suspects. However, this may be hindered by offenders who frequently change their IP addresses (using dynamic IP addresses) so as to avoid detection. Investigators face similar difficulties in tracing the offender when information in the IP header is falsified or when a source IP address has been falsified and tracking becomes a lengthy and tedious process of examining log files on all of the routers that the information passed through. [16]

Therefore, given our current digital society, the concept of digital evidence is expansive in scope. There has been a sea change in the purposes and the manner in which computers are used with advent of microprocessor technology and digital communication. The computer started with being a giant calculating machine. It then metamorphosed itself into a standalone personal tool for performing assorted routine tasks like word processing and accounting and then to today's network device permeating virtually everything including instantaneous and global personal and business interaction. The way business is conducted and records are maintained today is a far cry from days past. Accordingly, in enforcement agencies, more and more information is being stored, transmitted or processed in digital form.

The law of the country has also taken cognizance of this reality. The Information Technology

[9] Supre Note 5.

[10] I Walden , Computer Crime, ***available at*** http://kavehh.com/my%20Document/KCL/Internet%20Law/reading/Computer%252Crime%2520%25286th%2520ed.%2529.pdf.

[11] P Sommer 'Downloads, Logs and Captures: Evidence from Cyberspace' [2002] CTLR 33.

[12] Supra Note 5 at p8, 133.

[13] Supra Note 10.

[14] Digital Preservation Coalition, Organizational Activities, ***available at:*** http://handbook.dpconline.org/organisationalactivities/ storage.

[15] Supra Note 8. at p 8.

[16] Supra Note 5.

Act, 2000 has been enacted recognizing electronic records as evidence, governing access to and acquisition of digital and electronic evidence from individuals, corporate bodies and / or from the public domain. By way of this enactment, amendments were also brought in other laws like Indian Penal Code; Special provisions as to evidence relating to electronic record have been inserted in the form of section 65A & 65B, after section 65, in Indian Evidence Act. These provisions are very important and they govern the integrity of the electronic record as evidence, as well as, the process for creating electronic record. Also the Criminal Procedure Code, (Cr.PC) was amended thereafter. The Income - tax Act, 1961 has also been amended thrice by way of Finance Act 2001, Finance Act 2002 and Finance Act 2009 thereby according recognition to electronic evidence, facilitating access to them and giving when need be, powers to impound and seize them. By Finance Act, 2001, Clause (22AA) was inserted in Section 2 to provide that the term "document" in Income Tax Act, 1961, includes an electronic record as defined in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000. By Finance Act, 2002, Clause (iib) was inserted in Sub-Section (1) of Section 132 requiring any person who is found to be in possession or control of any books of account or other documents maintained in the form of electronic record as defined in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000), to afford the authorized officer the necessary facility to inspect such books of account or other documents; and by Finance Act, 2009, clause (c) was inserted in sub-section (1) of Section 282 providing that service of notice in the form of any electronic record as provided in Chapter IV of the Information Technology Act, 2000 (21 of 2000) will constitute valid service Maintaining the integrity of electronic evidence through various processes such as identification of evidence, retrieval of deleted evidence, examination of such evidence, etc., presents problems which are different from the problems encountered in handling of traditional physical or documentary evidence. Also the Supreme Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and also the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible. Thus, the only options left to prove the electronic record/evidence is by producing the original electronic media as Primary Evidence in court or its copy by way secondary evidence U/s 65A/65B of Evidence Act. But this would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases where the reliance is being placed on the audio video recordings which are being forwarded in the form of CD/DVD to the Court. Therefore here seem to be a need for some liberal and welfare rule for the governance of digital evidence for delivery of justice.

II. OBJECTIVES OF THE PAPER.

The central aim of this thesis is to cast light on the current problems of adducing digital source as evidence before the Indian courts during trial of civil and criminal cases. The thesis has also a law reformist ambition. It also aims to fill the gaps of the pre -existing discussion on the admissibility of electronic evidence and will try to provide an answer to a question that: whether the law subsisting in the country is adequate to deal with the problems associated with the interpretation and admissibility of digital source as digital evidences?

The answer would bring following agendas into productive dialogue as under.

1. How well informed are litigants, investigating agencies, Executive, Lawyers and Judges about the nature and application of digital Source as evidence.

2. What is the impact of digital source upon being considered as evidence on adjudication of any civil and criminal trial?

III. 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 admission of digital source as evidence in court a part from the law already existed..

REFERENCES

[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)

