BILETA

17th BILETA Annual Conference

April 5th - 6th, 2002.
Free University, Amsterdam.

Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000

Subhajit Basu & Richard Jones

(Liverpool John Moores University)

1. Introduction

The impact of e-commerce over the global economy is well documented. Europe and the United States are the main beneficiaries, with countries such as India and China with their huge pools of technologically skilled manpower, also hoping to benefit. Business-to-Business (B2B) e-commerce is a fact; the bigger players are driving their associates into this model. Governments and inter-government agencies are working hard to facilitate the expansion of such transactions, through the clarification of the legal issues and the liberalization of ISP industry. However business-to-consumer (B2C) is a more difficult to facilitate. Consumer resistance to the removal of what is a social experience is proving harder to break than anticipated.

In this paper our focus will be on India, a rural economy where e-commerce is set deal with the problem in today's Indian producer/consumer chain, that is the middlemen (powerful distributors), who make most of the money, while the poor producer gets a pittance. E-commerce has the potential to change this scenario dramatically and it is beyond question that there is a need for a coherent yet flexible legal network to felicitate the e-entrepreneurs spirit and the confidence of consumers. The *Information and Technology Act 2000* is India's attempt to formulate such legal network. It is our view that the Act is too prescriptive. The attempt to relate to particular forms of technology and to foresee all possible options has created an over complex set of provisions that will hinder rather than encourage the development of e-commerce.

2. What is E-Commerce?

Electronic commerce (or e-commerce) encompasses all business conducted by means of computer networks. It reflects a paradigm shift driven by two primary factors:

- A wide range of converging technological developments and
- The emergence of the so-called "*knowledge economy*".

Recent advances in telecommunications and computer technologies have moved computer networks to the centre of the international economic infrastructure, everyone with a computer and connected to the Internet has become a potential player and a potential market for the e-entrepreneur. These technological developments have gone hand in hand with a trend, predominantly in the developed world, towards a post-industrial knowledge economy. This new paradigm, which is already having a significant impact on the way in which people lead their lives, is difficult to define but is characterised by -

- An emphasis on the human mind, rather than merely physical automation;
- Being information- rather than energy intensive;
- Sustainability through networks, not single organisations;
- Supporting distributed rather than centralised intelligence;
- Requiring multiple skills and continuous learning;
- Replacing lifetime employment with labour market flexibility;
- Customised rather than standardised products; and
- Being enabled by information and communications technologies (ICTs), whilst simultaneously driving the development of new ICTs.

Just as the industrial society built on and then dominated the agricultural society, the knowledge society is now building on the platform provided by the industrial society. It can be argued that e-commerce, along with the technologies and knowledge required to affect it, is the first real manifestation of the knowledge society. The question for the less industrialised developing countries is whether they can use appropriate technologies to leapfrog into the knowledge society, by-passing some of the stages of the industrial paradigm.

The vast majority of these 'e-commerce' transactions to date have taken place in countries with advanced economies and infrastructure. For developing countries such as India, e-commerce offers significant opportunities; e-commerce diminishes existing advantages of cost, communication, and information, and may create huge new markets for indigenous products and services. While many companies and communities in India are beginning to take advantage of the potential of e-commerce, critical challenges remain to be overcome before its potential can be fully realised for the benefit of all citizens.

3. E-Commerce Survey

According to Goldman Sach's study of Internet users, the number of users in India is expected to grow from 0.5 million in 1998 to 9 million in 2003, which translates to a compounded annual growth rate ("CAGR") of 76% - the fastest in Asia.

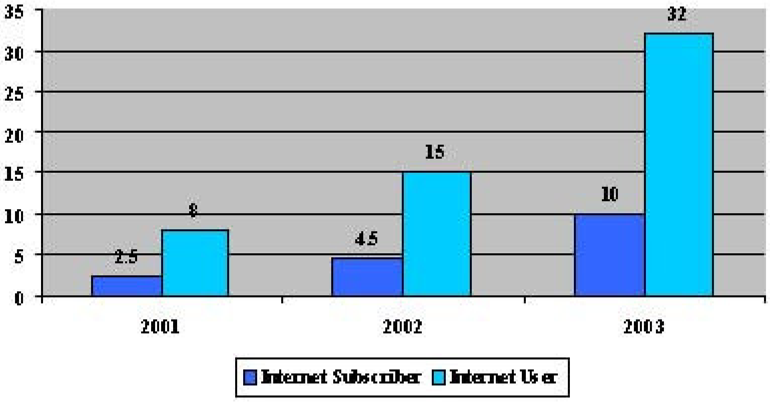

Figure 1: NASSCOM Survey of Internet Users in India (millions)

The difference between the two projections may be on account of recognition by NASSCOM that the number of users can be more than the number of subscribers. The use of cable television to facilitate access to the Internet may result in a faster growth of the number of Internet users in India since presently there are 37 million cable connections.

At present, India is not amongst the top 15 Internet using nations. This is primarily on account of the low PC penetration in India. According to a NASSCOM survey, there were about 5 million PCs in

India as on August 31, 2000, against a population of 1 billion.

4. Technology developments

It is projected that a rise in mobile or m-commerce would reflect the attitudes to risk taking and employee participation, already standard in the US. According to Ian Taylor (chairman, CMG, UK), web-commerce will require greater cross fertilisation of skills across traditional `silo' mentalities separating IT marketing, and sales. These factors will determine differences among enterprises across the countries. As Nicholas Negroponte, known as a digital guru, says "*the internet economy does not pit the big against the small. Its about the swift against the slow*".

Traditionally the big fish eat small fish, now the small fish have a chance. For example, Bill Gates has serious plans to develop hi-tech houses based on convergence of consumer electronics. Such houses would provide a sustained market potential for high value-added e-commerce if a supplier were well prepared. Undoubtedly, this is an area in which international barriers to entry are low, be it technology, communication, language, or time. Indeed, e-commerce helps over-come even `comparative disadvantage' arising due to geography, notably long distance and land-locked supply positions, as in northern India. Furthermore, businesses now have an opportunity to interact directly with foreign consumers, and if the products and services are competitive, they will compel the erstwhile oligopolies to break, and accept Indian supplies.

Amongst the Asian nations, the growth of e-commerce in India between 1997 and 2003 is expected to be the highest with CAGR of 246% (Fig 2). As per ICRA report released in September 2000, e-commerce activities are expected to witness the highest growth rates in the period between 2000-2001 and 2002-2003 following the emergence of broadband and improvements in the connectivity infrastructure. It is estimated that currently there are around 50,000 dot coms which are of Indian origin or are India-oriented (established outside India with India centric content). However, the volume of e-commerce, in India, is far below the levels achieved in USA, which was about 1 percent of the total GDP in 1999. Further, the expected volume of e-commerce in India in 2001 (US$ 255.3 million) is also below the levels expected to be achieved, which in comparison to Australia (US$ 3 billion), China (US$ 586 million), South Korea (US$ 876 million) and Hong Kong (US$685 million) is quite less.

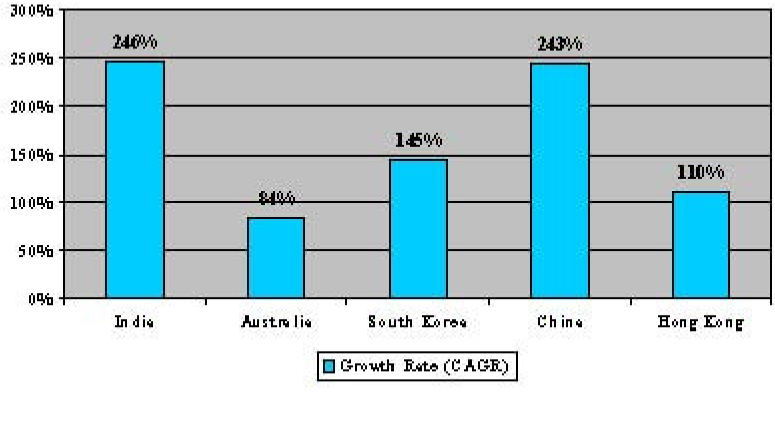

Figure 2:Growth Rate of E-Commerce between 1997-2003

An *Arthur Andersen* study expects 3,000 digital marketplaces to be operational by 2005.The global market for IT enabled services is estimated to grow to $ 142bn over the next eight years (by 2008), and according to the NASSCOM-McKinsey report, India could corner $ 17 bn, 12% of this market by means of meeting the outsourcing requirements. The B2B segment is expected to account for 90% of the total e-commerce in India (Indian Credit Rating Agency)(Fig 3*)*.

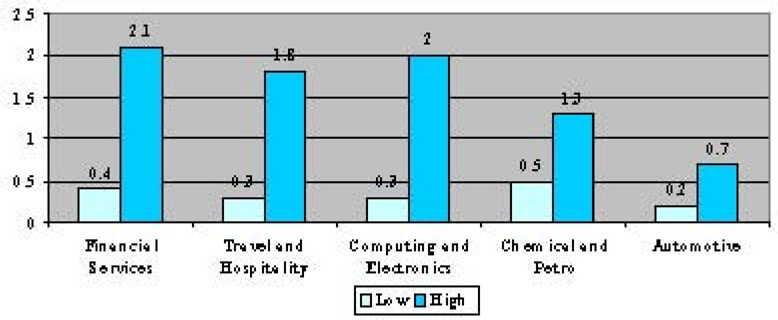

Figure 3:Growth by the year 2008 in US $ (billion)

Amongst these segments, financial services and computing & electronics are expected to have purely domestic components whereas others will have both domestic and export components (Interview; McKinsey Analysis). This may be a realistic projection, considering exports estimated at $ 2.65 bn in 1998-99 (out of total turnover of $ 3.9bn) and $ 3.9 bn in 1999-2000 (total $ 5.7 bn). Export revenues are reflected in private transfer receipts under BOP (RBI). Import figures do not come out from private transfer payments, and DGCI and S figures show software import worth only $ 12.8 million for April-December 104 of Fortune-500 companies are reported to be outsourcing software from Indian companies. IT and software exports can, however, be a part of the whole story of India's international business. The larger issue needs to be tackled which is scaling up aggregate exports using information technology, particularly for e-commerce. India's (total) exports are broad-based, which are reported to be making remarkable headway in e-commerce, requiring their trade partners including India to switch to e-commerce at the earliest (Fig 4).

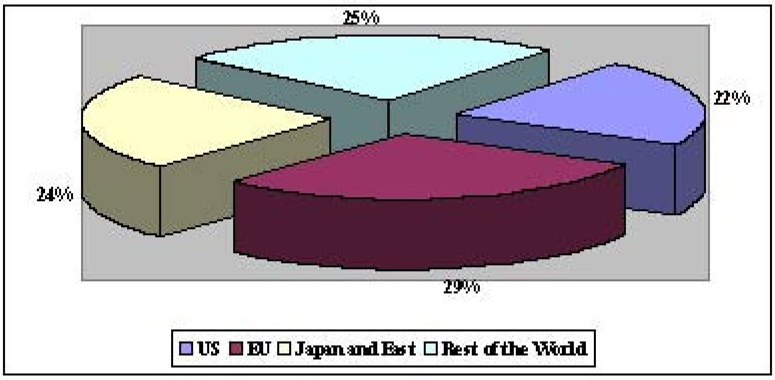

Figure 4: India 's Total Export (1998-99)

A study by Securities and Exchange Board of India ("SEBI") estimates that Internet trade in shares and securities accounts for only 0.36 percent of the total trade, while in value terms the share of Internet trading is merely 0.19 percent. The main impediments to the growth of Internet trade have been identified as apprehension regarding the robustness of the hardware systems and software applications, lack of online banking and low speed of Internet access. According to the Reserve Bank of India ("RBI"), in the banking sector in India the Internet is being used, at present, only for accessing information about accounts and transfer of funds between two accounts of the same account holder or across accounts maintained within the same bank. Electronic ordering and processing with a fully integrated online payment system is likely to be in place within the next few years.

5 Information Technology Act, 2000

Many legal rules assume the existence of paper records and documents, signed records, original records, physical cash, cheques and a face-to-face meeting. Electronic transactions require new forms of record, and recognition of new forms of communication. The *Information and Technology Act 2000* is based on the *Model Law* on E-Commerce adopted by the *United Nations Commission on International Trade Law* (UNCITRAL) and pioneering e-commerce enabling legislations such as the *Utah Digital Signatures Act, 1995*, the *Singapore Electronic Transactions Act, 1998* and the *Malaysian Electronic Signatures Act*. The essence of the Act is captured in the long title of the Act, "*An act to provide for the legal recognition of transactions carried out by ... alternatives to paper-based methods of communication and storage of information...*"

The Act, comprises of three significant aspects:

- Legal recognition of electronic records and communications - contractual framework, evidentiary aspects, digital signatures as the method of authentication, rules for determining time and place of dispatch and receipt of electronic records.
- Regulation of Certification Authorities ("CAs") - appointment of a Controller of CAs, grant of licenses to CAs, duties vis-à-vis subscribers of digital signature certificates, recognition of foreign CAs.
- Cyber contraventions - civil and criminal violations, penalties, establishment of the Adjudicating Authority and the Cyber Regulatory Appellate Tribunal, etc.

Further, the Act amends the *Indian Penal Code, 1860*, the Indian *Evidence Act, 1872, Bankers Book Evidence Act, 1891* and the *Reserve Bank of India Act, 1934*. The main purpose of these amendments is to address the related issues of electronic crimes and evidence, and to enable further regulation as regards electronic funds transfers.

Unlike similar legislation, the Act also seeks to regulate the Internet in some form by making publication of obscene information in electronic form an offence and for providing offences of hacking and of destroying or altering data. It is also to the credit of the Indian legislature that the Act was one of the first pieces of legislation in India to be thrown open for public comment, prior to it being finalized.

5.1 Contractual Issues

There are two main methods of electronic contracting; the electronic mail or e-mail and the click wrap method used on the World Wide Web[1].

- The Agreement and Form

The basis of a contract is an agreement. An agreement notionally comprises of an offer, which is then accepted. Offers may be made directly or through a mass email or through a web page. It is important to distinguish an offer from an invitation to make an offer. Whilst a direct contact is likely to be construed as an offer, a mass email or advertisement on a web page may be either an offer or an invitation to make an offer. The distinction is important as an offer if accepted results in a contract whereas an invitation to offer required the recipient to make an offer, which may then either be accepted or rejected.

A contract is concluded when an offer is accepted. If any advertisement over the web or any communication over the Internet (automatic or otherwise) is construed as an offer, and if that offer is unconditionally accepted, the contract is concluded. On the other hand, if the advertisement is construed as an invitation to make an offer it only invites users to make an offer for the advertised product or service. The choice whether to accept that offer is in the hands of the person who invited the offer.

An invitation to offer opens the process of negotiation. In order to identify such invitations the law has developed presumptions as to whether certain common statements or actions amount to an offer or are mere invitations to make an offer[2]., thus we can say with some authority that shop displays are invitations to treat as are items for sale at auctions[3] and advertisements[4]. A web advertisement is closer to shop displays than to advertisements in magazines or on television due to the interactivity of Websites. As such web advertisements will be an invitations to offer unless it clearly indicates the web advertiser's intends to be bound upon the acceptance[5].

Under the *India Contract Act,* 1872, contracts are binding irrespective of their form. Therefore unless a specific form is proscribed a contract is binding whether it is oral or in another form. It can be assumed that electronic contracts will be valid as under the other form. The *Information and Technology Act,* 2000 however puts the matter beyond doubt and while adopting the Model Law[6], states that unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of "electronic records"[7].

- **Offer**

Under the *Information and Technology Act, 2000*, the offer is made, unless otherwise agreed between the originator and the addressee, at the time when the electronic record enters any information system designated by the addressee for the purpose, or, if no system is designated for the purpose, when the electronic record enters the information system of the addressee, or, if an information system has been designated, but the electronic record is sent to some other information system, when the addressee retrieves such electronic record. This reflects the Model Law[8] as to when an offer is made[9]. The Act further provides that an electronic record shall be attributed to the originator if it was sent (a) by originator, or (b) by a person who had the authority to act on behalf of the originator in respect of that electronic record, or (c) by an information system programmed by or on behalf of the originator to operate automatically.[10] This will presumably cover situations when an intelligent `agent' is programmed to issue offers on behalf of an individual.[11] But does not cover a where a file containing the offer is found by another. What would be the motive attributable to the author of the file?

- **Acceptance**

Under the *Indian Contract Act, 1872*, the acceptance of a valid offer[12] results in a valid contract. Such an acceptance may be expressed, in written or oral form or may be implied by the conduct of the offeree. The timing of an acceptance depends upon whether the context, inter *praesentes* (when the contracting parties are face to face with each other) or inter absentees (where the contracting parties are not face to face with each other). Section 4 of *Indian Contract Act, 1872* states acceptance is complete as against the offeror, when it is put in the course of transmission; the communication of acceptance is complete as against the offeree, when it reaches the knowledge of offeror.

In e-commerce environment, there are four possible ways to convey acceptance: by sending an e-mail message of acceptance, or by delivery online of an electronic or digital product /service, or by delivery of the physical product, or by any other act or conduct indicating acceptance of the offer. The *Information and Technology Act, 2000* provides that the acceptance is binding on the offeree when the acceptance is out of his control, and binding on the offeror when he receives the acceptance. This differs from the position under the Contract Act. Section 12 of the Act provides for a default acknowledgement process, if the originator and the addressee have not agreed upon the particular method of acknowledgement. It is provided that an acknowledgement may be given by:

- any communication by the addressee (automated or otherwise) or
- any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received

Subsection 12(2) stipulates further that "*where the originator has stipulated that the electronic* *record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the electronic record shall be deemed to have never been sent by the originator*".

While this provision prima facie appears reasonable, but it can lead to unrealistic situations. To illustrate, if A sends a message and insists on an acknowledgement and B responds with an acknowledgement, but with a rider that that acknowledgement must be acknowledged, then A and B may be constantly acknowledging each other's message and may never be able to complete the loop. If one of them does not acknowledge the receipt of the other's message, then the other's message will be deemed as never sent. This may result in the previous message being deemed as never sent, which would affect the earlier message and so on! Thus such legal fiction can create issues that lead to ridiculous situations. It must be noted however, that the provisions of the *Information and Technology Act* 2000 requires that they should be interpreted in tune with the provisions regarding the manner in which offers and acceptances are communicated and revoked under the contract act.

- **Revocation of offer**

Section 5 of the Contract Act[13] states that a revocation of offer can be made at any time before the acceptance becomes binding on the offeror. [14] The position under *Information and Technology Act, 2000,* which is similar to the Model law, states that the offeror is bound by an acceptance when he is in receipt of it. Therefore, if a revocation of the offer enters the information system of the offeree before the offeror is in receipt of the acceptance, the revocation is binding on the offeree and no valid acceptance can be made.

- **Revocation of acceptance**

Under principles of contract law, the revocation of acceptance can be made only before the acceptance becomes binding on the offeree, but not afterwards. Section 5 of the Contract Act states that an acceptance may be revoked at any time before the communication of the acceptance is complete as against the acceptor, but not afterwards.

The *Information and Technology Act, 2000* and Model law differ from the Contract Act and state that an acceptance becomes binding on the offeree the moment the acceptance enters an information system outside the offeree's control.

- **Where the Contract is concluded**

The time and place of a communication are relevant to the issue whether a contract has been concluded or not. The time of the contract indicates the time from which the parties are bound to act in accordance with the contract. This is also relevant in cases where actions are time-critical. The place of contract, on the other hand, plays an important role in establishing the jurisdiction for any cause of action due to breach. Further, the time and place may be also relevant to determine whether an obligation or a condition has been performed.

Under the Contract Act, the modes to determination the time of the formation of a contract through various alternative forms of communication have examined in several cases. As regards postal contracts, a variety of theories have been propounded. They include (a) the theory that the contract is complete as soon as the offeree has made a declaration of his acceptance, (b) the theory that the contract is formed when a letter or telegram has been dispatched accepting the offer, and (c) the theory that communication of the acceptance must be received by the offeror. When the proposal and acceptance are made by letters, the contract is made at the time when and at the place where the letter of acceptance is posted.

The Contract Act does not specifically deal with where a contract is concluded but courts in India have generally been guided by the common law principles where no statutory provision to the contrary is in existence.[15] In *Entores* [16], it was held that in the case of oral communication or communication by telex or over the telephone, acceptance is communicated when it is actually received by the offeror and therefore the contract is deemed to be placed where it is received, this view was accepted by the Supreme Court of India. [17]

The question now remains whether in the case of electronic contracts, a contract is concluded when the acceptance is dispatched from the sender or when the acceptance is actually received by the offeror. The *Information and Technology Act, 2000* provides that the dispatch of an electronic record occurs when it enters an information system outside the control of the person who sent the record, unless otherwise agreed. The time for receipt of an electronic record is determined by the time when the electronic record enters the computer resource designated by the addressee or if the electronic record is sent to a computer resource not designated by the addressee, it occurs at the time when the addressee retrieves the electronic record. Alternatively, if no computer resource has been designated, then receipt occurs when the electronic record enters the "*computer resource of the addressee*"[18]. The above provision, combined with the ambiguous definition of "*computer resource",* may pose practical problems in the real world of communication, where timing is often critical (e.g. closing of bids, last time for receiving acceptances, etc). If A were to instruct B to send an acknowledgement to A's e-mail address XYZ@hotmail.com then, would A have designated a "*computer resource"* for receipt? If it were not construed as a designation of a computer resource, then would the alternative section apply (i.e. that receipt occurs when the electronic record enters the computer resource of the addressee)? What exactly would be the computer resource of the addressee? Will the message deemed to be received when the message reaches A's designated hotmail inbox at a remote server, or when A actually logs on to his hotmail service and retrieves the mail? What if A is notified that A has received a new message but A does not open his hotmail inbox and read the message? If the addressee's e-mail capability is operated on the server of a third party service provider, it could be said that e-mail is received when it arrives on that server. It would be fair to the addressee that receipt should be when the e-mail is received in the local mailbox of the addressee, or even when the addressee is notified that the e-mail has arrived or when she has also read it.

In E-commerce, more often than not, acceptance is made via email or by pressing the 'Accept' or 'Buy' icons[19]. It remains to be seen whether the Indian judiciary likens E-mail communication to that of communication by post or over the telephone. Also, in case, the acceptance is made over the Internet by clicking the 'Accept' or 'Buy' icon, the question 'where did the offeror actually receive acceptance?' still remains open. Would the acceptance be deemed to have been communicated at the place where the offeree clicks the 'Accept' icon (as the action of clicking the icon is done on the offeree's computer)? Or would it be deemed to have been communicated where the server (which actually hosts the 'Accept' icon) is located? Or would it be the place where the offeror actually reads the acceptance on his computer (which can be at different place than the location of the server)?

In Germany, judicial practice has established that a message sent by email is deemed to be received when it reaches the host computer of the addressee (if the addressee has published the email address on his visiting card or letterhead or otherwise makes it publicly known).[20]

The *Information and Technology Act 2000* Act also sets default rules for the place of dispatch and receipt of documents. The electronic records are deemed to have been dispatched at the place the originator of the message has his principal place of business and received at the place where the addressee has his principal place of business. These rules as regards "place of business" are in consonance with the rules in this regard under the UNCITRAL Model Law, and are identical to those under the Singapore legislation.

- **Law relating to written documents**

A contract may be required to be in writing or to be evidenced in writing or neither. The General

Clauses Act, 1897, in Section 3 (65) states that expressions referring to "writing" shall be construed as including references to printing, lithography, photography and other modes of representing or reproducing words in a visible form. It is doubtful whether an electronic contract would have the requisite degree of visibility required for the *General Clauses Act.* It may be arguable that information on a VDU could amount to writing as it can be viewed or even printed out. The matter is now dealt with under section 4 of *Information and Technology Act, 2000* which 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. The Article 5 of 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.

Soft copies may be accommodated under the definition of document as stated in the *General Clauses Act 1897*,Sec 3(18) that "document" shall 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 in soft copies is stored as bits and bytes; it may be argued that bits and bytes are stored in the electronic medium as zeros and ones. It can be contended that zeros and ones are figures or marks that are expressed on the disc, so that they fall within the definition of "document". If the requirement of writing were satisfied, the definition of document for the purposes of the *General Clauses Act, 1897* section, would also be satisfied since documents include any written matter.

- **Evidence**

Rights and remedies have no implication unless they can be enforced. Enforcement requires that a party prove, in accordance with the rules of evidence, that a contract existed, what were its terms were, how it was breached and to what extent such party was damaged. As such the contractual documents must be admissible to the court that is it must comply with the evidentiary standards.[21] The key to admissibility of e-commerce transactions and documents is the evidence of data integrity. A pre-condition to the admissibility of a record in the judicial proceedings is its authentication, which can be satisfied by "*evidence sufficient to support a finding that the matter in question is what its proponent claims*". Digital agreements, invoices and related e-mails and other digital communications must be authenticated with respect to it origin and accuracy of storage, retrieval and printing or other visual display. Due to the common perception that electronic file are susceptible to purposeful or accidental alteration or incorrect processing, authentication of digital evidence may require, in some situations a higher level of foundational proof that traditional evidence.[22]

Section 14 of the *Information and Technology Act 2000* provides that an electronic record would be deemed "*secure",* if "*any security procedure*" has been applied to an electronic record. It shall be deemed secure from the time the security procedure was applied up to the point in time of verification. It is not clear what could amount to a "*security procedure*" valid under this Section, though the scope seems to be very wide. A secure electronic record and a secure digital signature can avail of beneficial provisions in the amended *Evidence Act.*The *Information Technology Act,* 2000 [23] states that a file produced by techniques that accurately reproduce the original will be admissible as the original itself. This admissibility is curtailed if a *bona fide* question is raised as to the authenticity of the original. Further output readable by sight, or a printout of data is stored on a computer will be construed as original[24].

The Model law states that where the law requires information to be presented or retained in original form, that requirement is met by a data message if: (a) 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 (b) 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. The criteria for assessing integrity include the use of digital signatures. Further 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[25].

5.2 Digital Signature and Encryption

Transaction security is a significant barrier to the development of e-commerce. Parties must be able to use techniques to ensure that the business conducted over the networks will be secure. The most reliable means is through cryptography i.e. encryption and decryption techniques. Cryptography uses sophisticated mathematical algorithms, particularly a technology known as "*asymmetric cryptography*"[26]. Cryptography can be differentiated between the following:

- Use of cryptography for confidentiality of a message
- Use of cryptography in Digital Signature

The most popular and useful method of encryption for general messaging is public key[27] cryptography; i.e. encryption and decryption techniques involve the use of two kinds of keys, public keys and private keys[28], both of which are mathematically linked. One key is used for encryption and other corresponding key is used for decryption. Each user has a pair of keys, of which the private key is kept secret and the public key is open to all. Thus if X wants to send a message to Y, X will encrypt the message with Y's public key and send it to Y. The message can only be decrypted using Y's private key, which is a secret and only known to Y. Thus, only Y would be able to access the message. However, cryptography may hamper national security, as detection of espionage activities by government authorities becomes more difficult. This explains the reluctance of certain countries such as US, which does not allow the export of encryption software with key-length of more than 56 bits. It also intends to seek controls on its domestic use. At present, the Information Technology Act, 2000 regulates encryption in India through the Department of Telecommunication (DoT), which controls all aspects regarding Tele-communications[29], including encryption. As at the time of writing, permission is required from the DoT to send encrypted messages. The DoT has, while giving licenses to ISPs, permitted individuals or organizations to deploy indigenous or imported encryption equipment for providing secrecy in transmission up to a level of encryption to be specified. However, if encryption equipment of levels higher than those specified are to be deployed, individuals / groups / organizations should obtain Government clearance and shall deposit one set of keys with the authority, which the government will specify. The Indian government is moving towards evolving a national encryption policy that would facilitate e-commerce, and at the same time check cyber terrorism and laundering.

Whilst encryption provides a mechanism for providing security of content other techniques need to be used to satisfy authentification. In a written transaction the signature on the document or contract serves the purpose of authenticating the document and to identify and bind the person who signs (endorser). For contracts entered into electronically the question will be whether a digital signature, can perform the same function as a conventional signature. Signature has not been defined under Indian law. The *General Clauses Act, 1897* whilst not defining the term 'sign' extends its meaning with reference to a person who is unable to write his name to include a mark, with its grammatical variations and cognate expressions. Thus if a mark or thumb impression has been affixed to a document by a person who is able to write his name, it would not be considered as a signature[30]. Also, if the name were inserted into a document of acknowledgment in such a way as to signify that the acknowledgement was intended to be his own, such a name whether written *or printed* would constitute his signature[31]. Thus it is possible that the scanned signature or person's name may be deemed as a signature if affixed, either by the person or his agent, with intention to acknowledge his authorship.

Section 2(p) read with Section 3 of *Information Technology Act, 2000* establishes that signature could be sent using public key cryptography [32]. In order to link the identity of the sender with the signature it is necessary to attach a digital certificate,[33] which is issued by so called Certifying Authorities (CAs)[34], these confirm the identity of the sender. *The Information Technology Act, 2000* also lays down the duties of certification authorities[35], limitation of liabilities of certification authorities, and framework for regulation of certification authorities that includes appointment of controller of certification authorities, and its powers. The regulation of CAs is primarily done by the Controller of Certification Authorities ("Controller"), who is vested with the functions of licensing, certifying, monitoring and overseeing the activities of CAs. The Central Government has notified the Certifying Authority Rules ("CA Rules") on October 17, 2000, which prescribe the conditions under which CA's can apply for a license in India, and carry on their operations. The Act has adopted and extremely complex mechanism for the registration and operation of the Certifying Authorities. The approach is in stark contrast to the EU Directive on a Community Framework for Electronic Signatures[36] where certification-service-providers are free to provide their services without prior authorisation[37]. Member States may introduce voluntary accreditation schemes. This flexible approach enables member states to develop their laws to the levels of security demanded by the evolving market. The 2000 Act has tied itself to one form technology and to a cumbersome registration system that may stifle the development of e-commerce. (The UCITA, the UNCITRAL Draft Uniform Rules and the OECD principles appear to be more neutral in the choice of methods [38]). Technological developments may mean the systems in place become redundant as suppliers and consumers move to other authentification systems, possibly based around biometric systems. The Indian Parliament has legislated for a complex and cumbersome system that is far more rigid than systems adopted by it's near neighbours[39] and that is geographically isolated in an area of development that is recognised as global. It remains to be seen whether the system will significantly hinder e-commerce development in the Indian sub-continent.

Section 5 is the main provision, which provides for the legal recognition of digital signatures as a substitute for handwritten signatures. Section 5 provides also that this would be available to digital signatures, which are affixed in the manner prescribed by the Central Government. Further, Section 10 empowers the Central Government to prescribe rules regarding certain aspects of digital signatures. On the other hand, Section 15 provides that a digital signature is a "*secure digital signature"* if it can be verified using a security procedure applied by the parties concerned. A secure digital signature enjoys the benefit of certain favourable presumptions under the *Indian Evidence Act, 1872*. Section 16 provides that the Central Government shall prescribe "the security procedure", after taking into account certain prevailing commercial circumstances. However, one interpretation of Section 3 indicates that a digital signature is one, which is issued by a licensed CA. The support for this interpretation is drawn from the usage of the word "subscriber", instead of the word "person". This interpretation would necessarily mean that digital signatures, which are not issued by a licensed CA, are not recognized under the Act. However, the language of Section 15 which refers to a security procedure `*agreed between the parties'*, as distinct from one `*prescribed by the Central Government'*, leaves some room for doubt, as regards the status of digital signatures not issued by a licensed CA.

At present, the digital signature law already exists in more than 12 other countries. All these countries have Certifying Authorities who have been recognized by the respective regulatory authorities and have issued digital certificates to many of their clients. Almost all e-commerce sites in India and many individuals have obtained certificates from International (Non-Indian) Certifying Authorities like *Verisign* or *Globalsign*. Now as per *Information Technology Act 2000* this does mean that all these digital certificates invalid under the Indian Law. Even though any foreign Certifying Authority is free to apply for license in India, Sec 32 implies that such an applicant needs to maintain an office in India where the copy of the license needs to be displayed. Not all foreign Certifying Authorities would be interested in maintaining an office in India and hence may opt not to register in India. Only those companies that are interested in doing business in India would be applying for the license. As a result, a large number of digital certificate owners abroad, who are being served by niche players, would not be able to use their Digital Certificates for their transactions in India. This would in turn disable many of the Indian Certificate holders from using the digital mode of entering into contracts even if they hold valid Certificates. Further, e-commerce sites in India using digital certificates for customer identification will be unable to transact business with all those customers who hold Certificates from unrecognised Certifying Authorities, which will raise many inconvenient questions when a contract has one invalid digital signature.

Hence we feel that while enacting these provisions, it seems the lawmakers have looked at the Regulations as if all contracts are likely to be between parties within the geographical boundaries of the country, which is quite contrary to the objective of the Act and E-Commerce in general.

6 Conclusion

Electronic commerce systems operating over open systems such as the Internet can, for all intents and purposes operate outside of clear geographical boundaries. Within India, this creates potential questions concerning the applicability of the state laws to transactions that may be initiated by a consumer in one state who uses a financial institution headquartered in a second state to make payments to recipients located in yet other states, by means of a computer at some unknown location. These challenges are even greater at the international level. Financial intermediaries are no longer complacent: if innovation is the first name of the game then regulatory arbitrage is the second. Whilst the *Information Technology Act, 2000* deals with the domestic legal issues nation states may find unilateral enforcement of electronic commerce related rules difficult.

This Act is a set too far, the over complex provisions relating to contract formation, the ties to particular technology in the regulation of digital signatures, the over elaborate mechanisms for controlling certification authorities and the attempts to define the technology stand in stark contrast to more minimalist approaches adopted in other jurisdictions.

Appendices

Information and Technology Act 2000.

Chapter: 1

Chapter: 1

1.

2. Definitions-

(1) In this Act, unless the context otherwise requires,-

(a) "access" with its grammatical variations and cognate expression means gaining entry into, instruction or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "adjudicating officer" means an adjudicating officer appointed under sub-section (1) of section 46;

(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) "appropriate Government" means as respects any matter,-

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

(f) "asymmetric crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

(h) "certification practice statement" means a statement issued by a Certifying

Authority to specify the practices that the Certifying Authority employs in issuing

Digital Signature Certificates;

(i) "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulation 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 computer system or computer network;

(j) "computer network" means the interconnection of one or more computers through-

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, date, computer database or software;

(l) "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 perform logic, arithmetic, data storage and retrieval, communication control and other functions;

Chapter II: Digital Signature

3. Authentication of electronic records-

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation- For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Chapter III: Electronic Governance

4. Legal recognition of electronic records-

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 satisfied if such information or matter is-

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

5. Legal recognition of digital signatures-

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation-For the purposes of this section "signed", with the grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written or any mark on any document and the expression "signature" shall be construed accordingly.

6. Use of electronic records and digital signatures in Government and its agencies-

(1) Where any law provides for-

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in

force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-

(a) the manner and format in which such electronic records shall be filed,

created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

10. Power to make rules by Central Government in respect of digital signature-

The Central Government may, for the purposes of this Act, by rules, prescribe-

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

Chapter V: Secure Electronic Records And Secure Digital Signatures

14. Secure electronic records-

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure digital signature-

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated. then such digital signature shall be deemed to be a secure digital signature.

16. Security procedure-

The Central Government shall for the purpose of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference to their technological capacity;

(c) the volume of similar transactions engaged in by other parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications.

Chapter VI: Regulation Certifying Authorities

19. Recognition of foreign Certifying Authorities-

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purpose of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that the Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing in the Official Gazette, revoke such recognition.

21. Licence to issue Digital Signature Certificates-

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this sections shall-

(a) be valid for such period as may be prescribed by the Central Government; (b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

24. Procedure for grant or rejection of licence-

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application: Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

29. Access to computers and data-

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that nay contravention of the provisions of this Act, rules or regulations made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purpose of sub-section (1), the Controller or any person authorised by him may, by order,

direct any person in-charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures-

Every Certifying Authority shall, -

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(c) observe such other standards as may be specified by regulations.

Chapter VII: Digital Signature Certificates

35. Certifying Authority to issue Digital Signature Certificate-

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applications;

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the Certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application: Provided that no Digital Certificate shall be granted unless the Certifying Authority is satisfied that-

(a) the application holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed held by the applicant : Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Chapter XI: Offences

65. Tampering with computer source documents-

Whoever knowing or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer Programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both. Explanation.- For the Purpose of this section, "computer source code" means the listing of programmes, computer commands, design and layout and Programme analysis of computer resource in any form.

66. Hacking with computer system-

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss r damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

67. Publishing of information which is obscene in electronic form-

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Chapter XII: Network Service Providers Not Be Liable In Certain Cases

79. Network service providers not to be liable in certain cases-

For the removal of doubts, it is hereby declared that no person providing an service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.- For the purposes of this section,- (a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

---

[1] Web based contracts are termed click wrap as they are seen as the modern equivalent of shrink wrap contracts. Bainbridge, Introduction to Computer Law (4th edn, 2000) Chapter -18 Licence agreements for off-the- shelf software pg 234.

[2] *Pharmaceutical society of Great Britain v Boots Cash Chemists (Southern)* ltd. (1953) 1 QB 401.

[3] *Fenwick v Macdonald Fraser & Co*. (1904) 6 F 850. Sale of Goods Act 1930 Section 64 (India).

[4] Partridge v Crittenden(1968) 2 All ER 421.

[5] Something along the principle of *Carlill v The Carbolic Smoke Ball Co. Ltd (1893) 1 QB 256.*

[6] UNCITRAL Model Law: The UNCITRAL Model Law ("Model law") 1996 states that in the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of "data messages". Valid contracts can therefore, be formed where offer and acceptance is conveyed via Internet. The Model law defines "data message" to mean 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 telecopy.

[7] Electronic records are defined in the ITAct U/s 2(1)(t) as "electronic record" means date, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

[8] Model Law: Under the Model law, unless otherwise agreed between the offeror and the offeree, the offer will be made at the time when the data message enters any information system designated by the offeree for the purpose, or, if no system is designated for the purpose, when the data message enters the information system of the offeree, or, if any information system has been designated, and the data message is sent to some other information system, when the offeree retrieves such data message (hereinafter referred to as "Receipt of Data Message").

[9] Art 11(1) Model Law: In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose

[10] Sec 11 IT Act 2000

[11] Lodder, A.R. & Voulon, M.B. (2002),]*Intelligent agents and the information requirements of the Directives on distance selling and e-commerce*, International Review of Law, Computers and Technology, Vol. 16, No.1

[12] Subject to compliance of section 10 of the Act.

[13] Sec 5. Indian Contract Act 1872 Revocation of Proposals and acceptance A proposal may be revoked at any time before the communication of its acceptance is complete as against the proposer, but not afterwards. An acceptance may be revoked at any time before the communication of the acceptance is complete as against the acceptor, but not afterwards.

[14] *Payne v Cave* (1789)

[15] Pollock & Mulla, Indian Contract and Specific Relief Acts, Vol.1, 11th edn., N.M.Tripathi Private Ltd., Bombay, 1994. p. 6.

[16] *Entores Ltd. v. Miles Far East Corporation* (1955) 2 Q.B. 327, 332. In this case, the offer was made in Amsterdam and notification of the acceptance was received in London; the contract resulting thereupon was held to be made in London.

[17] *Bhagwandas v/s Ghirdharilal & Co* (1966) 1 S.C.R. 656.

[18] Sec 13 IT Act 2000

[19] *Hotmail Corp v Van Money Pie* C98 20064 ND Cal (20th April 1998)

[20] "Electronic Contracting with Suppliers under German Law" by Dr. Alexander Loos, pg. 5

[21] (1) the rule of authentication; (2) the hear say rule; and (3) best evidence rule.

[22] GIIC E-Commerce in India, 1999.

[23] The Second Schedule (sec 91 IT Act 2000) Amendments to the Indian Evidence Act, 1872

[24] The Second Schedule (sec 91 IT Act 2000) Amendments to the Indian Evidence Act, 1872, sec 65B: Admissibility of electronic records

[25] Art 8 Model Law

[26] U/S 2(1)(f) "asymmetric crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

[27] U/S 2(1)(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

[28] U/S 2(1)(zc) "private key" means the key of a key pair used to create a digital signature;

[29] Under Section 4 of Telegraph Act, 1885

[30] *Raghubir Singh v. Thakurain Sukhraj Kuar*, A.I.R. 1939 Oudh 96 at pg 99

[31] Within the meaning of the expression as used in Sec. 18 of Limitation Act, 1963; See pg. 236 of Swami Kaku's Commentaries on General Clauses Act, Law Publishers (India) Pvt. Ltd.

[32] Sec 3 IT Act (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

[33] U/S 2(1)"Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35.

[34] U/S 2(1)"Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24.

[35] Section 24 IT Act

[36] Directive 1999/93/EC, OJ 2000 L 13/12.

[37] Directive 99/93/ EC, rec. 10.

[38] See UCITA, ss. 102(a)(6), 107, 108; UNCITRAL Draft Uniform Rules on Electronic Signatures, art. 3; OECD Guidelines for Cryptography Policy, principles no.2-4; see also Hogg, Secrecy and Signatures, pp 53-4; H L MacQueen, M A Hogg and P Hood, `Muddling Through? Legal Responses to E-Commerce from the Perspective of a Mixed Legal System', in Grosheide and Boele Woelki (eds), Molengrafica: Euopees Privatrecht, Lelystad, 1998, pp 214-5.

[39] The Sri Lankan government has not yet legislated on digital signatures.