A. INTRODUCTION

The rapid development of information and communication technologies over the past decade has revolutionized both business and individual practices.\(^1\) The worldwide explosion of electronic commerce and the developments in the computer and telecommunications sectors are deeply changing the delivery and availability of information, acts, transactions and services.

The proliferation of computers has created a number of problems for the law. Many legal rules assume the existence of paper records, of signed records, of original records. The law of evidence traditionally relies on paper records as well, though of course oral testimony and other kinds of physical objects have always been part of our courtrooms, too. As more and more activities are carried out by electronic means, it becomes more and more important that evidence of these activities be available to demonstrate the legal rights that flow from them.

Most electronic records are, in practice, being admitted in litigation.\(^2\) However, courts have struggled with the traditional rules of evidence, with inconsistent results. The common term “reliability” has caused confusion between the principles of authentication, best evidence, hearsay and weight.

What is worse, many record managers and their legal advisers have not been confident that modern information systems, especially electronic imaging with the paper originals destroyed, will produce records suitable for use in court.

For this reason, there has been a growing demand from industry and users for new types of signature, to effectively substitute the hand-written signature in the electronic environment, granting integrity, confidentiality and authenticity of information and documents.


\(^2\)Litigation based on computer records has been extensive in countries like the United States, Canada, Japan, UK, etc., where the establishment of facts depends entirely on computer generated evidence. In India too, electronic records have been dealt with, albeit not comprehensively. In this context, see Section 610 A, Companies Act, 1956 (Admissibility of micro-films, facsimile copies of documents, computer print-outs and documents on computer media as documents and as evidence) which was inserted by the Companies (Amendment) Act, 1996.
The legal regime envisaged should not view the Internet and electronic records in a negative manner. The legal environment must aim at facilitating the use of such technologies to best serve society. The focus must be on weeding out the undesirable while simultaneously encouraging and facilitating the spread and use of technology. With specific reference to evidence, following are considerations to be borne in mind when legislating:

i. the nature of the threshold that should apply to the admissibility of electronic evidence;

ii. the burden of proof on the proponent or opponent of the evidence; and

iii. the procedural requirements to ensure a proper examination of electronic evidence adduced before the court.

The system so devised must be broad to encompass technologies past, present and future.³

The computer software plays a vital role in modern technology and communication system. In a recent case, the Supreme Court observed that the computer software is a term used to describe programmes that cause a computer to operate in a particular way. The other non-hardware parts of a computer system such as manuals are, sometimes, regarded as software.⁴

B. INFORMATION SYSTEM

The definition of “Information System” is intended to cover the entire range of technical means used for transmitting, receiving and storing information. The UNCITRAL Model Law does not address the question of whether the information system is located on the premises of the addressee or on other premises, since location of information system is not an operative criterion under the Model Law.

C. EVIDENTIARY REGIME AND THE INTERNET

Almost all evidence to prove facts in litigation involving the Internet will be computer-generated. This is primarily because technology today only allows for

³ For example, legislations in the UK and US of the 1970s and 80s were intended to be comprehensively covering all technologies, but the advent of the Internet has shown there to be serious inadequacies in the legal regime and development and spread of technology. Technology will grow as long as there be a use for it, and the spread of technology will depend on the kind of legal coverage or insurance the users of such technologies will posses.

⁴ Sheela v. Presiding Officer, 1st Additional Labour Court, Chennai, (2001) 4 SCC 634
Internet usage through computers. The “computer” means “any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a compute system or computer network.”

The Indian Evidence Act, 1872 does not define a computer, but allows for “copies” to be made by “mechanical processes” or through uniformly “printing”. References to “computer” and “media” are also made as regards evidence in the Companies Act, 1956. Unlike the U.K., for the purposes of the Companies Act, it is not necessary for the computer to be working properly. The only mechanical device that needs to be checked for functional problems are the media such data are stored in. In the United Kingdom, it is necessary to prove the computer was working properly before adducing computer-generated evidence.

This gives rise to the first problem as regards Internet-based evidence. For example, X in an E-mail to Y confirms that he accepts Y’s offer, thereby concluding a contract. Y accesses his E-mail account and directly downloads X’s e-mail onto a diskette. The E-mail does not pass through the Computer Y is using, but a virus piggybacks onto the file while saving is occurring and, thereby, changes the content of the E-mail. Now, all that has to be proved to admit this tampered E-mail (for the

---

5 However, technology is fast embracing mobile technology, where users can access the Internet, use E-mail, send and receive faxes, etc. by mobile phones through the Wireless Application Protocol (WAP). Also, a mushrooming industry is Internet service through television and cable companies. Either way, all these modes of communication involve processing the transaction through a mechanical device.

6 The Information Technology Act, 2000; Section 2 (1) (i)

7 The Indian Evidence Act, 1872; Section 63(2)

8 Ibid., Section 62, Explanation 2

9 The Companies Act, 1956; Section 610 A

10 The Civil Evidence Act, 1968; Section 69

11 In this context, see Bech-Bruun & Trolle, “When has an E-mail `reached the addressee?'”, 3rd June, 1999, Denmark, at http://www.internationallawoffice.com/lettersdetail.cfm?Newsletters_Ref=615

12 This is not a very hard thing for hackers to do. They merely write a code that activates itself when Y downloads (saves) E-mails. This code is referred to as a worm and lies dormant till called into operation by an ancillary act, in this case, Y saving his E-Mail. Now what this code does is activate another code that piggy-backs itself by writing itself into the data stream and merging with the already logically flowing data onto the disk. Once carrying this piggy-back, the code can insert itself into the file contents and tamper or alter the data so contained on the disk.
purposes of the Companies Act), is that the diskette (media on which the data was stored) was functioning properly.\textsuperscript{13}

Though this sort of situation is highly improbable, and maybe it will never occur, it does highlight that there is a difficulty in using the term ‘media’ when the purpose was to include ‘computer’. If the Act required computers to be scanned, the tampered E-mail would not be admitted. Thus, it is better to be clear as to what a computer is, and this should be expressly and clearly used and defined. It is also necessary to harmonize the principles in the various laws such as the Evidence Act and the Companies Act after the enactment of the IT Act and the resultant changes in the legal system. This will pre-empt much confusion that is likely to reign. For example, one might ask which provision between section 610 A of the Companies Act and section 65 B of the Evidence Act (brought in through amendment by the IT Act) would apply to a particular situation?

\textbf{D. \quad \textsc{Types of Computer-generated Evidence}}

Computer-generated documentary evidence will be of following 3 types:

\textbf{1. \quad \textsc{Real Evidence}}

The calculations or analyses that are generated by the computer itself through the running of software and the receipt of information from other devices such as built-in-clocks and remote sensors. This type of evidence is termed as real evidence.\textsuperscript{14} Real evidence arises in many circumstances. For e.g. If a bank computer automatically calculated the bank charges due from a customer based upon its tariff, the transactions on the account and the daily cleared credit balance, this calculation would be a piece of real evidence.\textsuperscript{15}

\textbf{2. \quad \textsc{Hearsay Evidence}}

There are the documents and records produced by the computer that are copies of information supplied to the computer by human beings. This material is treated as

\textsuperscript{13} Since the damaging code has written into the file directly, it does not affect the diskette itself, and does not show up on a scan of the disk.

\textsuperscript{14} Real evidence is defined as evidence of a tangible nature from which the tribunal of fact can derive information by using its own senses. (Source: Peter Murphy, \textit{A Practical Approach to Evidence}, 1988, Blackstone Press, London, p. 186). Real evidence has been described as the most satisfactory kind of evidence since, save for identity or explanation, neither testimony nor inference is relied upon. Unless its genuineness is in doubt, the thing speaks for itself. See M.N. Howard (Ed.), \textit{Phipson on Evidence}, 1990, Sweet & Maxwell, London, p.3.

\textsuperscript{15} Other examples of real evidence include voice spectography and DNA evidence.
hearsay evidence. For e.g. Cheques drawn and paying-in slips credited to a bank account are hearsay evidence.

3. **Derived Evidence**

   It is information that combines real evidence with the information supplied to the computer by human beings to form a composite record. This, too, is usually treated as hearsay evidence. For e.g. Figure in the daily balance column of a bank statement since this is derived from real evidence (automatically generated bank charges) and hearsay evidence (individual cheque and paying-in entries).

E. **VIDEO-CONFERENCING AND EVIDENCE**

   Recording of evidence by video-conferencing also satisfies the object of the Evidence Act that the evidence be recorded in the presence of the accused.\(^\text{16}\) The accused and his pleader can see the witness as clearly as if the witness was actually sitting before them. In fact, the accused may be able to see the witness better than he may have been able to do, if he was sitting in the dock in a crowded court-room. They can observe his or her demeanour. In fact the facility to play-back would enable better observation of demeanour. They can hear and rehear the deposition of the witness. The accused would be able to instruct his pleader immediately and thus cross-examination of the witness is effective. The facility of play-back would give an added advantage whilst cross-examining the witness. The witness can be confronted with documents or other material or statement in the same manner as if he/she was in court. Thus, no prejudice of whatsoever nature is likely to be caused to the accused.\(^\text{17}\)

   In *Delhi Serial Blasts Case*, the Delhi court has issued notice to jail authorities in Gujarat and Maharashtra where the Delhi serial bombing accused are lodged so that court proceedings could be conducted through video-conferencing to avoid delay in shifting them.\(^\text{18}\)

   Taking into consideration the security lapses which occur when undertrials have to be shunned between the court and jail during case hearings, courts have formulated the perfect means of taking case of any faults which may occur during this process. Thus, linking of courts through video-conferencing is started with the

---

\(^\text{16}\) The Evidence Act, 1872; Section 273

\(^\text{17}\) *State of Maharashtra v. Dr. Praful B. Desai*, (2003) 4 SCC 601

\(^\text{18}\) “Notice on Trial through Video-conferencing”, *Times of India*, August 9, 2009, p. 6
purpose of saving time and money and also to facilitate the security of prisoners. The video linkage systems will drastically bring down the number of police personnel deployed on escort duty. The surplus staff could be used for other duties. The prospects of escape during transportation to and from the courts could be bleak as the number of prisoners would be manageable.19

F. ADMISSION

Since computer generated evidence is a recent development, Indian law has not addressed the issue yet. Thus, even though the focus is on the Indian Evidence Act, positions in the U.K. and U.S are also looked into. References to the UNCITRAL Model Law on Electronic Commerce20 are also made.

Advance of science and technology is such, that now it is possible to set up video-conferencing equipment in the court itself. In that case, evidence would be recorded by Magistrate or under his dictation in open court. If that is done, then the requirements of Cr.P.C., 1973 that evidence be taken down in writing by the Magistrate himself or by his dictation in open court would be fully met.21 To this method, there is, however, a drawback. As the witness is not in court, there may be difficulties if he commits contempt of court or perjuries himself and it is immediately noticed that he has perjured himself. Therefore, as a matter of procedure, evidence by video-conferencing in open court should be taken only if the witness is in a country which has an extradition treaty with India and under whose laws contempt of court and perjury are also punishable.22

G. NATURE OF THRESHOLD REQUIREMENT

1. Certification

There is no express threshold requirement for computer-generated evidence to be adduced before an Indian court of law.23 In contrast, the United Kingdom treats

20 Available at http://www.uncitral.org/english/texts/electcom/ml-ec.htm
21 The Code of Criminal Procedure, 1973; Sections 274 and 275
23 This is in reference to the Indian Evidence Act, 1872 which, de facto, contains the rules as to evidence before Indian courts. However, section 610 A of the Companies Act, 1956 does lay down 3 pre-conditions to be satisfied before adducing such evidence, but it is solely for the purposes of Companies Act and litigation commencing therein. As regards the general rules of evidence, there is no formal requirement to be fulfilled.
computer-generated evidence differently from other evidence. It is trusted less and requires a certificate as to the authenticity of the evidence. Like the Police and Criminal Act, 1984 in England, the Indian Companies Act, 1956\textsuperscript{24} requires the media on which the data is stored to be “scanned” and “authenticated” by the Registrar. These certification requirements raise problems as regards Internet-based evidence and special rules of this nature will hamper the encouragement and growth of e-commerce in India.

Like the Indian Companies Act, 1956 and the U.K. Civil Evidence Act, 1968, the section 69 of the U.K. Police and Criminal Evidence Act, 1984, will only admit computer evidence if it satisfies following 2 tests:

i. there must be no reasonable ground for believing that the statement is inaccurate because of improper misuse of the computer.\textsuperscript{25}

ii. the computer must have been operating properly at all material times or at least the part that was not operating properly must not have affected the production of the document or the accuracy of the contents.\textsuperscript{26}

In \textit{R. v. Shephard},\textsuperscript{27} the accused was alleged to have shoplifted from Marks and Spencer stone in London. She contended that she had thrown her receipt away. The prosecution relied upon the store’s central computer system’s records. Thus, the question before the House of Lords was whether this evidence should satisfy the requirements of section 69 of the 1984 Act. Lord Griffiths made the following statement:\textsuperscript{28} “If the prosecution wishes to rely upon a document produced by a computer, they must comply with section 69 in all cases.”

Section 69 poses a negative requirement that, unless the evidence sought to be adduced meets the criteria, it is inadmissible. It is a powerful tool to ensure that both prosecution and defence rely only on approximately reliable evidence. A critical

\textsuperscript{24} The Indian Companies Act, 1956; Section 610 A
\textsuperscript{25} The U.K. Police and Criminal Evidence Act, 1984; Section 69 (1) (a)
\textsuperscript{26} \textit{Ibid.}, Section 69 (1) (b)
\textsuperscript{27} \textit{R. v. Shephard}, (1993) 1 All ER 225
\textsuperscript{28} \textit{Id} at p. 230. However, this statement is not absolutely correct. Some computer evidence may be adduced not for any fact therein, but as an actual fact. For e.g. a bank statement showing an entry of X sum of money into a bank account. This evidence is not a statement that the account is credited, rather the fact. U.K. Courts have admitted evidence which is alleged to have been modified without clearing the section 69 hurdle. See Collin Manchester, “Computer Pornography”, (1983) \textit{Crim. LR} 472; DPP V. McKeown, (1997) 1 WLR 295. In all the above circumstances, the code was adduced not as evidence of the fact therein, but as the fact itself.
analysis of the types of evidence used in a digital case reveals that there will be little evidence that will not be required to meet the requirements of this section. The evidence may include logs stored on the client’s, host’s, victim’s, or accused’s computers. It will also possibly include data or programmes to which the prosecution alleges the defendant gained access. In such circumstances, the prosecution may, unwisely, rely on ‘date-stamps’. As the name suggests, these dates show the last time that a computer file was modified or even viewed. These date-stamps may appear useful to the prosecution to show the exact time and date when, say, a programme was infected with a virus. The evidential difficulty with these stamps is that they are notoriously unreliable and this can be challenged by the defence.

2. Problems with Certification and Internet-based evidence

As stated earlier, there are 3 kinds of evidence generated from computers: real, hearsay and derived. Prior to this judgment, real evidence was not subject to such statutory scrutiny, and was rendered admissible and with good reason too. It is submitted that this distinction should be maintained. Otherwise, when applied to Internet evidence, it would be almost impossible to admit computer evidence. Thus, the principle that should be applied is: if the instrument is one of a kind which, to common knowledge, are more often than not in working order, then, in the absence of evidence to the contrary, the Courts should presume that the machine was in working order at the material time.

The problem with certification, as posed by Internet evidence, can be broadly brought under 2 heads:

i. Continuity of Access Evidence

A look at the technical aspect of how the Internet is used as a medium of communication demonstrates the inherent difficulty of applying a strict rule of positive certification. Messages over the Internet split into “data packet” and travel

30 Recordings from automatic recording devices were accepted as real evidence in England as early as 1968. The Statute of Liberty, [1968]1 W.L.R. 739, case turned on a record of radar recordings showing the location of two ships involved in a collision. The recording was made by a technical device without human intervention. Simon P., J. held such recording to be admissible as real evidence. He cited R. v. Maqsood Ali, [1966] 1 QB 688
31 This effectively transfers the burden of proof that the machine was ‘not’ working properly onto the defendant.
individually, through different routes, from computer at origin to computer at destination. In demonstrative terms, an E-mail does not go from A to B in entirety, but in a number of parts, which reconstruct themselves at their destination (B). It is also a technological fact that a computer does not receive a message and send it on its way. In fact, every time a data packet passes through a computer over the Internet during its journey, the computer copies the data packet into its domain, and then sends this “new” copy.

Apart from the certification implications, to prove beyond reasonable doubt, that the defendant was responsible for unauthorized access to the victim’s computer, the prosecution can be forced to prove continuity of evidence. That is, the prosecution should be able to follow or trace a line of access from the hacker’s own computer to the victim’s. Any discontinuity may raise the court’s reasonable doubt that the defendant in the court was not the person responsible for the final unauthorized access. In cases of hacking, it is also well-known that hackers rarely attempt to gain access to their victim’s computer directly. Instead, their preferred method is to login to one computer on the Internet and from there login to another and so on. This process is repeated many times. And each new login made by the hacker presents another piece of evidence that the prosecution may have to prove to establish continuity from the first to the final unauthorized access.32

ii. False Identification – Spoofing

A hacker logging into a computer on the way to his victim will often login under a different identity. This is called “spoofing”. The hacker is able to do this by having previously obtained actual passwords, or having created a new identity by fooling the computer into thinking he is the system’s operator.33 Whatever the technical method, the legal result remains the same. The prosecution must establish that the hacker at his own computer was the person who has logged into countless other computers.

The evidential implications are manifold. The prosecution will be required to obtain multiple certificates, because of the gravity of the computer’s reliability. Each certificate must adequately verify the proper workings of the computer, and is,

32 R. v. Cochrane, [1993] Crim L.R. 48, illustrates the utility of focusing on one computer in a chain to ‘break’ the continuity.
33 See “Hackers : Who they are and How they operate”, at http://www.543.77.com/welcome.htm
therefore, potentially, a weak link in the continuity chain.\textsuperscript{34} The computes, which a hacker may journey through to finally arrive at the victim’s computer, will be scattered throughout the world. There is one cost of accessing any computer on the Internet: there are no financial restraints on crossing borders and continents. This will require certification from multiple jurisdictions.\textsuperscript{35}

A hacker will not only spoof his identity, but also attempt to tamper with the logging software actually used by the system. This poses following 2 problems:

i. technically it may be impossible to prove that the defendant in the court was the hacker modifying the log.

ii. to admit that the log has been tampered at all raises suspicions that the computer was not operating properly at the material time.\textsuperscript{36}

Any admission by the prosecution of tampering should be met by the defence with a question as to whether the evidence still deserves a certificate, or that the operator be orally examined.

Thus, there are inherent problems with applying the certification rule in the context of Internet-evidence, and this would hamper the development of E-commerce and the spread of Internet usage if applied, as the proponent of the case would be required to adduce an almost impossible pore-condition, which in itself, may be very shaky evidence.\textsuperscript{37} There is no justification for imposing the evidential burden on the proponent of Internet evidence, if the public-policy aim is to facilitate the use of such kind of evidence. The threshold requirements to Internet evidence should be the general tests of relevancy, as outlined in the Indian Evidence Act.\textsuperscript{38}

\textbf{H. \quad BURDEN OF PROOF}

The need for having a check on computer-generated evidence is due to the fact that computers are machines, unreliable, and unavailable for cross-examination in court. Thus, till now, the burden of satisfying the computer operation requirement rested on the proponent of such evidence. As already discussed, there are difficulties


\textsuperscript{35}This raises the twin issues of: (1) procuring the certificates, which itself will be almost impossible; and (2) recognizing the validity of an international certificate.

\textsuperscript{36}\textit{DPP v. McKeown}, [1997] 1 W.L.R.295

\textsuperscript{37}\textit{East-West Transport v. DPP}, (1995) Crim L.R. 642-643, where machine print-out was admitted even though there was no evidence to show that the machine was working properly.

\textsuperscript{38}The Indian Evidence Act, 1872; Sections 6-55
with certification as regards Internet-evidence. The method of communication imposes an almost impossible requirement of the proponent. If the aim of the evidential regime is to facilitate the spread of Internet usage, and allied technologies, such a requirement would hamper these efforts. Thus, the burden of proving the malfunction of a computer should lie with the defence. Further, it must be kept in mind that the malfunction must be affecting the data sought to be adduced. If there are other malfunctions, which do not affect the data adduced, they should be rendered irrelevant. However, a balanced approach (to ensure that computer-generated records are not abused because of the strong evidential presumption), could be laid down that ‘if the defence proves the existence of a malfunction in the computer in question, it should be up to the prosecution to prove that such malfunction did not affect the data sought to be adduced.’

This approach envisages a reversing of the presumption contingent on a demonstrated objection by the defence. This would balance out the problem with computer generated evidence as regards the Internet and would ensure that the evidence adduced is reliable and not prejudicial to either party. This would impose a reasonable and balanced check on the admissibility of Internet and computer evidence.

However, this framework does not envisage the unfettered admission of Internet-based, computer-generated evidence. It merely provides an umbrella to the recognition of an electronic record as not being valid solely on the ground of it being in electronic format. This framework provides a method of adducing and objecting to electronic records on substantial grounds, and not merely because of the format of the record. It does not provide an unnecessary burden on either party, and ensures that the evidence sought to be adduced is reliable and authentic. The discretion as to proof of objections (how the parties would prove their objections to be valid and true) should rest with the court.\textsuperscript{39}

\textsuperscript{39} The court should be given discretion as to whether the objections as to malfunctions and relevancy thereof (imposed on opponent and proponent respectively) should be proved by oral, documentary, real, demonstrative or any other kind of evidence. In this context see G v. DPP, (1997) 2 All ER 755, where the court held that it has the discretion and entitlement to admit expert testimony as to whether video-testimony should be admitted. This discretion should be given because any hard and fast rule regarding proving of objections in the context of advancing technology would not be technology neutral and would prejudice the legal rights flowing out of such technology.
The international consensus emerging is that an electronic record is not to be denied validity on the sole ground that it is electronic in format.40

I. ADMISSION OF ELECTRONIC RECORD

The UNCITRAL Model Law on Electronic Commerce (1996)41 deals with the admissibility and evidentiary weight of data messages.42 In any legal proceeding, the rules of evidence should not apply to exclude a data message, either, solely because it is a data message (electronic in format)43 or, if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.44

The Enactment guide45, as regards Article 9 states: “The purpose…of Article 9 (1) is to establish that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form, puts emphasis on the general principle stated in Article 446 and is needed to make it expressly applicable to admissibility of evidence, an area in which particularly complex issues might arise in certain jurisdictions.”

The Indian IT Act lays down a blanket permission for records not to be denied legal effect if they are in electronic format, as long as they are accessible for future reference. The Act amends the definition of ‘evidence’ to include “all documents including electronic records produced for the inspection of the court.”47

Further, the IT Act provides that “where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

40 UNCITRAL Model Law ; Article 9
42 Supra note 40, Article 9 (1) deals with admissibility, while paragraph (2) of the same Article deals with evidential weight of data messages
43 Ibid., Article 9 (1) (a)
44 Ibid., Article 9 (1) (b)
46 Supra note 40, Article 4 lays down the principle that development of the Model Law should be through contracts, not legislation. This is because the subject of the law is so dynamic in nature that it is imperative to allow development within a framework. This is termed as the principle of “part autonomy”, the essence of Article 4.
47 Indian Evidence Act, 1872; Section 3
(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference.”

It also describes the manner in which the electronic document is to be proved in law.

The principle of not excluding evidence solely on the ground of its form is fundamental to the encouragement of the use of Internet and communications technologies. It also allows for flexibility in the case of the danger of tampering of an electronic record. It resolves the conflict of encouragement of transacting in this medium and safeguarding against the abuse of technologies to mislead the court.

J. DOCUMENT

Computer-generated evidence has been treated as “documents” in England and other common law jurisdictions. In India, the term ”Document” is defined to include “any matter written, expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means which is intended to be used, or which may be used for the purpose of recording that matter.”

Information on computer media is stored as bits and bytes, the electronic equivalent of zeros and ones. Now it may be argued that these zeros and ones are expressions on the computer disc in the form of a figure or mark, thereby classifying electronic records as document under Indian Law. The IT Act settles this issue very simply, by mandating that, subject to exceptions that legislators provide for, the legal requirement of writing and consequently of documents will be satisfied by electronic records.

K. EVIDENTIARY DOCUMENT

1. Indian Law

The Indian Evidence Act, 1872, when compared with the General Clauses Act, 1897, excludes the word “written” from its definition of “document”. The focus of

---

48 The Information Technology Act, 2000; Section 4
49 Section 65 A and section 65 B of the Indian Evidence Act, introduced by the IT Act, 2000 amending provisions
51 The General Clauses Act, 1897; Section 3(18)
52 Supra note 47, Section 3 defines “document” to include any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.
this statute is on the purpose the document is to be used for, i.e. recording the matter. The laws of interpretation indicate that when a statute specifically excludes, that definition overrides any general definition, in this case, the General Clauses Act. Bits and bytes are comparable to zeros and ones, which in turn are equated with letters and marks. It can further be contended that since the purpose of bits and bytes are to record information, they can be included in this definition.

The Evidence Act further state that, with some limited exception, when the contents of a document are to be proved, the document itself has to be adduced and copies of it shall not be admissible. Electronic records raise the question of what is an original. If being adduced as original, the electronic document itself has to be examined by the trier. The only way to examine an electronic document is by displaying it on a secondary device, either a screen or a printout. It is a tenable argument that such display is not original, but amounts to a copy, and is, therefore, inadmissible as evidence. Indian law does not resolve this issue.

An alternative route could be using the evidence for corroborative purposes. Oral evidence can be introduced if it relates to a relevant fact. Further, if the oral evidence refers to the existence or condition of any material thing other than a document, the court may require the production of such material thing for inspection. Thus, if oral evidence as to the existence of a contract is adduced, then computer evidence may become admissible as it can be termed a material thing. Therefore, computer evidence may be allowed to corroborate the oral evidence extended. Indian courts have allowed tape recordings to be admissible in this manner.

It has been long accepted that photographs constitute a document. It has also been held that data can be said to constitute a photograph. Thus, A=B; B=C, and

---

53 Ibid., Section 64
54 Ibid., Section 59
55 Ibid., second proviso to section 60
56 M.P. Verma v. Surinder Kaur, AIR 1982 SC 1043
57 Z.B. Bukhari v. B.R. Mehra, AIR 1975 SC 1788, which held, “tape recordings stand on the same footing as photographs and are documents per section 3 of the Evidence Act.”
58 R. v. Fellows; R. v. Arnold, (1997) 2 All ER 548 (557) where Evans, J., held “...We conclude that there is no restriction on the nature of the copy, and that the data represents the original photograph, in another form.”
therefore, A=C. This is one further argument to bring electronic records within the ambit of the definition of “document”.

2. The UNCITRAL Model Law

The Model law mandates that if there is a legal requirement of an original, this requirement will be met by a data message if it satisfies the following two tests: 59

i. there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

ii. where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

Digital signatures can also be used to ensure the integrity of messages or information. 60 The Model law states that information in the form of a data message shall be given due evidential weight, after considering the reliability of the manner in which the data message was generated, stored or communicated, reliability of the manner in which the integrity of the information was maintained, the manner in which the originator was identified, and any other relevant factor. 61

3. The Information Technology Act, 2000

The IT Act, through its amending section, brings in a new section into the Indian Evidence Act which reads as under:

Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be also a document and shall be admissible in any proceedings, without 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. 62

The conditions referred above in respect of a computer output shall be following:

---

59 Supra note 40, Article 13
60 Ibid., Article 8 (1) (a), (b)
61 Ibid., Article 9 (2)
62 Supra note 47, Section 65 B (1)
63 Ibid., Section 65 B (2)
(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.

Thus, an electronic document can for all practical purposes have the same legal effect as a paper based original document.

I. **WRITING**

Documents are required to be in written form for primarily following 2 reasons:

i. to give the document a formal validity, and

ii. to be made admissible as evidence in court.

1. **Indian Law**

There are a number of enactments in India requiring documents to be written.

The question that arises with respect to online transactions is: Will a document generated by a computer satisfy this requirement of writing?

The General Clauses Act mandates that expressions referring to “writing” shall be read to include references to printing, lithography, photography and other modes of representing or reproducing words in a visible form. Thus, any information conveyed in any kind of the visible format would satisfy the requirement of writing. Computer information can be viewed either on a screen or printout. It is,

---

64 The General Clauses Act; Section 3 (65)
thus, tenable to contend that information keyed into a computer, as long as it can be viewed, would amount to writing. The confusion arises when the computer is turned off, making the information no longer visible. These soft copies would, since they are not visible, not amount to writing. Printouts, however, may be regarded as writing. As of today, it is unclear whether this interpretation is valid or not.

If material keyed into computers were allowed to satisfy the requirement of writing, then the position would become clear. This should be allowed in all cases unless the government decides otherwise.

2. **The UNCITRAL Model Law**

The Model law states that where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.\(^{65}\) This applies whether the requirement is in the form of an obligation or whether the law simply provides consequences if it is not in writing.\(^{66}\) This shall not apply in such cases where the government of each State feels that it should not apply.\(^{67}\)

3. **The Information Technology Act, 2000**

The IT Act states that where a law requires information to be written or to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule if the information contained therein is accessible so as to be usable for subsequent reference.\(^{68}\)

Thus, an electronic record should be admissible, be interpreted to constitute a document, and the data comprising the record should be taken to be a writing.

M. **RULE AGAINST HEARSAY**

The rule against hearsay is an important evidential tool in common law countries, and has been often used to exclude a large amount of evidence. “Evidence

---

\(^{65}\) *Supra note* 40, Article 6(1)

\(^{66}\) *Ibid.*, Article 6(2)

\(^{67}\) *Ibid.*, Article 6(3)

\(^{68}\) The Information Technology Act, 2000; Section 4(b)
from any witness which consists of what another person stated (whether verbally, in writing, or by any other method of assertion such as a gesture) on any prior occasion is inadmissible, if its only relevant purpose is to prove that any fact so stated by that person on that prior occasion is true. Such a statement may, however, be admitted for any relevant purpose other than proving the truth of facts stated in it.”69 This principle has been recognized and accepted by the US, UK, Canada and India, all characterized by the common law, adversarial systems of law. The rationale for barring hearsay evidence from trial stresses the importance of cross-examination. An out-of-court statement offered to establish the truth of a matter at bar effectively precludes its opponent from confronting and questioning its declarant to expose the statement’s weaknesses.70 Weaknesses within a hearsay statement may include defects in the declarant’s perception; defects in the declarant’s memory; lack of the declarant’s sincerity or veracity; and defects in the declarant’s narration or transmission of the statement.71 The underlying assumption of the hearsay rule is, therefore, that the untested nature of such evidence justifies its exclusion.72

The emphasis of this doctrine should be on guarding the trier from being misled, though the interpretation seems to stress protection not of the trier, but of his adversary.73 The question that arises in the context of electronic documents74 is that: Since the document is subject to traceless tampering (because of electronic format) and does not state the truth of the matter contained therein, should not the rule against hearsay apply, and thus exclude the admissibility of electronic documents?

Litigants in complex commercial litigation and parties in criminal cases must rely on computer records or printouts to prove that a particular event or circumstances occurred. A computer printout has been considered an out-of-court statement, and

---

71 Id. at p. 182
72 Id. at p. 183
74 It is not a matter of contention that documents too attract the hearsay rule. In this context see Myers v. DPP, [1964] 2 All ER 881, where a companies business records were treated as hearsay; R v. Patel, [1981] 3 All ER 94, where the Immigration Records at the Home Office were treated as hearsay; Laksmi Raj Shetty v. State of Tamil Nadu, AIR 1988 SC 1274, where the Indian Supreme Court held newspaper reports to be hearsay evidence.
when the printout is offered in court for the truth of what it asserts, it is deemed to be hearsay.75 The admissibility of a computer printout or record will, therefore, depend on whether it fits under any of the numerous exceptions to the hearsay rule.

1. **United States**

The rule against hearsay evidence has been called “that most characteristic rule of the Anglo-American Law of Evidence – a rule which may be esteemed, next to jury trial, the greatest contribution of that eminently practical legal system to the world’s methods of procedure.”76

As defined by the Federal Rules of Evidence, ‘hearsay’ is “a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.”77

A ‘statement’ for purposes of hearsay is defined as, “an oral or written assertion, or non-verbal conduct of a person, if it is intended by the person as an assertion.”78

The Americans have had a history admitting computer-generated evidence as an exception to the hearsay rule.79 The Federal Rules prescribe certain exceptions to the hearsay rule.80 Thus, if it can be proved that the evidence sought to be adduced falls under an exception, it can be made admissible. The most relevant exception in the case of E-Commerce is the Records of Regularly Conducted Business Activity.81

Yet, there are practical differences between manually maintained business records and those kept on a computer. Some doubt exist as to whether the aforementioned

---

77 Fed. R. Evid. 801 (c )
78 Fed. R. Evid. 801 (a)
80 Art. VIII (Hearsay). Rule 803 (Hearsay Exceptions)
81 Fed. R. Evid. 803 (6); See Rosenberg  v. Collins, 624 F. 2d 659, 665 (5th Cir. 1980)
statutory criterion will ensure computer record’s trustworthiness as evidence.\footnote{\textsuperscript{82} See “Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence”, 1977, \textit{Wash U.L.Q.} 59 (73); See also, “Discovery and Use of Computerized Information: An Examination of Current Approaches”, 13 \textit{Pepperdine L. Rev}. 405 (414) (1986), at http://www.law.ppdine.edu/Rev/archives/compo/1986/M-405.html} Because computerized records and other documents are stored on magnetic disks, tapes and punched cards, the data they contain is often indecipherable to the human operator without a computer-produced copy on paper.\footnote{\textsuperscript{83} Ibid.} To this end, the court may order that a computer printout be furnished.\footnote{\textsuperscript{84} Fed. R. Civ. P. 34; See also Westinghouse Electric supply Co. v. B.L. Allen, Inc. 183 Vt. 84, 413 A.2d 122 (1980)} The resulting uncertainty surrounding the admissibility of such a printout stems from the nature of its storage and retrieval. The foundational requirements for the business records exception as regards computer records are as follows:

(i). computer printouts may be altered more easily than traditional handwritten records since false information can readily be entered in the computer’s memory.\footnote{\textsuperscript{85} Mills, Lincoln & Langhead, “Computer Output – Its Admissibility into Evidence”, 3 \textit{Law & Computer Tech} 14 (17) (1970)} A possible pitfall in analyzing computerized business records is that the investigation may be limited to the computer and software themselves; the environs of the computer – such as the manual practices employed for inputting the data – may be neglected. The “regularity/business” statutory provision cannot ensure that the computer’s database and it’s printout have not been falsified unless the court imposes specially-developed foundational tests for tampering or orders a review of the computer input procedures.

(ii). once computer tampering has occurred, it is not always possible to follow a “paper trail” to the source. Because a computerized record-keeping system involves minimal human participation and produces no immediate records, a party may falsify it’s own records and leave few traces of its activity.\footnote{\textsuperscript{86} See “Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence”, 1977 \textit{Wash. U.L.Q.} 59 (79) (1977); See also Roberts, “A Practitioner’s Primer on Computer-Generated Evidence”, 41 \textit{U. Chi. L. Rev}. 254 (272-278) (1974); Peritz, “Computer Data and Reliability: A Call for Authentication of Business Records under the Federal Rules of Evidence”, 80 \textit{NW. U. L. Rev}. 956 (960) (1986), at http://www.library.nwu.edu/law/depts/research/guides/libgui.html} Changes in a computer programme or manipulations of the data it contains can occur without any obvious clues appearing on the resulting printout.\footnote{\textsuperscript{87} Supra note 69, p. 178}
Therefore, the “regularity/business” statutory provisions do not improve a court’s ability to detect computer tampering.

(iii). the statutory foundations for business records as they presently exist are better adapted for manually-kept records than for computerized records. While it may be sufficient to investigate only the business practices surrounding manually-kept records’ creation and the time they were entered, such an analysis is insufficient for computer records. Traditional records are often created by direct manual entry, such as writing entries in an account ledger book. But use of a computer to store and retrieve business documents interjects an automation element between the record and its custodian. Accurate analysis of computerized record-keeping systems, therefore, requires separate inquiries into the custodian’s input procedures and into the reliability of the computer programme.88

In United States v. Russo,89 Russo, an osteopathic physician was convicted of mail fraud when he defrauded Blue Shield of Michigan of reimbursement monies by filing false patient claims. At trial, Blue Shield sought to introduce as evidence a computer printout showing stored records of false claims the defendant had filed.90 A Director of Blue Shield’s Service Review testified “in great detail” as to the accuracy of internal billing procedures undertaken by his department.91 Additionally, Michigan Blue Shield’s Vice President in-charge of all computer functions testified as to the computer equipment used, the verification procedures used to check the data, and the testing of the record-keeping programmes for precision.92 On appeal, the defendant objected to the introduction of the computer printouts supplied by Blue Shield, claiming that no proper foundation for the computer records had been laid.93 The court disagreed, saying that a reliable foundation for the printouts had been established by both witness’ testimony. The input data had been shown to be accurate, the output data reliability had been verified, and the reliability of the computer

89 480 F.2d 1228 (6th Cir. 1973) cert. denied, 414 U.S. 1157 (1974)
90 480 F.2d 1228 (1239)
91 Id. at p. 1233
92 Id. at p. 1234-35
93 Id. at p. 1241
hardware was not at issue. Thus, the Court took the additional important step of laying a foundation for both the input and output data when admitting computerized records into evidence under the business records exception. In doing so, that court took better notice of the evidentiary differences implicated by computerized record keeping.

*Monotype Corporation Plc v. International Typeface Corporation* involved admissibility of an E-mail message under the business record exception to hearsay rule. The court held that the E-mail is not a regular, systematic record meeting the foundational requirements of the business records exception.

As computers are being used widely in the public sphere as well in the US, there will be a need to introduce them under one of the other exceptions to hearsay. However, the issue of Internet evidence as a public record is well settled in the United States. In *Armstrong v. Executive Office of the President*, the court unequivocally held that government E-mail is a record as per the Federal Records Act, and it is insufficient for the Government only to preserve a print-out.

### 2. United Kingdom

The hearsay rule has been formalized by the House of Lords in a number of cases. The position regarding hearsay in England today is still governed by the landmark case in 1965 of *Byers v. DPP* that concerned an alleged conspiracy to deal in stolen cars. The defendant would buy a wrecked car and its log-book, and then steal an almost identical car. He would then convert the stolen car so that the details matched the logbook and proceed to sell it for a profit. Evidence produced by the car manufacturers at the time of the production of the cars was critical to the

---

94 Id. at pp. 1239-40
95 *Monotype Corp., Plc. v. International Typeface Corp.*, 43 F.3d 443 (9th Circuit)
96 However, in *U.S. v. Catabran*, 836 F.2d 453 (9th Cir. 1988), the court held that computerized printouts of accounting and other booking keeping records are admissible as business records. Critical to admissibility of the computer records was testimony establishing the foundational requirements of Federal Rule of Evidence 803(6); See also *Quality Auto Serv. v. Fiesta Lincoln-Mercury Dodge, Inc.* No. 04-96-00967-CV, 1997 WL 563176 (Tex. App. Sept. 10, 1997) holding that computer generated compilations of original invoices qualified as business records; *U.S. v. Kim*, 595 F.2d 755 (D.C. Cir. 1979), where discussing the admissibility of a telex, the court explained that the “critical factor in determining whether the document satisfied the ‘business purpose’ requirement lies in the reason that the message was prepared and sent, not the means by which it was transmitted.”
97 1F.3d 1274 (DC Circuit, 1993)
98 *Taper v. Reginam*, 1952 All ER 447; *Myers v. DPP*, (1964) 1 All ER 877; *R. v Patel*, (1981) 3 All ER 94
99 *Myers v. DPP*, (1964) 1 All ER 877
prosecution’s case. As the cars moved along the production line, workers recorded
details of the serial numbers of the various components fitted to a particular car. The
worker responsible recorded these details on a card. Eventually, the completed card
was photographed and recorded on microfilm. The prosecution sought to put the
microfilm in evidence at the trial under the exception to the hearsay rule which
covered business records in the Evidence Act, 1938. The Act did not mention
microfilm as a type of business record because the product was not in common use by
the businesses in the 1930s. The House of Lords held the evidence to be inadmissible
as hearsay, because any exception to the hearsay rule had to be construed restrictively.
In R. v. Golizadeh it was held that, “the unpronounceable machine…is not subject
to the vagaries of human recollection and the hearsay rule is an inappropriate
mechanism for regulating the input of material obtained from it.” In this case, the
question before the court was whether expert evidence relying on a machine’s printout
where the print-out was not exhibited and accuracy not challenged amounted to
hearsay. The court dismissed this contention of the defence and held the evidence to
be admissible.

3. Canada

Generally speaking, if a record is created in the ordinary course of business
and is relied on in the business, then it is admissible. Some rules require that it be
created more or less at the same time as the event recorded, and sometimes by a
person with a duty to record it. These circumstances give the record sufficient
assurances of the truth of its contents that it may be admitted.

The rule does not require separate proof of the truth of a record’s contents.
The making and the use of the record in the course of business provides sufficient
guarantee of the truth of the record’s contents to support admission.

Canada is one country where the issue of hearsay and computer evidence has
been raised in courts with frequency. In R. v. Pecciarich, the accused was charged

---

100 This statute has been repealed and replaced by the Civil Evidence Act, 1968 and is thus defunct.
102 Canadian Evidence Act; Section 30
with distributing child pornography by sending computer files to computer bulletin board using a code name. The identity of the accused was proved by circumstantial evidence, which consisted of documents found in accused’s possession and files on accused’s computer used as original circumstantial evidence that accused and the code name were linked in meaningful way. The inference sought to be made was that the accused and person using the code name were the same person. The defence raised the contention that the documents comprising circumstantial evidence from the computer were hearsay, and therefore inadmissible. The court rejected this contention and held the evidence to be not hit by the hearsay rule and admissible as circumstantial evidence.

In R. v. Weir, the question involved was whether an E-mail carried a reasonable level of privacy. The evidence sought to be adduced were user logs and E-mail messages supplied by the Internet Service Provider. The Court held that, “The Crown relies on an unseen process of extraction of non-visual information from a CPU. Further, the Crown had the diskettes which contain the extracted copies of what was on the CPU, again non-visual information, made exhibits at the voir dire. Although visual representations (i.e. printouts) of the data were made exhibits, they were made exhibits only for ease of reference. In other words, to be consistent with the alleged offence in which computer generation of the images is alleged (i.e. no hard copy), the hard copy was entered only to allow me to consider the evidence outside the courtroom without the need to use a computer. The use of unseen procedures to extract information is not new. Blood analyses, breathalyzer tests and photo radar are examples of processes of information extraction which have been subjected to reliability tests over the years. Because computer data can be manipulated, extraction reliability may arise in another case. It did not arise in this one. Second, because the evidence extracted from the CPU to diskette is not something I can see without the use of a computer, exhibit control is exceedingly important. The exhibits in this case were well controlled. The police were careful to keep the confirmatory evidence of the tip separate from the evidence extracted from Mr. Weir’s CPU. Although some of

the attachments extracted from both sources look the same, their source has been identified, they have been kept separate, and their continuity ensured.\textsuperscript{107}

Thus, a positive judicial attitude, coupled with an effort to create a “Law of Electronic Evidence” has ensured that Canada is in the lead in the development of such jurisprudence.

4. India

The idea that hearsay is applicable to documentary evidence is applicable in India, currently stands as law.\textsuperscript{108} The Indian Evidence Act, 1872,\textsuperscript{109} has been interpreted as containing the statutory rule against hearsay in this country.\textsuperscript{110} This mandates all oral evidence to be direct. Further, it is clear that the real evidence as regards computers is admissible. There has been no case in India challenging the admission of computer evidence under Section 32 (2). Section 34 also allows for evidence made in books of accounts. It may be noted that the IT Act has amended Section 34 to include books of accounts kept in electronic form.

Thus, there is no difficulty in admitting electronic evidence in India, and any arguments as to hearsay will not stand unless there are compelling reasons, such as the electronic record under examination indeed falling into the hearsay category. Electronic evidence does not demand any change to the rules on hearsay. The character of the record can be sufficiently demonstrated under existing law to meet the exceptions, regardless of the medium of the record.

N. \textbf{PAPER VERSUS ELECTRONIC DOCUMENT}

Since there is a difference in the manner with which we treat paper and electronic documents, each kind has its own peculiarities and characteristics as discussed below:

1. \textbf{Paper Document}

A paper document is comprised of following 4 components:

i. the carrier (the sheet of paper),

ii. text and pictures (the physical representation of the information),

iii. information about the originator / issuer, and

\textsuperscript{107} \textit{Id.} at para 38-40
\textsuperscript{108} \textit{Laksmi Raj Shetty v. State of Tamil Nadu, AIR 1988 SC 1274 (1290)}
\textsuperscript{109} The Indian Evidence Act, 1872; Section 60
iv. some measures to verify the authenticity (usually a written signature).

Carrier, information content, lay-out and signature are physically connected, so that we can say that the paper is the document.\textsuperscript{111} There exists only one original, and the peculiarity of a document of paper is that this single original can be reproduced any number of times.

There exists no disparity in the storage and exhibition of the matter in a paper document. In other words, the content is recorded and viewed in the same form. A consequence of this would be that in the long run, large amounts of paper are accumulated.

Paper, as the sole mean of recording a document to serve as primary evidence, does not go without its own weaknesses. Forgery of documents and signatures led to the establishment of a field of scientific experts and handwriting experts to solve such situations.

2. Electronic Document

The electronic or informatic document is the document produced by computer. Generally, we distinguish between an electronic document strictu sensu, i.e., the documents stored in a digital form and non perceivable by a person without using a computer, and an electronic document lato sensu, i.e., all that documents produced using a computer and issued with a printer connected to it.\textsuperscript{112}

The strictu sensu document is one that is rewritable, in the sense that it is imprinted on a magnetic base and can be deleted, modified and rewritten. This gives an electronic document its unique position compared with paper documents since each modification in the former leaves no mark or indication of tampering, whereas modification of a paper document always leaves a trace. This gives rise to the proposition that the integrity of an electronic document is “genetically” impossible to verify.

The additional need for caution arises because a digital document cannot be sealed in the way paper documents can. In the paper scenario, the author affixes his signature, name and address to validate the document and provide for attribution. This


\textsuperscript{112} Ibid.
cannot be as well accomplished in the electronic scenario. Therefore, it is impossible for the electronic document to have the same value of the paper document, because the signature carries out the 3 fundamental functions namely identification, declaration and proof.

O. PROOF

Only documents produced and proved by a witness in the Court can be regarded as evidence.\textsuperscript{113} How does one resolve the question of whether the electronic record is authentic? Is there to be a different scale of authenticity to apply to paper based documentary evidence as opposed to an electronic record? Should there be a presumption as to the attribution of the record. If so, what should this presumption be? How does one ensure integrity of the system generating the evidence? How, if desirable, should the best evidence rule apply in such a context? Is the said record to be considered primary or secondary evidence? Is the electronic record an original, or is it a copy? These questions are important in light of the treatment the evidence is to be accorded in a proceeding, and they are dealt with in the subsequent points.

P. AUTHENTICITY

A document’s admissibility is one thing, its probative value quite another.\textsuperscript{114} The traditional rationale for authenticating a document is to ascertain that the document is, in fact, what it purports to be in order to prove a relationship between it and an individual.\textsuperscript{115} An example of authentication is the establishing of a relationship between a monthly computer-generated summary of account activity and it’s corresponding customer.\textsuperscript{116} The summary of account must be shown to be an authentic statement of transactions between the customer and the plaintiff before the writing may be deemed relevant to an issue raised in litigation. For the document to be carrying any evidential weight and conviction, it must be shown to be authentic.

The means of doing this would be through an identification of the person the document relates to. Now, everybody who reads a writing can relate it to it’s issuer and signer and determine, without any reasonable doubt, the origin of the text. Thus, a

\textsuperscript{113} Anupam Chakraborty v. State of Assam, 1984 Cr. L.J. 733

\textsuperscript{114} State of Bihar v. Radha Krishna Singh, AIR 1983 SC 684


\textsuperscript{116} Ford Motor Credit Co. v. Swarens , 447 S.W. 2d 53 (Ky. 1969)
signature can be used to identify a person and to associate the person with the content of that document.

If it is accepted that a signature deems a document authentic in the case of a paper record, the question that arises is whether the same doctrine and standards can be made to apply as regards electronic records.

A signature could perform a variety of functions, depending on the nature of the document which was signed. For example, a signature might: attest to the intent of a party to be bound by the content of a signed contract, the intent of a person to endorse authorship of a text, the intent of a person to associate itself with the content of a document written by someone else, the fact that and the time when, a person had been at a given place.\(^{117}\)

A hand-written signature is easy to be affixed and read: these are two of the most important qualities of subscription and the first objection to the introduction of a digital signature system.

A common aspect in all legal systems is the absence of a prescription of an exclusive modality of signing. Everybody can use their full name, their initials, a nickname, a seal or even a cross if they intend those characters to be a token of their will and responsibility. What is important is not the nature of the symbol anybody uses to identify themselves, but the intent behind the symbol.

This means that there are almost no authoritative rules for the way of signing and that, from a legal point of view, nothing is against the introduction of new types or techniques of signature.

Every legal system recognizes the contractor’s right to rule their own contractual relations, defining also the way each one can sign the agreement.\(^{118}\)

Private persons can also decide to conclude their contracts using only computers, either in the negotiation or in the conclusion phase. Contractors can mutually accept the digital signature instead of the hand-written, simply inserting a clause that gives to digital signature the same powers and functions of hand-written


signature. Nowadays, in legal literature, it is a common statement that hand-written signature and paper document are overcome by technology. With modern instruments, such as scanner and plotter, it is possible to reproduce every signature perfectly and to copy it innumerable times.

Q. **ELECTRONIC SIGNATURE**

It is possible to accord the same legal treatment to an electronic signature, if such signature can perform the same function as a conventional signature. This electronic signature is not a written or embossed statement at the end of a document endorsing it. It is not a password to access the document. What it is, is the result of applying encryption to specific information. Countries like Malaysia, Singapore, Germany and several States in the US were early in having enacted specific laws to deal with Electronic Signature.\(^{119}\) The Indian IT Act not only gives legal validity to electronic signatures but also sets up a public-key infrastructure for asymmetric key encryption digital signatures.

R. **PRIMARY OR SECONDARY EVIDENCE**

If the document is shown to be authentic, the next query for the adducer is to look into whether it constitutes primary evidence\(^{120}\) or secondary evidence.\(^{121}\) Internet technology, as with computer technology, at every stage of the transaction, transmits only a copy of the data package. There is no original. Primary evidence envisages the existence of a single original, and this is an impossible proposition as regards computer documents. Since the glaring dangers of “manufactured evidence” are inherent in computer documents, and the divisive benchmark between primary and secondary evidence is the issue of original versus copy, presently, computer evidence should not be regarded as primary evidence.\(^{122}\)


\(^{120}\) The Indian Evidence Act, 1872; Section 62, It only restricts itself to the document in its original form.

\(^{121}\) Ibid., Section 63, The common thread running through the different types of secondary evidence throughout sub-sections 1 to 5 are that they are all not the original document, that is, they are all copies.

\(^{122}\) However, Indian law has not resolved the issue as to original versus copies. However, in the American case of *King v. State ex rel. Murdock Acceptance Corp.*, 222 So. 2d 393 (Miss., 1969), the issue was whether a print out satisfied the requirement of being an original record. It was held that the printouts were admissible evidence of a permanent record on magnetic tape. This was because of the obvious fact that records stored on magnetic tape were unavailable and useless except by means of printouts.
S. **BEST EVIDENCE RULE**

This rule essentially means that if the evidence sought to be admitted indicates the existence of better evidence, it should not be admitted, unless a satisfactory explanation of the absence of that better evidence has been given.

The solutions, which have been devised to deal with paper-based records, are not readily applicable to electronic records. It is with this principle in mind that the IT Act has included, through amendment, Section 65 B into the Indian Evidence Act. A careful reading of the provision will show that it overcomes all these problems of original versus copy, deeming electronic documents to be sufficient for proof of what the original could have legally proved, so long as:

i. 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;

ii. 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;

iii. 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 the operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

iv. 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.

T. **PUBLIC VERSUS PRIVATE DOCUMENTS**

In Monotype,\textsuperscript{123} it was held that a private E-mail message was not a regular, systematic record of business activity, and was thus hearsay evidence.

As regards public documents however, it was held in Armstrong,\textsuperscript{124} that a government E-mail is a record as per the Federal Records Act, and it is insufficient for the government only to preserve printouts.

U. **EFFECT OF ELECTRONIC EVIDENCE**

Now that the evidence is admitted and produced before the court, and proved to be what it purports to be, the next question in sequence would be: what is the weightage that should be given to such evidence, keeping in mind the vagaries of adducing computer evidence.

It must be remembered that once admitted, the evidence may be challenged on a number of grounds, including its lack of integrity, lack of truthfulness and lack of relevance to the issue. Has it been tampered with? How is the security to be demonstrated? Have the data degraded over time?

Proving such deficiencies is up to the opponent of the evidence, who has at least a tactical burden of doing so. Tactically, the proponent may lead evidence in response, to support the weight of the record.

If the proponent was not required to support the integrity of the record to have it admitted, the opponent could be in a difficult position in challenging the weight of the electronic record. The best person to give evidence on the reliability of the proponent’s system is probably the systems manager of the proponent, who if called by the opponent to testify, cannot be cross-examined.

The IT Act does legislate on a related aspect through an amendment brought about in the Indian Evidence Act\(^\text{125}\) which provides as under:

(i). In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(ii). In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that-

a. the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

---

\(^{124}\) *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (DC Circuit, 1993)

\(^{125}\) The Indian Evidence Act, 1872; Section 85 B
b. except in the case of a secure electronic record or a secure digital signature, nothing shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Hence the presumption as to authenticity and integrity of electronic records operates only in cases of secure electronic records. This does not mean that the authenticity and integrity of other electronic records cannot be proved by adducing evidence. It is only that the presumption will not operate in such a case.

The weight of evidence is traditionally not the subject of statute. It depends very much on the facts of the case at bar.

Nonetheless, the UNCITRAL Model Law provides as follows\(^\text{126}\). “Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.”

Alternatively, instead of this mandatory approach, it would be possible to set out factors in the statute that the court may, but need not, consider. However, a disadvantage of this approach is that, in practice, setting out such discretionary factors sometimes becomes a minimum requirement.\(^\text{127}\)

The statute should not give guidance on the factors that go to weight. The factors that may be suggested to courts and counsel and records managers should be adapted from the literature in the field.\(^\text{128}\)

The weightage also may be drawn from the opponent of the data. In \textit{R. v. Fellows} and \textit{Arnold}\(^\text{129}\), the only evidence consisted of data, which the court held to be

\(^{126}\) The UNCITRAL Model Law; Article 9 (2)
\(^{127}\) \textit{United States of America v. James Moriarty}, Criminal Action No. 96-30055-FHF, April 3, 1997, United States District Court of Massachusetts, at \url{http://www.bna.com/e-law?cases/moriarty.html}, where the court held that illegal wire-tapping should not be basis for conviction and allowed the defendant’s appeal to be dismissed.
\(^{128}\) \textit{Davis v. Gracey}, United States Court of Appeals, 10\(^\text{th}\) Circuit, No. 95-6245, April 21, 1999, at \url{http://www.bna.com/elaw?cases/davgracey.html}, where the court looked at various authorities on meaning of term ‘transport’ as applicable to data and the Internet, and reversed the charge of transporting and distributing obscene materials.
\(^{129}\) \textit{R. v. Fellows} and \textit{R. v. Arnold} (1997) 2 All ER 548
photographs.\textsuperscript{130} Affirming the lengthy sentence for the defendants, Lord Evans, J. referred to the opponent’s character in conjunction with societal concerns, and reasoned that where specialized computer operators use their skills for anti-social purposes, strict cognizance should be taken and treated with seriousness.\textsuperscript{131}

V. \textbf{FORENSIC COMPUTING}

The topic of appreciation is being properly addressed by the new science of forensic computing.\textsuperscript{132} This complicated discipline starts by considering ‘reliability’ as a combination of following 2 elements:

(i). the trustworthiness of the content of a piece of computer derived evidence; and
(ii). the trustworthiness of the process by which it was produced.

Together, the trustworthiness of content and process form the actual reliability of the evidence. Factors which have to be taken into account in determining this trustworthiness can include the quality of the original source, the quality of the internal computer manipulations, the strength of any control or audit mechanism which might reduce error or provide corroboration, the integrity of the way in which an exhibit has been derived, and integrity of the way in which the exhibit has been handled by or brought into being by the investigators. All of these factors will interact with each other.

W. \textbf{ELECTRONIC MESSAGE –COMMUNICATION THROUGH}

With the advancement of technology, a pertinent question arises as to whether in case of communication of electronic messages, the general rule or the exception with rule adopted in case of postal correspondence will apply. The Information Technology Act, 2000 provides that the dispatch of an electronic record occurs when it enters a computer resource (i.e. computer, computer system, computer network, data, computer data base or software) so as to be outside the control of the originator.\textsuperscript{133}

\textsuperscript{130} Id. at p. 557
\textsuperscript{131} Id. at p. 559
\textsuperscript{133} The Information Technology Act, 2000; Section 13 (1)
Further, if a computer resource has been designated by the addressee for the receipt of an electronic record and it is sent to the said resource, it will be deemed as received when the electronic record reaches designated computer resource. Thus, unless otherwise agreed, the postal rule will apply and the communication of electronic message or acceptance will be complete when it enters a computer resource not designated, the record will be considered as received when it is retrieved by the addressee. That is to say, the acceptance will be complete when it comes to the knowledge of the addressee. Where a computer resource has not been designated by the addressee, the record is deemed as received when it enters the computer resource of the addressee. In such a case, the sender of electronic message or record is entitled to consider that the record sent shall be binding only on receipt of acknowledgement of record.

X. REVIEW

The objective, to keep pace with the changing face of globalization, should be to facilitate the use of information and telecommunication technologies not only in the context of E-commerce, but also on a more individual, personal level. Technology is rapidly expanding at speeds too fast for society. The statute drafters should thus be careful in applying strict rules, definitions and interpretations to the subject matter. Yet, the framework must be broad and clear as to its content.

With the enactment of the IT Act, some of our fundamental issues are solved – the law recognizes electronic counterparts of paper documents and signatures, they are admissible in court and may be proved with few barriers such as requirement of originals. This is, however, only the first stage of moving into the secure electronic environment that the Act envisages. We must acknowledge that electronic records are vulnerable to tampering and there is no foolproof way of authentication and the acceptance and reliance on such forms of evidence should be tailored to the needs of each case. Judges ought to exercise careful discretion as to testing the integrity of the data. There must not be any strict method of deciding this, as integrity depends on system of system.

134 Ibid., Section 13 (2) (a) (i)
135 Ibid., Section 13(2) (a) (ii)
136 Ibid., Section 13(2) (b)
137 Ibid., Section 12
In the cyber age the evidence of crime lies in the digital formats like e-mails, chats, documents, digital pictures, pen drives, mobile phones etc. but the law enforcement agencies are handicapped in understanding these technical evidences and therefore digital forensics training needs to be imparted to them so as to crack cyber crimes.138