Digital Forensic Evidence: Legislative and Judicial Policies Developed in Uk, USA and India

Nalini Ambad
Sukdeo Ingale
A) INTRODUCTION:

Development of science and technology has universally benefited the world by providing all comforts and luxuries of life. Undoubtedly, it has given new dimensions to human capabilities and human activities in the present day world. Both, science and technology have contributed to the development of human society. From radio, telephone, television to supercomputers all such Technical Mechanisms are the contributions made by science and technology only.

But one should not forget that the advancement in technology has always brought with it increasing criminal applications and an ever increasing opportunity for committing crime and Internet is no exception to this.

The same fact is also equally true with digital equipments. The development of computer technology has opened new opportunities and possibilities of the perpetration of crime in the field of cyber-world. In reality, the impact of such crimes is so great that it poses a serious threat to personal as well as public security, social and cultural integrity, economic and commercial transactions so on and so forth.

Hence now a day digital evidence is acceptable not only in criminal cases but also in the cases of civil and matrimonial nature. Specially in USA digital evidence has became a very common source of evidence for all type of violent crimes and even for disputes of civil nature like matrimonial disputes. It is to be noted that it may be either crime or dispute of civil nature, whenever there is use of electronic devices like computer, cell phones, ATM machine, iPods, PDAs, thumb drives etc, there has to be commission of some sort of cyber crime. For example in one case [1] a husband, who was fighting with his wife over custody of child, spoofed his wife’s e-
mail address and started sending terrible and threatening messages to himself. He introduces these messages in court as having been received by him from wife and wife lost custody. Wife returns to the court and asks for an order to have husband’s computer forensically examined. Upon examination, it was found that he had set up his “wife’s ID” and tested it once with his computer. Here the forensic evidence helped to give new dimension of cyber crime to matrimonial dispute.

Therefore the use of digital forensic has increased in the past few decades. And the development in science and technology forced judicial systems throughout world to develop ‘Jurisprudence of digital forensic evidence’ by allowing admission of digital evidence extracted from 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, digital video or audio files, iPods, PDAs, thumb drives, CDs, DVD, external hard drives used for backup, old hard drives, voicemail and on and on.

Against this backdrop, the authors would like to through light on the legislative and judicial policies developed in UK, USA and India about Digital Forensic Evidence.

B) MEANING OF DIGITAL FORENSIC EVIDENCE:

According to U.S. Department of Justice \(^2\) ‘electronic evidence’ is information and data of investigative value and that is stored on or transmitted by an electronic device.

According to DFRWS Technical Report \(^3\) digital forensic evidence means- “the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations”
Digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator. [4]

In short, digital evidence forensic includes preservation, identification, extraction, documentation, and interpretation of documentation, and interpretation of computer media for evidentiary and/or root computer media for evidentiary and root cause analysis.

**C) JURISPRUDENCE OF DIGITAL FORENSIC EVIDENCE:**

In every country, police and prosecutors are fashioning a new weapon against criminals, one of it is digital evidence. The sight of hard drives, internet files and e-mails as courtroom evidence is increasingly common. In the wired world, almost every crime intersects with the digital realm at one time or another. In recent past digital evidence has become an indispensable feature of investigation and convictions in most of the criminal cases. The changing world of technology is challenging Legislatures, investigating machinery as well as the courts to keep pace with new laws addressing potential evidence and preserving privacy. In response to these circumstances, following jurisprudence of digital forensic evidence is evolved in UK, USA and India-

**D) LEGISLATIVE POLICIES AND PROCESS IN USA:**

Following are some federal laws dealing with digital evidence in USA [5]:

1) The Electronic Communications Privacy Act of 1986 which prohibits the interception and disclosure of wire and electronic communications, except under order of the Court of Law.

2) The Computer Fraud and Abuse Act 1989 which prohibits a person from accessing a computer without authorization or from exceeding authorized access and thereby obtaining certain governmental, financial or consumer information.

There are a number of State Laws that may also apply to digital forensic evidence. Some of them do and some of them don’t carry a clause excluding the admission of illegally obtained evidence. And where they don’t contain such a
clause, especially at the state level, it is generally held to be at the discretion of the Trial Court whether or not to admit the evidence.

E) LEGISLATIVE POLICIES AND PROCESS IN UK:

In the United Kingdom there is no statutory law available dealing with digital forensic evidence. The examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence. The guidelines consist of four principles:

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

It is to be noted that these guidelines are widely accepted in courts of England and Scotland, but they do not constitute a legal requirement, as there is no enacted Law on this issue, and their use is voluntary.

F) LEGISLATIVE POLICIES AND PROCESS IN INDIA:

In India the Information Technology Act, 2000 is a comprehensive legislation which deals with computer related crimes and provides penalties for such offences. But it has no provision as to evolve jurisprudence of digital forensic evidence. In India the issue of evidentiary aspect of e-document or digital document is tried to be overcome by amendments to Indian Evidence Act, 1872, Indian Penal Code, 1860, The Banker’s Books Evidence Act, 1891 and the Reserve Banks of India Act, 1934.
By such amendments to Indian Evidence Act, the expression ‘Evidence’ (Sec.3) was amendment to include the world ‘the electronic record’ in the category of documents. Section 17 has been amended to include the words ‘oral or documentary or contained in electronic form’. Section 22A, Section 34, Section 35, Section 36, Section 59 was amendment to give authenticity to electronic document as evidence before the court. Section 47-A, Section 65-A, Section 65-B, Section 67-A (mode of proof of the digital signature), Section 73-A, Section 81-A, 85-A, B, C, 88-A, and 90-A were incorporated under the Indian Evidence Act to give evidentiary value to digital signatures and digital records.

Many provisions of the Indian Penal Code were also amended to insert the world ‘electronic record’ to widen scope of existing laws to consider digital record as a document.

**G) JUDICIAL POLICIES AND PROCESS IN USA:**

According to Harley Kozushko, for court of law, the digital forensic evidence is just like any other evidence in the sense that it must be authentic, accurate, complete, convincing to the Court, and in conformity with judicial law and legislative rules about admissibility of evidence.

For that purpose in USA the Supreme Court has evolved ‘Daubert Test’ which needs to consider following issues while deciding admissibility of digital forensic evidence

1. whether the theories and techniques employed while the scientific expert have been tested;
2. whether they have been subjected to peer review and publication;
3. whether the techniques employed by the expert have a known error rate;
4. whether they are subject to standards governing their application; and
5. Whether the theories and techniques employed by the expert enjoy acceptance by other experts.

For any type of evidence, including digital evidence, the evidence must lay the proper foundation because the Courts are concerned with the reliability of such digital evidence. Early court decisions required that authentication is necessary "for a
more comprehensive foundation."[10] As courts became more familiar with digital documents, they backed away from the higher standard and have since held that “computer data compilations… should be treated as any other record.”[11]

A common attack on digital evidence is that digital media can be easily altered. But the Court of Appeals made it clear in 2002 ruled that “the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness”[12]

Very often an opponent to digital evidence objects its admission as hearsay. But authors believe that as like documentary evidence, not all digital evidence is hearsay. First, there is some digital evidence which is not hearsay at all. Hearsay is a “statement, other than one made by the declarant while testifying at the trial… offered in evidence to prove the truth of the matter asserted.”[13] A declarant is a person. On the same line of thought therefore, the courts have declared that digital evidence is not hearsay when it is “the by-product of a machine operation which uses for its input ‘statements’ entered into the machine” and was “was generated solely by the electrical and mechanical operations of the computer and telephone equipment.”[14]

**H) JUDICIAL POLICIES AND PROCESS IN UK:**

In UK most of the evidence presented in the Court is in documentary form. A survey disclosed that not more than 5% cases required use of digital evidence, [15] though the British Law is very helpful. British Courts are also kind enough to grant an ex party order allowing a forensic examiner, accompanied by a solicitor, to go unannounced to a home to image a computer on the spot and sometime to remove it for imaging. The same procedure is applicable for home and workplace. On other hand US courts are showing more concern about individual privacy, free speech right, etc.

**I) JUDICIAL POLICIES AND PROCESS IN INDIA:**

Digital data forensics is relatively new in India. Laws dictating the validity of digital evidence are scattered and not widely known. However, validity is essential to fully prosecute the misuser. Prior to the enactment of Information Technology Act
2000, the TADA Court, Mumbai has treated digital evidence as direct evidence.\(^{[16]}\) The Court observed that the printouts are not copy of the magnetic tape because the tape by itself cannot be termed as a document. Evidence is something which can be perceived by the human senses. Hence which can not be perceived by a Judge cannot fall within the definition of the word ‘evidence’ or ‘document’. The printouts, on the other hand constitute direct evidence of the matter on magnetic tape.

On the other hand the SC has taken different stand on this issue in State (NCT of Delhi) v. Navjot Sandhu, SAR Gilani & Ors.\(^{[17]}\) The SC held that printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service providing Company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts based on his personal knowledge. The SC further held that irrespective of the compliance of the requirements of Section 65B (which is a provision dealing with admissibility of electronic records), there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely Sections 63 and 65.

Till today the law on digital evidence is not well settled and widely accepted in India. Recently Delhi High Court, while dealing with nature if the digital evidence held that \(^{[18]}\) when certain data (i.e. call records) were copied from Hard Disk to a CD and 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 CD can be admitted as true copy of original evidence.

**J) SUGGESTIONS:**

1. Country or region specific ‘uniform laws’ are necessary. Today different countries have different laws and regulations. Hence crime committed from different territory becomes difficult to investigate.
2. The first thing you need to do, when you suspect of cyber crime is -Not to allow any one (even any departmental expert from IT section of Institution or your friend) to look into computer to find out whether there is any useful evidence in your device. Do not try to copy the data. To preserve the digital evidence properly, if it computer, you must pull the plug without orderly shutting down. And
if it is server then only you need to shut down it orderly to preserve evidence
properly. File FIR and call certified expert to collect data.

3. Digital forensic evidence should be accepted as if any other document and there
is no need to treat it differently unless and until facts and circumstances of the
case demand so.

4. There is need of evolving different tools and techniques to preserve and collect
digital data so that more authentic and unobjectionable digital forensic evidence
can be extracted.

5. The ways of extracting evidence should be made public so that people will
understand that every activity of them can be traced and tracked easily. Most of
the time cyber crimes are committed under presumption that no one can find out
what criminal has done online. When people will understand that they can be
traced, then most of the people will change their mind due to fear of criminal law.

REFERENCES:

Spyware, Avatars, and Cybersex,” Available at: http://www.senseient.com
/storage/articles/Spyware_Avatars_and_Cybersex.pdf, (Visited on 06/12/2013).

First Responders”, Available at: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf,
(Visited on 1/12/2013).

Map for Digital Forensic Research”, August 7-8, 2001, Utica, New York,
Available at: http://www.dfrws.org/2001/dfrws-rm-final.pdf, (Visited on
6/12/2013).

Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf, (Visited on
7/12/2013).

Avatars, Cybersex and Hottie Honeypots”, Available at http://www.senseient.

(Visited on 5/12/2013).


[8] Supra, n.4.


