

“Electronic Evidence

In India

The Emerging Scenario”



Mr. B. Gopalakrishnan
President & Head (Law)
Axis Bank Ltd.

Conference on Intellectual Property Rights 2011, Mumbai

@ The Hotel Leela Kempinski on December 16, 2011 @ 5.15 p.m.

© B. Gopalakrishnan. All rights reserved

1. Introduction
2. Background
3. General Forms/ Types
4. Computer Forensics
5. Digital Evidence Analysis
6. Job of Digital Evidence Analyst
7. Indian Law on E-evidence
8. Admissibility of E-evidence
9. Important Cases
10. Legal Perspective
11. Changes in Bankers' Books Evidence Act
12. Legal Issues
13. Drawbacks of E-evidence
14. Recommendations
15. Way Ahead

Introduction

The last few years of the 20th Century saw rapid strides in the field of science and information technology.

The expanding horizon of science and technology threw new challenges for the ones who had to deal with proof of facts in disputes where advanced techniques in technology was used and brought in aid.

This brought out a new source of evidence namely **Digital OR Electronic Evidence.**

- ❏ Then came the question whether Digital evidence is admissible OR good enough in the Court?
- ❏ Whether the existing laws (especially the Indian Evidence Act), really provided for proving OR taking into consideration such evidences as admissible?
- ❏ If so, whether it is a Primary Evidence OR supplementary evidence?

E-evidence – Is it admissible in the Court of Law?

Background:

- 📄 The need to have an accurate, authentic, complete, durable and reproducible memory of facts.
- 📄 The need to be able to believe the story that is being told to us.
- 📄 If we know all the facts for sure, we will know how to judge the situation fairly in front of the law.

Thus, the need to have reliable evidence, capable of providing objective conviction about the facts.

The absence of appropriate evidence opens the door to:

i) uncertainty about what the true story is; ii) misconception of the reality; iii) injustice.

Digital Evidence: According to the Scientific Working Group on Digital Evidence (SWGDE), Digital Evidence is “information of probative value that is stored or transmitted in binary form”. Therefore, according to this definition, evidence is not only limited to that found on computers but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices

- Most countries admit it as evidence;
- Its strength as evidence depends very much on the reliability of the technology;
- How to prove reliability of technology;
- Is it durable evidence? (evolution of technology)

Kind of Evidence Normally used

- Witnesses (testimony and confession);
- Documentary (photographs, writings, objects, etc.)
- Opinion of experts, site inspections and technology (forensic activity).

The means we use to record the memory of our activity.

What makes evidence credible

- It must be complete;
- It must be accurate;
- It must be authentic;
- It must be enough;
- It must be obtained and submitted validly.

Use of E-evidence

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

General forms of Electronic Evidence

- 📧 Email
- 📄 Wordprocessor, Electronic Spreadsheet files
- 📄 Relational database (record) file
- 📄 Software source code
- 📄 Various image files (.tiff, .jpeg, .pcx)
- 📄 Web browser bookmarks / cookies / cache memory
- 📄 Calendar; to-do-list, contact list
- 📄 Voice mail

Types of Electronic Information

- 📄 Active files
- 📄 Archival files
- 📄 Residual files

Computer Forensics

- ❏ Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics.
- ❏ The goal of computer forensics is to explain the current state of a digital artifact. The term digital artifact can include a computer system, storage medium (such as a hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image) or even a sequence of packets moving over a computer network.
- ❏ Thus, computer forensics is the "who, what, when, and how" of electronic evidence.
- ❏ Typically narrow in scope, it attempts to reconstruct events, focusing on the computer-based conduct of an individual or group of individuals.
- ❏ According to the Sedona Conference, a legal and political think tank founded for the purpose of establishing reasonable standards and principles for handling electronic evidence, "computer forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage.
- ❏ Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. At the heart of computer forensics is the idea that within the electronic realm of evidence, delete does not really mean delete.

Digital Evidence Analysis

- ❏ Digital Evidence Analysis involves the collection, investigation and analysis of digital evidence.
- ❏ This digital evidence may be found in computer hard disks, cell phones, ipods, pen drives, digital cameras, CDs, DVDs, floppies, computer networks, the Internet etc.
- ❏ Digital evidence can be hidden in pictures (steganography), encrypted files, password protected files, deleted files, formatted hard disks, deleted emails, chat transcripts etc.
- ❏ Digital evidence can relate to online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, divorce cases, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling etc.

Job of Digital Evidence Analyst

- ❏ Performs forensic analysis of digital information using standard computer forensics & evidence handling techniques.
- ❏ Uses forensically sound procedures to identify network computer intrusion evidence and identifies perpetrators.
- ❏ Employs forensic tools and techniques to identify and examine malicious files.
- ❏ Employs forensic tools and techniques to crack file and system passwords.
- ❏ Detects steganography and recovers deleted, fragmented and corrupted data from digital media of all types.
- ❏ Observes proper evidence custody and control procedures.
- ❏ Documents procedures and findings in a manner suitable for courtroom presentation and prepares comprehensive written notes and reports.

Indian Law on E-evidence

- ❏ The proliferation of computers, 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.
- ❏ The Information Technology Act, 2000 ("IT Act") based on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce and, together with amendments to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in electronic world.
- ❏ The definition of 'evidence' has been amended to include electronic records. The definition of 'documentary evidence' has been amended to include all documents, including electronic records produced for inspection by the court.
- ❏ Section 3 of the Evidence Act, 1872 defines evidence as under:
"Evidence" - Evidence means and includes:-
 - 1)-----
 - 2) all documents including electronic records produced for the inspection of 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 microfiche".
- ❏ Section 2(c) of the IT Act, 2000 reads: "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 record."



Admissibility of E-evidence

- ❏ The definition of 'admission' (Section 17 of the Evidence Act) has been changed to include a statement in oral, documentary or electronic form which suggests an inference to any fact at issue or of relevance.
- ❏ New Section 22A has been inserted into the Evidence Act to provide for the relevancy of oral evidence regarding the contents of electronic records. It provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question.
- ❏ New sections 65A and 65B are introduced to the Evidence Act under the Second Schedule to the IT Act.
- ❏ 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, 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 are satisfied.

Admissibility of E-evidence (Contd...)

- ❏ A perusal of the title to Section 65B which has been introduced by an Amendment made in 2000 simultaneous with the enactment of the IT Act with effect from 17th October, 2000 indicates that it concerns admissibility of the electronic records' at the stage of the trial when the question arises whether a certain electronic record is admissible in evidence or not.
- ❏ Section 65B(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 65B(2) being satisfied.
- ❏ Both in relation to the information as well as the computer in question such document 'shall be admissible in any proceedings when further proof or production of the original as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.'

The conditions specified in Section 65(B)(2) are:

1. 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. It must be shown that during the said period the information of the kind contained in electronic record or of the kind from which the information contained is derived was 'regularly fed into the computer in the ordinary course of the said activity'.
3. 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 that break did not affect either the record or the accuracy of its contents.
4. 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 65B(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 the relevant device 'shall be evidence of any matter stated in the certificate.'

Rationale from Important Cases on E-evidence

A] In **Amitabh Bagchi Vs. Ena Bagchi**, sections 65A and 65B of Evidence Act, 1872 were analysed. The court held that the physical presence of person in Court may not be required for purpose of adducing evidence and the same can be done through medium like video conferencing. Sections 65A and 65B provide provisions for evidences relating to electronic records and admissibility of electronic records, and that definition of electronic records includes video conferencing.

B] The same rationale was followed in **State of Maharashtra v Dr Praful B Desai** which involved the question whether a witness can be examined by means of a video conference. The 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 a 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.

Rationale from Important Cases on E-evidence

C] In **Bodala Murali Krishna Vs. Smt. Bodala Prathima**, the court held that, "...the amendments carried to the Evidence Act by introduction of Sections 65-A and 65-B are in relation to the electronic record. Sections 67-A and 73-A were introduced as regards proof and verification of digital signatures. As regards presumption to be drawn about such records, Sections 85-A, 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."

D] Dharambirv. CBI (pronounced on 11th March 2008)

- Certain data (i.e. call records) were copied from Hard Disk to a CD.
- Cyber Forensics Lab in Hyderabad confirmed that the recorded data (i.e. call conversation) on CD were true copies of the originals and that the Hard Disk was in working condition.
- A question came: difference between "electronic device "and "electronic record".. It was held that if the electronic device has ever recorded any data which is relevant for a case, such "electronic device" shall be treated as "electronic record" for the purpose of evidence.

Scope of definition of the word "data" was contended and was held that "data" would include active memory as well as subcutaneous memory.

Legal Perspective

The Law Commission in England reviewed the law relating to computer generated evidence. It summed up the major problem posed for the rules of evidence by computer output in the words of Steyn, J.:-

"Often the only record of the transaction, which nobody can be expected to remember, will be in the memory of a computer. ... if computer output cannot relatively readily be used as evidence in criminal case, much crime (and notably offences involving dishonesty) would in practice be immune from prosecution. On the other hand, computers are not infallible. They do occasionally malfunction."

Indian courts have responded fairly well to the challenge that the E-evidence has thrown. The legal community has recognized the significant evidentiary role that computers play in civil and criminal cases. Some of the important computer forensic case law in both criminal and civil cases includes cases dealing with email investigations, deleted data etc.

Evidence –Bankers'Books Evidence Act, 1891

What is permissible as evidence?

A “**certified copy**” of any entry in a banker's book shall in all legal proceedings be received as prima facie evidence of the original entry itself. {Section 4}

What are banker's book in electronic form?

Any record stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism, either onsite or at any offsite location including a back-up or disaster recovery site of both. {Section 2(3)}

How a certified copy of electronic record be obtained?{Section 2(8)}

- A copy obtained through mechanical process can be certified if a certificate of the principal accountant or the manager of the bank.
- A printout containing a certificate in accordance with Section 2A.

Evidence –Bankers' Books Evidence Act, 1891 (Contd.....)

Nature of certificate for a copy obtained through mechanical process:

A certificate from principal accountant or manager of the branch that the mechanical or other process adopted to obtain the copy has ensured the accuracy of the copy.

Nature of certificate for a copy obtained through mechanical process:

- Authenticity certificate from principal accountant or branch manager, AND
- Certificate from person in-charge of computer system regarding
- *Details of computer system*
- *Process of data storage*
- *Safeguard to protect computer system and data*

A further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.









State Bank of India vs. RizviExports Ltd (DRT, Allahabad)

- State Bank of India (SBI) had filed a case to recover money from some persons who had taken various loans from it.
- As part of the evidence, SBI submitted printouts of statement of accounts maintained in SBI's computer systems.
- The relevant certificates as mandated by the Bankers Books of Evidence Act (as amended by Information Technology Act) had not been attached to these printouts.
- The Court held that these documents were not admissible as evidence.

E-evidence: Issues on the admissibility of computer records

- 📄 **Authentication:** Electronic records, like paper documents, must be authenticated before they can be admitted as evidence in court. The possible areas for challenge may be the reliability of the computer program that generated the records, and the identity of the author of a computer-stored record.
- 📄 **Identifying the Author of a computer-stored record:** A computer-stored record is a document that contains the writings of a person or persons in an electronic form. As with any evidence containing human statements, a computer-stored record is subject to the hearsay rule on the admissibility of evidence.
- 📄 **Challenging the Reliability of Computer Programs:** This is likely to be an important issue for computer-generated records. A computer-generated record contains the output of computer programs, without any human intervention.
- 📄 **Computer records that are both computer-generated and computer-stored:** A Excel spreadsheet containing financial figures processed by a person is an example of this type of computer record. The evidentiary issues here are : (a) the information contained in the Excel spreadsheet is subject to the hearsay rule; and (b) the Excel program itself is subject to challenge as to the reliability of the program.
- 📄 **The Hearsay Rule:** The hearsay rule exists to exclude out-of-court statements (statements made outside the courtroom) when such statements are used to affirm the truth of the facts contained in these statements and the makers of these statements are not witnesses in the court.
- 📄 **The Best Evidence Rule:** The *best evidence rule* states that “there is but one general rule of evidence, the best that the nature of the case will admit”. This rule has been interpreted in some jurisdictions to mean that no evidence other than the original of a writing is admissible to prove the content of the writing.

Drawbacks of E-evidence:

-  **Privacy Concerns:** One of the primary concerns of computer forensics is the impact it will have on the computer owner's privacy.
-  **Preservation:** Digital longevity problems stem from the short life of digital information caused by storage media deterioration, rapidly changing storage devices and shifting file formats.
-  **Cost:** Another major disadvantage of computer forensics is the cost. The cost to maintain a laboratory containing appropriate computers, computer analysis tools, software and security implements to safeguard information can be enormous.
-  **Data Corruption:** The forensics investigator can play a role in the preservation or the destruction of important data. A number of issues concerning the corruption of important data are necessary to note.
-  **Malicious programs/ Virus:** There are also the chances of introduction of some malicious programs in the computer system that may corrupt the data at a later stage of time. During the analysis process there could be chance of release/ introduction of computer virus in the system.
-  **Opportunity for criminals:** Phishing, corporate fraud, intellectual property disputes, theft, breach of contract and asset recovery are some of the situations wherein computer forensics can be used by criminals.
-  **Readily available data:** Digital evidence stored in one computer is readily available to a miscreant using another computer half a world, and several legal jurisdictions, away.
-  **Knowledge of Legal practitioners:** Legal practitioners involved in the case must also have knowledge of computer forensics. If not, they will not be able to cross examine an expert witness. This also applies to the judge, solicitors and barristers. Computer forensics is still fairly new and some may not understand it.

Recommendations....

A clear road map with a set of milestones should be outlined by Government of India with the ultimate objective of transforming the citizen-government interaction at all levels to the e-Governance mode by 2020. This may be enshrined in a legal framework keeping in consideration the mammoth dimension of the task, the levels of required coordination between the Union and State Governments and the diverse field situations in which it would be implemented.

The legal framework should, inter alia, include provisions regarding:

- Definition of e-Governance, its objectives and role in the Indian context;
- Parliamentary oversight mechanism;
- Mechanism for co-ordination between government organizations at Union and State levels;
- Role, functions and responsibilities of government organizations with regard to e-Governance initiatives, especially business process re-engineering;
- Financial arrangements;
- Specifying the requirements of a strategic control framework for e-Government projects dealing with the statutory and sovereign functions of government;
- Framework for digital security and data protection; and
- Responsibility for selection and adoption of standards and inter-operability framework.

This legislation should have an overarching framework and be able to provide flexibility to organizations.

The way ahead

- ❏ There are many obstacles and challenges to the admissibility of electronic evidence in court.
- ❏ Electronic evidence challenges the traditional rules on the admissibility of evidence, for example, the best evidence rule.
- ❏ New obstacles are created because of the nature of computer technology itself such that it is necessary to re-examine the application of the hearsay rule, or to make evidentiary presumptions for or against the hearsay rule.
- ❏ Besides there is a need for overhauling the entire justice system by adopting E-governance in Judiciary.
- ❏ E-Governance to the judiciary means, use of information and communication technology to smoothen and accelerate case progression to reach its logical end within the set time frame, with complete demystification of the adjudicatory process ensuing transparency. This would perhaps make us closer to the pursuit of truth and justice.

THANK YOU