ISSN 1991-8976

RAJSHAHI UNIVERSITY LAW JOURNAL

FACULTY OF LAW
RAJSHAHI UNIVERSITY
2006

ARTICLES

ISSN 1991-8976

Rajshahi University Law Journal

Volume 03 2006

Published by:
Dean
Faculty of Law
Rajshahi University
Rajshahi- 6205
Bangladesh

FACULTY OF LAW
UNIVERSITY OF RAJSHAHI

Rajshahi University Law Journal 2006

Rajshahi University Law Journal

FACULTY OF LAW

UNIVERSITY OF RAJSHAHI

Volume 03 2006

Published by
Dean
Faculty of Law
Rajshahi University
Rajshahi- 6205
Bangladesh

Cover Design & Printed by
B T S Commercial Institute
Benodpur Bazar, Rajshahi

Printed at:
Barendra Printing Press & Packaging
Sapora, Rajshahi

Subscription Rates
For Individuals: **Tk. 100.00 US$ 20** (without postage)
For Organisation: **Tk. 150.00 US$ 30** (without postage)

[Published in December 2006]

Rajshahi University Law Journal 2006

Rajshahi University Law Journal, 2006: 97-112

The Nexus between Electronic and Paper Evidence under the Evidence Act, 1872

Zulfiquar Ahmed*

Abstract

The Article is to explore the nexus between the electronic records and paper based records. If electronic records are considered as evidence "while Bangladeshi evidence law did not support it as admissible and authenticate. So, it is a conflicting matter in the case of evaluation for evidentiary value. This Article also shows that how the revolution of Information and Communication Technology (ICT) has been made lag behind our legal system, i.e., evidence law, penal law, banking law etc. This Article also discusses the different provisions of UNCITRAL Model law on Electronic Commerce, UNCITRAL Model law on Electronic Signatures and ICT Bill, 2005 that are applicable as evidence regards electronic evidence.

1. Introduction

The lower courts in Bangladesh and the lawyers Practicing there are still more comfortable with the ticking sound of the manual typewriters rather than the silent clicking of computers. But in the judge court of Dhaka, even today, the ratio between manual typewriters and computers must not be any better than 90:10. If this is the ratio in the judge court of Dhaka, the state affairs in other parts of the country can be imagined. For this section of the legal community in Bangladesh, consisting of the lower judiciary and the lawyers practicing there, computers and the Internet are so far away. On the other hand, the worldwide rapid explosion of ICT (Information and Communication Technology) and the growth of use of computer and the expansion of electronic commerce are deeply changing the delivery and availability of information acts, transactions and services. Recording of evidence is one of the most important functions of the trial courts, both civil and criminal and therefore they shall be significantly affected by electronic/ computer evidence.[1]

As a general rule, "electronic evidence" can be any information created or stored in digital form whenever a computer is used to accomplish a task.[2]

---

* *LL.B (Honours), LL.M. (RU), Ph.D. Fellow, IBS and Lecturer, Department of Law & Justice, Rajshahi Univesity.*

[1] Vivek Sood, *Cyber Law Simplified,* (New Delhi: Tata McGraw-Hill, 2001), p.471.

[2] *See, e.g.,* Susan E. Davis, *Elementary Discovery, My Dear Watson, CAL. LAW.,* Mar. 1996, at 53, 53 (discussing different forms of electronic evidence); Susan J. Silvernail, *Electronic Evidence: Discovery in the Computer Age,* ALA. LAW., May 1997, at 176, 177 (explaining the expanding definition of discoverable

But 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.[3] A heavy onus would lie on the trial courts to answer questions inter-alia of the admissibility, relevance, authenticity, best evidence, hearsay evidence, proof of probative value of computer/electronic evidence and the manner of proving digital signature which are inconsistence to the traditional rules of evidence.[4] As this broad definition suggests, electronic evidence may exist whenever a person enters information into a computer, a computer generates information in response to a request by an operator or a computer uses or processes information. Electronic evidence, therefore, may include informat.on databases, operating systems, applications programs, "computer-generated models", electronic and voice mail messages and records and other information or "instructions residing in computer memory." A physical or bodily signature is necessary to formulate any transaction about business or to make any valid contract in the light of *the Evidence Act of 1872.* Any electronic contract is void under the *Evidence Act of Bangladesh.* The Evidence Law should be modified to recognize the validity of a digital signature.

2. Categories of evidence: ICT regime

The types of computer generated evidence and documentary evidence is almost same; but the concept of the both evidence is different. In general, evidence has been classified by under three heads, i.e., direct or indirect which is called circumstantial evidence, real or personal evidence and original or unoriginal evidence. Computer generated documentary evidence will be of three types.[5]

Real evidence is defined as evidence of a tangible nature from which the tribunal of fact can derive information by using its own senses.[6] By real evidence is meant evidence of which any object belonging to the class of thing, is the source, person also being included, in respect of such properties

---

"documents" in terms of electronic evidence).

[3] Devashish Krishan, "Internet Evidence and the Indian Legal Regime," *Law relating to Computers, Internet and E-commerce, ed. by* Nandan Kamath, (Delhi: Universal Publishing Co. Pvt. Ltd.,2000), p.49.

[4] Vivek Sood, *op. cit.*, pp.471 & 472.

[5] Devashish Krishan, *op. cit.*, p. 5 3.

[6] Peter Murphy, *A Practical Approach to Evidence,* (London: Blackstone Press, 1988), p. 186.

as belong to them in common with things.[7] On the other hand, real evidence under the computer generated documentary evidence is called that 'will be calculation 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'.[8]

Circumstantial evidences are the evidences of collateral facts and circumstances for which a reasonable conclusion about the question in issue may be drawn which is always based on experience and thereby a relation is established known and proved facts and the fact sought to be proved.[9] The presence of circumstantial evidences is probable through computer generated documentary evidences. For example, a person is charged with the offence of hacking or deleting or an unauthorized access of any computer network system or any personal computers without permission of the owner. The following facts would be proved:

1. Hacked computer is run by online and hacker's computer is run by on line at the same time;
2. Showing a certain types of massages at the time of hacking;
3. And the same massages showed all the users' computers of the computer network system;
4. And the same massages exist on the hacker's computer,
5. Some code number recovers from destroyed computer which is same hacker's computer.

Computer generated evidence is used as a hearsay evidence. When 'there are documents and records produced by the computer that are copies of information supplied to the computer by the human beings'[10] who are kept their books or accounts in due course of business. Exceptions of hearsay evidence are stated in section 32. Section 32(2) lays down that

> When the statement was made by such person in the ordinary course of business, and in particular when it consists of any entry or memorandum made by him in books kept in the ordinary course of business, ——— written of signed by him.

---

[7] K.K. Singh & H. P. Gupta, *The Indian Evidence Act, 1872.* (2nd ed.; Lucknow: Eastern Book Company, 2001), p. 8.

[8] Devashish Krishan, *op. cit.*, pp.54 & 55.

[9] K.K. Singh & H. P. Gupta, *op. cit.*, p. 6.

[10] Devashish Krishan, *op. cit.*, p. 54.

And section 34 makes an entry in books of account relevant when the account book was regularly kept in the course of business.[11] The above both sections have used the books for hearsay evidence and relevancy of entries. The court established books as a number of collected papers and bound together in one volume and the binding must be permanent.[12] Therefore, any person kept his entries into a computer and cell-phone or digital diary in the ordinary course of business. But the content of above entries are not relevant under the existing provisions *of the Evidence Act, 1872.* Since it has already been argued that electronic records constitute "writings and documents", further liberal interpretation should be employed by the court when a case as to this comes before it.[13]

3. Status of electronic record and law of evidence

It is a general perception that electronic/computer evidence is a new breed which was not covered in *the Evidence Act, 1872,* thus necessitating certain amendments therein.[14] Evidence is defined under section 3 *of the Evidence Act, 1872* as follows

Evidence means and includes-

(i) all statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;

(ii) all documents produced for the inspection of the Court; such documents are called documentary evidence.

According to the above definition evidence does not mean all the matters, through the help of which the court comes to any conclusion in any case.[15] The aforesaid definition of evidence would be amended by *the (Proposed) ICT Act, 2005,* which will read as follows[16]

Evidence means and includes-

(i) all statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence;

---

[11] K.K. Singh & H, P. Gupta, *op. cit.*, p. 102.

[12] *Ganash Prasad Roy v. Narendra Nath Sen,* AIR 1953 SC 431.

[13] *Chandradhar Goswami v. Gauhati Bank Ltd.*, AIR 1967 SC 1058.

[14] Vivek Sood, p.472,

[15] K.K. Singh & H. P. Gupta, *op. cit.*, p. 14.

[16] The Second Schedule, (Sec. 97 (2)), Proposed Information and Communication Technology Act, 2005.

(ii) all documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence.

In section 17 of *the Evidence Act, 1872,* which defines an admission, for the words, 'oral or documentary', the words, 'oral or documentary or contained in electronic form, shall be substituted.[17] In section 34 *of the Evidence Act, 1872,* which states of relevancy of entries in books of accounts regularly kept in the course of business, for the words, 'Entries in the books of account the words, 'Entries in the books of accounts, including those maintained in an electronic form shall be substituted. In section 35 *of the Evidence Act, 1872,* which states of relevancy of entry in public record made in performance of duty, for the word, "record", in both the places where it occurs, the words, "record or an electronic record," shall be substituted.[18] In section 59 *of the Evidence Act, 1872,* which provides the principle that all facts except the contents of documents, may be proved by oral evidence, for the words, "contents of documents," the words, "contents of documents or electronic records," shall be substituted.[19]

4. Electronic Document

Electronic document sometimes got the evidentiary value in the trial system of common law countries. But the computer-generated documents have no evidentiary value of our legal system. The judges of the civil law countries and many developed countries do not hesitate to introduce computer or electronic records as evidence for principle of free introduction and free evaluation of evidence. The judges of the common law countries, like Bangladesh, India, Sri Lanka, Pakistan, hesitate to accept computer or electronic records as evidence for principle of adversarial procedure until their evidence law permits thereby. For instance, the judges of the common law countries reluctant to accept e-mail as evidence. Document means any matter expressed or described upon any substance by means of letters, figures of 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.[20] For instance, a writing, words printed, lithographed or photographed and a map

---

[17] *Ibid.*
[18] *Ibid.*
[19] *Ibid.*
[20] Section 3, The Evidence Act, 1872 lays down that

or plan and an inscription on a metal plate or stone and a caricature are treated documents.[21] Section 3(18) of *the General Clauses Act, 1897* defines document in an inclusive manner. Document is to include 'any matter written, expressed or described upon any substance by means of letters, figures of 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.'[22] If a writing on a paper of leaflet, words printed, lithographed or photographed and a map or plan and an inscription on a metal plate or stone and a caricature are treated documents, there is no reason why electronic or computer record are not so.[23]

So, writing in a computer or web pages makes itself a document as per section 3 of *the Evidence Act, 1972* and Section 3(18) of *the General Clauses Act, 1897,* Bangladeshi courts have allowed video cassettes[24], tape recordings[25] and snap shot of hand cameras to be admissible on this manner. Tape recordings stand on the same footing as photographs and are documents as per section 3 of *the Evidence Act*[26] A video cassette is a document within the meaning of *the Evidence Act* and is accordingly admissible on evidence.[27] On the basis of the decisions of the cases *(Khaleda Akter v. State, M* P. *Verma* v. *Surinder kaur and* Z *B. bhkhri* v. *B. R. Mehra),* an electronic/computer record would be covered in the definition of document[28] It is shocking to say that a writing in ink on a piece of paper is a document, but the same when expressed or described electronically on the screen of the monitor, hard disk, floppy or compact disk (CD) is not so.[29]

Electronic record or electronic document and computer document which an expression or description of matter upon any substance on the screen of the monitor or stored on hard disk, floppy or compact disk (CD), pen drive and flash media etc. would be appeared legal document after passing *the (Proposed) ICT Bill, 2005. The (Proposed) ICT Bill, 2005* explains the

---

[21] Sec. 3 (illustrations) of the Evidence Act, 1872.
[22] Sec. 3(18), the General Clauses Act, 1897,
[23] Vivek Sood, *op. cit.* p.479
[24] *Mrs. Khaleda Akter v. The State.* 37 DLR 275.
[25] PLD 1977 (SC) 72. and PLJ 1977 (AJ & K) 1.
[26] *M. P. Verma v. Surinder Kavr,* AIR 1982 SC 1043 and *Z. B. bhkhari v. B. R. Mehra,* AIR 1975 SC 1788.
[27] *Mrs. Khaleda Akter Case. Id.*
[28] Vivek Sood, *op. cit.* p.479.
[29] *Id.* p.478.

electronic record, data and Computer system. "Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche.[30]

"Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.[31] The "data massage" is also defined by the *UNCITRAL Model Law on e-Commerce, 1996.* Data massage means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange *(EDI),* electronic mail, telegram, telex or tele copy.[32]

'Computer system' means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.[33]

4.1 Differences between Electronic Data and Traditional Paper Records

One of the key differences between electronic data and traditional paper records is the sheer volume of electronic data and the velocity with which electronic data is generated. E-mail is only one form of electronic evidence. More than 40 million e-mail users worldwide, sending an estimated 60 billion messages annually and creating reams of electronic data with a mere click of a button.[34] Many of these records will be generated using employer-owned

---

[30] Sec. 3 (t), the (Proposed) Information and Communication Technology (ICT) Act, 2005.

[31] Sec. 3(o), the (Proposed) Information and Communication Technology (ICT) Act, 2005.

[32] Article 2(a), the UNCITRAL Model Law on Electronic Commerce, 1996.

[33] Sec. 3 (1), the (Proposed) Information and Communication Technology (ICT) Act, 2005.

[34] Frank C. Morris, Jr., *E-Mail Communications: The Next Employment Law Nightmare,* CA 30 ALI-ABA 571, 573 (1995).

and employer-operated e-mail systems.[35] Businesses, organizations, and individuals around the world generate computerized information at incredible speeds, often instead of traditional paper records and in circumstances where a paper record might not exist.[36] As one district court recognized, '[c]omputers have become so commonplace that most court battles now involve discovery of computerstored information.'[37]

Another key difference between electronic and paper records is the distinctively durable nature of electronic evidence. Those who wish to discard paper records may simply throw out or mince the records. Those who wish to discard digital information do not possess such straightforward solutions. Contrary to popular belief, hitting the delete button does not destroy the computer records, nor is it the digital equivalent of throwing out or shredding a hard copy document.[38] Instead, the computer may "mark" the files as space that can be "overwritten" with new information in the future.[39] Deleting a file also may command the computer to mark the record for storage in a "back-up" or archive system, where the machine will save the record for a period of time. Whether the information is marked for overwriting, archived, or dealt with in some other manner, computer experts often can recover supposedly "deleted" information long after the computer user thought it had been destroyed. Thus, electronic data can appear unexpectedly, with the potential to generate litigation or dramatically impact its results.

Other key differences between electronic evidence and paper records are how, when, and why people record information in electronic form. As numerous litigants and commentators have found, people routinely use

---

35 *Ibid.*, (As of 1994, ninety percent of all companies with more than 1,000 employees had "some form of e-mail.").

36 Anthony J. Dreyer, When the Postman Beeps Twice: The Admissibility of Electronic Mail under the Business Records Exception of the Federal Rules of Evidence, 64 Fordham Law Review (1996), pp. 2285 and 2289 (noting the tremendous growth in the use of e-mail to conduct business and the "technological advances [that] have created a new type of 'virtual office' where paper records" are disappearing and documents increasingly are stored in electronic form).

37 *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 462 (D. Utah 1985).

38 Susan E. Davis, *Op. cit.* (discussing different forms of electronic evidence); see also: Susan J. Silvermass, *Op. cit. (Explaining the expanding detention of discoverable documents' in terms of electronic evidence).*

39 *Ibid.*

computers, particularly e-mail, to send draft, informal, or "uncensored" messages they would never "put in writing".[40] As a result, computerized records often contain insights into "corporate knowledge and behavior" and "off-the-cuff" remarks that people would never record on paper. Such remarks are often damaging in litigation.

Another important difference between electronic and paper records is the ease with which users may manipulate and exchange electronic information as compared to paper data. But today the electronic evidence has become critical to civil and criminal proceedings, largely because it differs from the traditional paper trial and it is not properly acceptable in our legal system for unavailability of the regulatory framework.

4.2. Admissibility of electronic document: Primary or secondary

A document must be proved by the primary evidence[41] and this is the best evidence rule. The secondary evidence may be given relating to the document under certain exceptional circumstances.[42] When the party is unable to produce the original for no fault of his own, he is given an alternative method to prove the contents of the document for the sake of justice.[43] Electronic or computer generated records may be classified for the purposive value of the terms of primary or secondary evidences as follows

- Original electronic record is treated as a primary evidence;
- And Computer copy or output is treated as secondary evidence.

Therefore, for proving the original electronic record on the basis of the principle of primary evidence, the computer system may have to physically be carried to the court, which would cause immense hardships and inconvenience, be very impractical and in many cases if not most, it would practically be an impossible exercise especially where a combination of computers is involved to generate the electronic record.[44] Thus the computer printout that was admitted as secondary evidence must have behind it an original 'document'.[45] There has been some academic debate m Nigeria

---

[40] Anthony J. Dreyer, toc. cit

[41] Sec. 64. the Evidence Act. 1872.

[42] Secs. 64 & 65, the Evidence Act, 1872.

[43] K.K. Singh & H. P. Gupta, op. cit, p, 151.

[44] Vivek Sood, *op.* cit p.478.

[45] Obenga Bamodn 'Information Communications Technology and E-Commerce: Challenges and Opportunities for the Nigerian Legal System and the Judiciary,

recently on the issue of whether computer print-outs, which have been held to be admissible in evidence by the Nigerian Supreme Court in *Anyaebosi v R T Briscoe Nigeria Ltd*[46], should be admissible as primary evidence or should always only be secondary evidence.[47] *The UNCITRAL Model Law on Electronic Commerce, 1996* deals with the admissibility in Art. 9(1) and evidentiary value of data massages in Art. 9(2). *The (Proposed) Information and Communication Technology (ICT) Bill, 2005* lays down a blanket permission for records not to be denied legal effect if they are in electronic format.[48] A more welcome recent development is that the current Draft *ICT Bill, 2005* seeks to lay down rules for the admissibility of electronic evidence and on the weight to be attached to such evidence. There is no comprehensive law on the admissibility of computer-generated evidence in Bangladesh. Even if an electronic record satisfies the tests that may be laid down for its admissibility, there is the further question of what weight is to be attached to such evidence.[49] In the case of *Ferber,*[50] both sides vigorously contested the admissibility of this e-mail message at trial. The government first argued that the [e]-mail mėssage was admissible under the business record exception to the hearsay rule.[51] The government argued that there was sufficient foundation for admitting the e-mail as a business record because the e-mail printout was "authentic and accurate", and because it was the employee's "routine practice" to e-mail relevant co-workers immediately after important conversations with clients.[52] The court, however, found that while the employee may routinely have sent such e-mails, his

---

2004 (2) *The Journal of Information, Law and Technology (JILT)*. Available at http://www2.warwick.ac.uk/fae/ soc/law/eli/jilt/2004_2/bamodu/.

[46] [1987] 3 N.W.L.R. 84 (part 59).

[47] T. Osipitan, 'Admissibility of Computer Pant out under Nigerian Law' (1995) 2(2) *Lawyers' Bi-Annual* 236 and T Osiptan, 'Legal Impact of Technology on Rules of Evidence in Banking and Commercial Litigation' (1998) 2 *Modern Practice of Finance & Investment Law* 71.

[48] Devashish Krishan *op.* cit., p. 65.

[49] Gbenga Bamodu, *loc,* cit.

[50] *United States v. Ferber,* 966 F. Sopp. at 98. (D. Mass. 1997).

[51] "Records of regularly conducted [business] activity" include "a[ny] memorandum, report, record, or data compilation . . . made . . . [by] a person with knowledge, if kept in the course of a regularly conducted business activity," FED. R EVID 803(6), and the nature of the business activity gives me to a duty to create such a business record. See also *Willco Kuwait (Trading SAK. v, deSavary,* 843 F.2d 618,628 (let Cir. 1988)).

[52] 13 *Ferber,* 966F.Supp.at 98.

employer, Merrill Lynch, had no business duty to make and retain records of this nature. Thus, the court held the email was not admissible as a business record.[53]

4.3. Authentication of Computer-generated Evidence

Authentication of computer-generated evidence has thus far been governed by the principles, rules and statues that existed before computer usage became widespread.[54] If a business record is computer- generated, the basic requirements for authentication persist.[55] A document's admissibility is one thing and its authenticity or probative value quite another.[56] A signature used to authenticate in the case of paper based record. The same doctrine and standards can be made to apply as regards electronic records. And digital signature system has a higher degree of security to authenticate the document and to identify and bind the person who signs or endorser. *The ICT Bill, 2005* recognises digital signature. It provides for digital signature as secure[57] and unreliable, public and private key[58], digital certificate[59], certification authorities[60], and recognition of foreign specified certification authorities[61]. Courts "have addressed the questions of witnesses" qualifications and trustworthiness of records.[62]

5. Digital Signature in Electronic Evidence

A digital signature is an electronic signature that can be used to authenticate

---

[53] *See id.* at 98-99 (eiting Willco Kuwait (Trading) S.AX. v. deSawary, 843 F.2d 618, 628 (1st Cir. 1988)) The court also noted dial wore the e-mail admitted, "virtually any document found m the files of a business which pertained in any way to die functioning of that business would be admitted 'willy-nilly' as a business record." *Id*, at 99.

[54] John Robinson Thomas, Legal Responses to Commercial Transactions Employing Novel Communications Media, 90 Mich. L. Rev. 1145,1147 (1992).

[55] *United States* v. *DeGcorgsa,* 420 F.2d 889, 893 n. 11 (9th Cir. 1969); See also *Rownberg case,* 624 F.2d at 665, citing *United Stages* v. *Fendley* 522 F.2d 181. 184 (5th Cir. 1975). See *United States* v. *Russo,* 480 F, 2d 1228. 1240 (6th Cir.), cert denied. 414 U.S. 1157 (1973)

[56] *State of Bihar v. Radha Krishna Singh,* AIR 1983 SC 684.

[57] Section 15, *the ICT Bill, 2005.*

[58] *Id., sec* .41.

[59] *Id.,* sec. 4.

[60] *Id.,* sec. 18.

[61] *Id., sec.* 20

[62] *King* v. *State ex rel. Murdock Acceptance Corp.,* 222 So. 2d 393, 398 (Miss.1969),

the identity of the sender of a message or the signer of a document. Digital signatures can also be used to ensure that the original content of an electronic message or document has not been changed. Digital signatures are used to guarantee the security of online transactions and information transfer. Digital or electronic signature is very essential to prove a document as copy of electronic evidence. "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message.[63]

Experts are of the opinion that all online communications and transactions in Bangladesh should be regulated by the Law on Electronic Signatures which is intended cover the online activities of government organizations, companies and individuals. Since Bangladesh's first Web-based transaction in 2001, the volume of e-commerce transactions has been increasing gradually and the demand for legislative protection is greater than ever. In 2001, *The UNCITRAL Model Law on Electronic Signatures* enumerate the process of digital signature. The use of digital signatures usually involves the following processes, performed either by the signatory or by the receiver of the digitally signed message:[64]

(1) The user generates or is given a unique cryptographic key pair;

(2) The signatory prepares a message (for example, in the form of an electronic mail message) on a computer;

(3) The signatory prepares a "message digest", using a secure hash algorithm. Digital signature creation uses a hash result derived from and unique to both the signed message and a given private key;

(4) The signatory encrypts the message digest with me private key. The private key is applied to the message digest text using a mathematical algorithm. The digital signature consists of the encrypted message digest;

(5) The signatory typically attaches or appends its digital signature to the message;

(6) The signatory sends the digital signature and the (unencrypted or

---

[63] Article 2 (a). The UNC1TRAL Model Law on Electronic Signatures, 2001.

[64] *Draft Guide to Enactment of the UNC1TRAL Model Law on Electronic Signatures,* United Nations Commission on International Trade Law, *Thirty-fourth session, Vienna, 25 June -13 July 2001. p.24.*

encrypted) message to the relying party electronically;

(7) The relying party uses the signatory's public key to verify the signatory's digital signature. Verification using the signatory's public key provides a level of technical assurance that the message came exclusively from the signatory;

(8) The relying party also creates a "message digest" of the message, using the same secure hash algorithm;

(9) The relying party compares the two message digests. If they are the same, then the relying party knows mat the message has not been altered after it was signed. Even if one bit in the message has been altered after the message has been digitally signed, the message digest created by the relying party will be different from the message digest created by the signatory;

(10) Where the certification process is resorted to, the relying party obtains a certificate from the certification service provider (including through the signatory or otherwise), which confirms the digital signature on the signatory's message. The certificate contains the public key and name of the signatory (and possibly additional information), digitally signed by the certification service provider.

6. UNCITRAL Model Law Electronic Commerce

The best-known UNCITRAL instrument in the sphere of electronic commerce is the UNCITRAL Model Law on Electronic Commerce. With a view to facilitating the increased use of modem methods of communication, *UNCITRAL* has prepared *the UNCITRAL Model Law on Electronic Commerce.* The purpose of *the UNCITRAL Model Law on Electronic Commerce* is to offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce". *The UNCITRAL Model Law on Electronic Commerce* also helped to remedy disadvantages that stemmed from the fact that inadequate legislation at the national level created obstacles to international trade, a significant amount of which is linked to the use of modem communication techniques. *The UNCITRAL Model law on Electronic Commerce*[65] legalizes the computer generated evidences. This law provides evidentiary value of data

---

[65] *The United Nations Commission on International Trade Law, 1996.*

massages if it satisfied the following two tests.[66] Information shall not be denied legal effect, validity or enforce-ability solely on the grounds that it is the form of a data massage.[67]

> 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 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.

Article 9(2) of *the UNCITRAL Model Law* provides clear concept for recognition of data message as evidence.[68] The Model law also states 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.[69] *The UNCITRAL Model law on Electronic Commerce* is created as a suggested pattern for lawmakers in national governments to consider adopting as part of their domestic legislation. Legislation implementing provisions of the Model Law has been adopted in: Australia (1999), China (2004), Colombia (1999), Dominican Republic (2002), Ecuador (2002), France (2000), India (2000), Ireland (2000), Jordan (2001), Mauritius (2000), Mexico (2000), New Zealand (2002), Pakistan (2002), Panama (2001), Philippines (2000). Republic of Korea (1999), Singapore (1998), Slovenia (2000), South Africa (2002), Thailand (2002) and Venezuela (2001).

7. UNCITRAL Model Law Electronic Signature

The UNCITRAL Model Law on Electronic Signatures, 2001 introduced for purpose of the increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (which may be referred to generally as "electronic signatures"). The risk that diverging legislative approaches be taken in

---

[66] Article 13, *the UNCITRAL Model Law on e-Commerce, 1996.*

[67] Article 5, *Id.*

[68] '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 m which the data message was generated, stored or communicated, to the reliability of the manner in which its originator was identified, and to any other relevant factor.'

[69] Article 6(1), *the UNCITRAL Model Law*, 1996.

various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal harmony as well as technical interoperability is a desirable objective. The Model Law is designed to assist States in establishing a modem, harmonized and fair legislative framework to address more effectively the issues of electronic signatures. In a modest but significant addition to the *UNCITRAL Model Law on Electronic Commerce*, the new Model Law offers practical standards against which the technical reliability of electronic signatures may be measured. In addition, the Model Law provides a linkage between such technical reliability and the legal effectiveness that may be expected from a given electronic signature. The Model Law adds substantially to *the UNCITRAL Model Law on Electronic Commerce* by adopting an approach under which the legal effectiveness of a given electronic signature technique may be pre-determined (or assessed prior to being actually used). The Model Law is thus intended to foster the understanding of electronic signatures, and the confidence that certain electronic signature techniques can be relied upon in legally significant transactions. Moreover, by establishing with appropriate flexibility a set of basic rules of conduct for the various parties that may become involved in the use of electronic signatures (i.e., signatories, relying parties and third-party certification service providers) the Model Law may assist in shaping more harmonious commercial practices in cyberspace. The objectives of the Model Law are enabling or making easy the exercise of electronic signatures and providing equal handling to users of paper-based documentation and users of computer-based information which are essential for promotion economy and efficiency in international trade.

8. The Information and Communication Technology *(ICT)* Bill, 2005

The enactment of ICT Bill should solve the question of writing or not written, document or file, admissibility and authenticity of electronic documents. The Government of Bangladesh responded by coming up with the draft of the first cyber law of Bangladesh- *The Information and Communication Technology Bill (ICT), 2005.* The Cabinet of Ministers of Bangladesh has approved *the Information and Communication Technology Bill (ICT)* of 2005 on 14 February 2005 and its enactment by Parliament is pending. This Bill has proposed significant amendment *of the Evidence Act of 1872.* Various sections *of the Evidence Act* has been modified for acceptance as an evidence of computer documentary, Internet documentary as well as electronic record or electronic form as an evidence at the age of ICT. By the enacting ICT Act is intended to amend *the Evidence Act* to facilitate the use of electronic records and signatures as evidence and to harmonize this Act with the electronic commerce and information revolutionized arena. It is noted that *the Information and Communication Technology Bill (ICT), 2005* is the first step for harmonizing with the world informatization process with respect to the uniform rules on electronic commerce and electronic signatures by providing *the UNCITRAL Model Law on Electronic Commerce,* 1996 and *the UNCITRAL Model Law on Electronic Signature, 2001,*

9. Concluding Remarks

All kinds of evidence are necessary to detect or identify the actual fact of any matter. The judges of the civil law countries can consider all kinds of evidence and they do not hesitate to introduce computer records as evidence. Under the Islamic law, computer crime or computer related offences fall within the area of taazir offences, which operates according to the same principles of evidence law as civilian system.[70] Contrary to the legal situation in civil or Islamic law countries, common law countries are characterized by an oral and adversarial procedure. The questions whether computer files or other computer generated documents are 'real evidence' and whether computer printouts fall under the one exceptions of hearsay rule have been the subject of extensive debate. The courts of some common law countries have accepted computer printouts, e-mails as falling within the business records exception.[71] Other common law countries have elaborated new laws allowing computer records to be admitted as evidence if certain conditions are met. The article proposes that the law be clarified to ensure that the proponent of an electronic record not have to demonstrate that the record is an original or is close to an original. Bangladesh Government should enact the Law on Electronic Signatures for the establishment of an online authentication system and designing to safeguard Internet-based transactions and legalizing the implementation of e-business and e-movement applications.

---

70 Civil law countries and many other countries including Islamic law countries operate according to tee principle of free introduction and free evaluation of evidence *(systeme de I 'intone-conviction).*

71 See, (USA cases) *United States* v. *Russo,* 480 F.2d 1228 (6th Csr. 1973), *Monotype Corp Pk* v. *International Typeface Corp..* 43 F. 3d 443. (UK cases) *Taper* v. *Regwam,* (1952) AB ER 447; *Myers v. DPP,* (1964) 1 AH ER 877; *R.* v. *Patel,* (1981) 3 All ER 94, R. v. *Shephard,* (1993) 1 All ER 225 and R. v. *Gotzadeh,* (1995) Crim. LR 232.