Presently in India the e-commerce is developing at a high speed. The conventional law doesn’t solve the problems related to e-contracts, so there is need for separate and stringent law to regulate it. This chapter is dedicated to deal with laws relating to e-contract; in addition to this various obstacles that e-contract has faced. Laws regulating e-contract are bit clear about B2B transactions but in matters of B2C, C2C and C2B they are not vivid.

In Indian context, it can be said that Information Technology Act, 2000 (hereinafter referred as IT Act) has solved some of the peculiar issues that arise in formation and authentication of electronic contracts. IT Act has brought changes to various enactments, such as, Indian Evidence Act, Indian Penal Code, Criminal Procedure Code, Reserve Bank of India Act, and some of others. Here some of the enactment enactments will be analyzed in the context of electronic contracts.

7.2. INFORMATION TECHNOLOGY ACT, 2000

Law governing electronic commerce can be divided into a number of categories. Some laws enable e-commerce by dealing with actual or perceived obstacles presented by the existing legal form like the requirements for written records and written signatures or any other impediments pertaining to admissibility in evidence of electronic records and signature. Others may regulate the detailed structure of particular electronic records and signature methods whereas certain other laws may
seek to extend or adapt existing regulation of commercial activity to cover analogous aspects of e-commerce like security, taxation, privacy etc. It is pertinent to note that many commentators are of the view that a technology neutral approach is to be followed by legal regulation, i.e. one which does not discriminate between forms of technology like paper and digital or electronic record.

A new era of trade, communication and transactions is coming to fore with the rapid development of e-commerce affecting our social and economic activities in a large way. This is on account of substantial influence that is rendered by information technology. There are a number of fundamental legal aspects that the Information Technology Act, 2000 touches upon ranging from electronic government transactions to facilitating electronic transactions per se. The policy which is embodied in the IT Act is one of recognizing both paper and electronic commerce on the same footing and maintaining a technology neutral approach.

In this segment we won’t be discussing IT Act in detail. Here we will confine ourselves to provisions dealing with e-contracts.

### 7.2.1. PREAMBLE

The Preamble of the IT Act, 2000, states that it is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ‘electronic commerce’. This may include the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government Agencies. Further, IT Act will seek to amend the Indian Penal Code, the Indian Evidence Act, the Banker’s Book of Indian Act, and the Reserve Bank of India, for related matters.
The Act, as laid down in the Preamble, also follows closely on the heels of the Model Law on Electronic Commerce adopted by the UNCITRAL. The aforementioned Model Law recommends that all States give favorable consideration to the said Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper based methods of communication and storage of information. Moreover, it has been stipulated that the said resolution may be given effect to and efficient delivery of Government services accomplished, by means of reliable electronic records. The Model Law provides a starting point for identification and discussion of areas where the law could be updated to consider new technology, as well as including certain internationally settled provisions for dealing with those issues and:

- Establish rules that validate and recognize contract contracts formed through electronic means;
- Sets default rules for contract formation and governance of electronic contract performance;
- Defines the characteristics of a valid writing and an original document;
- Provides for the recognition of electronic signatures for legal and commercial purpose; and
- Supports the admission of computer evidence in courts and arbitration proceedings.

### 7.2.2. STATEMENT OF OBJECTS AND REASONS

Day to day living, and the way we conduct business and trade has been dramatically altered by the growth and development of new technology and communications systems. This revolution is being led by computers and internet, which are being used by businesses and consumers on an
increasingly large scale as a substitute for the traditional paper based system of information creation and transmission. The advantages are apparent, speed and cost effectiveness being the major plus points. In spite of these advantages the lack of a clear legal framework had dissuaded many people from using this medium to conduct transactions using the electronic form. The biggest roadblock in the way to electronic commerce and its growth, speaking from a legal as well as a practical standpoint is that standard evidentiary practice is based on oral testimony and paper records coupled with this are the requirements as to writing and signature for legal recognition. Substantial changes in the legal system or existing legislation thus become top priority as e-commerce eliminates the need for paper based transaction. Moreover e-commerce has fuelled the growth of International Trade, which has resulted in a number of countries making the shift from the traditional paper based commerce to electronic commerce.

7.2.3. OBJECTIVES

The IT Act aims to give legal recognition in place of paper based methods of communications to transactions carried out by means of electronic data interchange and other means commonly referred to as e-commerce. Digital signatures are to be recognised as legal modes of authentication of any information that requires authentication under law. Among the main objectives of the Act is also the facilitation of electronic filing of documents, storage and transfer of data and to give recognition for keeping of books account by Bankers.

7.2.4. SCHEME

The first 17 sections of the IT Act are largely based on the UNCITRAL Model Law. It contains 94 clauses divided into XIII Chapters. It has 4
schedules. The Schedule I seeks to amend the Indian Penal Code; Schedule II Seeks to amend the Indian Evidence Act; Schedule III seeks to amend the Banker’s Book Evidence Act; and Schedule IV seeks to amend the Reserve Bank of India Act. Fourteen of the provisions deal with some aspects or other of digital signatures, and nineteen with private certifying authorities who will be licensed to issue digital signature certificates and the Controller, Deputy Controller and Assistant Controller who will be public servants licensing and supervising the work of the certifying authorities. Sections 65 to 79 of the IT Act set out the offences which will result in criminal liability which may entail imprisonment and/or fine, while Sections 43, 44 and 45 of the IT Act provide for penalties and compensation to be adjudicate by the adjudicating officers [Sections 46 and 47]. Appeals against the orders of the adjudicating authorities are to be made to the Cyber Regulations Appellate Tribunal and thereafter to the High Court. Section 48 to 64 of the IT Act deal with the Tribunal, appeals to the High Court and the compounding of contraventions of the law.

The IT Act deals with the concepts of Electronic Governance, Digital Signatures, Digital Signature Certificates, Electronic Records and Regulation of Certifying Authorities and will go a long way in facilitating and regulating e-commerce. Additional, Guidelines on Internet based trading and services have been prescribed.

7.2.5. RELEVANT PROVISIONS GOVERNING E-CONTRACTS

7.2.5.1. ELECTRONIC SIGNATURES

Electronic or Digital Signatures consist of cryptographic techniques which ensure privacy and verify the origin and integrity of the message; the techniques commonly used are a mix of algorithms, keys and codes. Symmetric cryptography uses just a single key to encrypt and decrypt the
messages, on the other hand asymmetric technique uses two keys one of which is public (because it is known by the parties) and one, which is private (just one of the parties knows it). Most modern signatures are based on asymmetric methods, described as a special door that can only be opened with four key lock, two on either side. Once both parties have locked the keys into the door, it is possible to open door and for the parties to be sure that they can negotiate through that open door safely.\(^{55}\)

Signatures serve the purposes of evidence,\(^{56}\) approval,\(^{57}\) and efficiency and logistics.\(^{58}\) To achieve these basic purposes a digital signature must be capable of Signer and Document authentication,\(^{59}\) these methods are tools used to exclude impersonators and forgers and are essential ingredients of what is often called non-repudiation service. This prevents a person from unilaterally terminating or making modifications to legal obligations arising out if a computer based transactions.\(^{60}\)

Authentication of electronic records is dealt with under Section 3 of IT Act, by way of affixing an electronic signature. It is stipulated that such authentication shall be achieved by using the asymmetric crypto system and hash function\(^{61}\) whereby the initial electronic record is transformed


\(^{56}\) A signature authenticates writing by identifying the signer with the signed document. When the signer makes distinctive mark it becomes attributable to the signer; cited by *Id*.

\(^{57}\) A signature expresses the signer’s approval or authorization of the writing, or his intention that the document has legal effect; cited by *Id*.

\(^{58}\) A signature on a written document imparts a sense of clarity and finality; cited by *Id*.

\(^{59}\) A signature should indicate who signed a document or record at the same time making it difficult for another to produce it without authorization. Identification of what is signed is also essential in order to make it impracticable to falsify or alter either the signed matter of the signature without detection; cited by *Id*.

\(^{60}\) *ibid*.

\(^{61}\) For the purpose of this section, ‘hash function’ means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as ‘hash result.’
into another electronic record. Thus, digital requirements should possess, as minimum requirements, the following characteristics:

- A crypto system which is asymmetric
- The initial electronic record transforming into another electronic record
- Hash function and hash result
- The hash function’s stability
- The hash function’s safety
- Public Key and Private Key

The digital signature is created by the formation of two steps:62

- The electronic records is converted into a message digest by using a mathematical function known as ‘hash function’ which digitally freezes the electronic record thereby ensuring the integrity of the content of the intended communications that the electronic record contains. A digital signature will be rendered invalid if the contents of such electronic record are tampered with.
- Secondly, by way of a private key, this attaches itself to the message digest and which can be verified by anyone who has the public key (corresponding to such private key), the identity of the person affixing the digital signature is authenticated.

A signature is not part of the substance of a transaction, but rather of its representation or form. Signing documents serve the following purposes:

- **Evidence:** A signature authenticates writing by identifying the signer with the signed document. When the signers make a mark in a distinctive manner, the writing becomes attributable to the signer.

- **Ceremony:** The act of signing a document calls to the signer’s attention the legal significance of the signer’s act hereby helps prevent ‘inconsiderate engagements’.

- **Approval:** In certain contexts defined by law or custom, a signature expresses the signer’s approval or authorization of the writing or the signer’s intention that it has a legal effect.  

A new Section 3A is inserted after Section 3 by amendment to the IT Act in the 2009. The amended Act is called the Information Technology (Amendment) Act, 2008. Section 3A explains about Electronic Signature as under:

1) Notwithstanding anything contained in Section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-
   
   a) is considered reliable; and

   b) may be specified in the Second Schedule.

2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-

   a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

---

63Ibid.
b) the signature creation data or the authentication data were at the time of signing, under the control of the signatory or, as the case may be the authenticator and of no other person;

3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that the person by whom it is purported to have been affixed or authenticated.

4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:
   Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.

7.2.5.2. E-CONTRACT

Chapter IV of IT Act contains provisions relating to electronic contracting. Sections 11, 12 and 13 deals with Attribution, Acknowledgment and Dispatch of Electronic Records respectively.
Attribution of Electronic Records

In the following circumstances, Section 11 mandates that the electronic record in the given context is required to be attributed to the originator:

1) If the record was sent by the originator himself or herself or
2) If the record sent by a person who was authorized by the originator to act so with regard to specific record or
3) By a system which was programmed either by the originator or by any person who is authorized to do so to operate automatically or otherwise.

This section can best be understood with the help of suitable illustrations.

Illustration 1: Pooja logs in to her web-based gmail.com email account. She composes an email and presses the “Send” button, thereby sending the email to Sameer. The electronic record (email in this case) will be attributed to Pooja (the originator in this case) as Pooja herself has sent it.

Illustration 2: Pooja instructs her assistant Siddharth to send the above-mentioned email. In this case also, the email will be attributed to Pooja (and not her assistant Siddharth). The email has been sent by a person (Siddharth) who had the authority to act on behalf of the originator (Pooja) of the electronic record (email).

Illustration 3: Pooja goes on vacation for a week. In the meanwhile, she does not want people to think that she is ignoring their emails.

---

64 According to section 2(1)(za) of the IT Act, originator is a person who:
1. sends, generates, stores or transmits any electronic message or
2. causes any electronic message to be sent, generated, stored or transmitted to any other person.

The term originator does not include an intermediary.

Illustration: Pooja uses her gmail.com email account to send an email to Sameer. Pooja is the originator of the email (Gmail.com is the intermediary).
She configures her gmail.com account to automatically reply to all incoming email messages with the following message:

“Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back”.

Now every time that gmail.com replies to an incoming email on behalf of Pooja, the automatically generated email will be attributed to Pooja as it has been sent by an information system programmed on behalf of the originator (i.e. Pooja) to operate automatically.

**Acknowledgment of Receipt**

According to Section 12(1) of the IT Act, where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by—

a) any communication by the addressee, automated or otherwise; or

b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

This sub-section provides for methods in which the acknowledgment of receipt of an electronic record may be given, provided no particular method has been agreed upon between the originator and the recipient. One method for giving such acknowledgement is any communication (automated or otherwise) made by the addressee in this regard.

---

65 According to section 2(1)(b) of the IT Act, Addressee means a person who is intended by the originator to receive the electronic record but does not include any intermediary. **Illustration:** Pooja uses her gmail.com email account to send an email to Sameer. Pooja is the originator of the email. Gmail.com is the intermediary. Sameer is the addressee.
Illustration: Let us go back to the earlier example of Pooja going on vacation for a week. She has configured her email account to automatically reply to all incoming email messages with the following message

“Thanks for your email. I am on vacation for a week and will reply to your email as soon as I get back”.

The incoming message is also affixed at the bottom of the above-mentioned message.

Now when Siddharth sends an electronic record to Pooja by email, he will receive Pooja’s pre-set message as well as a copy of his own message.

This automated communication will serve as an acknowledgement that Pooja has received Siddharth’s message.

Another method is any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received. Let us take another illustration.

Illustration: Rohit sends an email to Pooja informing her that he would like to purchase a car from her and would like to know the prices of the cars available for sale. Pooja subsequently sends Rohit a catalogue of prices of the cars available for sale.

It can now be concluded that Pooja has received Rohit’s electronic record. This is because such a conduct on the part of Pooja (i.e. sending the catalogue) is sufficient to indicate to Rohit (the originator) that his email (i.e. the electronic record) has been received by the addressee (i.e. Pooja).
According to section 12(2) of the IT Act, it says where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

**Illustration**: Suppose Priya wants to sell a car to Sam. She sends him an offer to buy the car. In her email, Priya asked Sam to send her an acknowledgement that he has received her email. Sam does not send her an acknowledgement. In such a situation it shall be assumed that the email sent by Priya was never sent.

According to section 12(3) of the IT Act, where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

**Illustration**: Rohit sends the following email to Sameer:

*Further to our discussion, I am ready to pay Rs. 25 Lakh for the source code for the PKI software developed by you. Let me know as soon as you receive this email.*

Sameer does not acknowledge receipt of this email. Rohit sends him another email as follows:
I am resending you my earlier email in which I had offered to pay Rs 25 lakh for the source code for the PKI software developed by you. Please acknowledge receipt of my email latest by next week.

Sameer does not acknowledge the email even after a week. The initial email sent by Rohit will be treated to have never been sent.

**Time and Place of Dispatch and Receipt**

As per section 13(1) of the IT Act, save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

**Illustration:** Shashi composes a message for Raj at 11.56 a.m. At exactly 12.00 noon she presses the “Submit” or “Send” button. When she does that the message leaves her computer and begins its journey across the Internet.

It is now no longer in Shashi’s control. The time of dispatch of this message will be 12.00 noon.

Section 13(2) of the IT Act Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:—

a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—
   (i) receipt occurs at the time when the electronic record enters the designated computer resource; or
   (ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource,
receipt occurs at the time when the electronic record is retrieved by the addressee;
b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

**Illustration:** The marketing department of a company claims that it would make the delivery of any order within 48 hours of receipt of the order. For this purpose they have created an order form on their website. The customer only has to fill in the form and press ‘submit’ and the message reaches the designated email address of the marketing department.

Now Suresh, a customer, fills in this order form and presses submit. The moment the message reaches the company’s server, the order is deemed to have been received.

Karan, on the other hand, emails his order to the information division of the company. One Mr. Sharma, who is out on vacation, checks this account once a week. Mr. Sharma comes back two weeks later and logs in to the account at 11.30 a.m. This is the time of receipt of the message although it was sent two weeks earlier.

Now suppose the company had not specified any address to which orders can be sent by email. Had Karan then sent the order to the information division, the time of receipt of the message would have been the time when it reached the server of the company.

As per section 13(3) of the IT Act, save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
**Illustration:** Keshav is a businessman operating from his home in Pune, India. Keshav sent an order by email to a company having its head office in New York, USA.

The place of dispatch of the order would be Keshav’s home and the place of receipt of the order would be the company’s office.

Section 13(4) of the IT Act says that, the provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

Illustration: Let us consider the illustration mentioned above of Keshav and the New York based company. Even if the company has its mail server located physically at Canada, the place of receipt of the order would be the company’s office in New York USA.

With regard to place of business Section 13(5) of the IT Act provides following explanation—

a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;
b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
c) “usual place of residence”, in relation to a body corporate, means the place where it is registered.

**Illustration:** Suraj sent an order by email to a company having its head office in New York, USA. The company has offices in 12 countries. The place of business will be the principal place of business (New York in this case).
Suraj is a businessman operating from his home in Pune, India. He does not have a separate place of business. Suraj’s residence will be deemed to be the place of business.

7.3. LEGAL ISSUES

7.3.1. INDIAN EVIDENCE ACT, 1872

Enactment of Information Technology Act brought certain regulation over cyberspace. As it is known to everyone that the contracts are admissible as evidence in court of law, therefore, the question arises that whether electronic contracts can be admitted as evidence? The answer to this question was given by IT Act itself in Section 92 and Schedule II. In this segment we will deal all relevant sections of Evidence Act, 1872.

Section 17

This section defines Admission. It says, an admission is a statement, oral or documentary, or contained in electronic form which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances.

Lucknow Court explained ‘admission’ as, it is a statement of fact which waives or dispenses with the production of evidence by conceding that the fact asserted by the opponent is true. Admissions are admitted because the conduct of a party to a proceeding, in respect to the matter in dispute, whether by acts, speech, or writing, which is clearly inconsistent with the truth of his contention, is a fact relevant to the issue.

Same way the e-contracts are admissible as above stated.

66Latefat Husain v. Lala Onkar Mal, (1934) 10 Luck 423
Section 22A

Section 22A\(^{67}\) is a newly inserted section in the Evidence Act. The purpose of the new section is to provide for the circumstances in which an oral admission could be proved as to the contents of an electronic record. The section disallows the evidence of oral admission as to the contents of an electronic record. It then talks of an exceptional situation, which is that when the genuineness of the electronic record produced before the court is itself in question. The section says that oral admissions as to the contents of an electronic record may be proved in evidence when the genuineness of the record has been questioned.

Section 39

According to Section 39\(^{68}\) of Evidence Act, when any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.

When evidence is given of a statement which forms part of (a) a longer statement, or (b) a conversation, or (c) an isolated document, or (d) a document contained in a book, or (e) series of letters of papers, or (f)

\(^{67}\) Section 22A of the Indian Evidence Act, 1872 says, Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.

\(^{68}\) This Section has been totally substituted because of the amendment introduced under the Information Technology Act, 2000.
electronic records, the Court has discretion as to how much evidence should be given of the statement, conversation, document, book, or series of letters or papers for the full understanding of the nature and effect of the statement and the circumstances under which it was made. The principle on which this section is based is that it would not be just to take part of a conversation, letter, etc., as evidence against a party without giving to the party at the same time the benefit of the entire residue of what he wrote or said on the same occasion. Thus, the rule enacted in this section will not warrant the reading of distinct entries in an account book, or distinct paragraphs in a newspaper, unconnected with the particular entry or paragraphs relied on by the opponent.69

Section 47A70

This new section has been added so as to provide for relevancy of expert opinion the genuineness of an electronic signature. The new provision says that when the court has to form an opinion as to the electronic signature of any person, the opinion of the certifying authority which has issued the Electronic Signature Certificate is a relevant fact. A ‘certifying authority’ means a person who has been granted a license to issue an electronic signature certificate under the Section 2471 of the IT Act, 2000.

70 Section 47A of the Indian Evidence Act, 1872 says, when the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.
71 Section 24 of the Information Technology Act, 2000 says, 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 license 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.
Sections 65A and 65B

The new section, namely Section 65A, says that the contents of electronic records may be proved in accordance with the provisions of Section 65B. This section is also a new provision. It prescribes the mode for proof of contents of electronic records. The primary purpose is to sanctify proof by secondary evidence. This facility of proof by secondary evidence would apply to any computer output, such output being deemed as a document. A computer output document for the purposes of proof. The section says in sub-section (1) that any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer and to be referred to as computer output, shall also be deemed to be a document. The section lays down certain conditions which have to be satisfied in relation to the information and the computer in question. Where those conditions are satisfied, the electronic record shall become admissible in any proceedings without further proof or production of the original as evidence of any contents of the original or of any fact stated in it.

The conditions which have to be satisfied so as to make a computer output as evidence are stated in sub-section (2) of Section 65B. They are as follows:

a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so
contained is derived was regularly fed into the computer in the ordinary course of the said activities;

c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Where the information was processed or fed into the computer on interlinked computers or one computer after the other in succession, all the computers so used shall be treated as one single computer. The references to a computer have to be construed accordingly Section 65B:

When a statement has to be produced in evidence under this section, it should be accompanied by a certificate which should identify the electronic record containing the statement and describe the manner in which it is was produced, give the particulars of the device involved in the production of the electronic record showing that the same was produced by a computer and showing compliance with the conditions of sub-section (2) of Section 65B. The statement should be signed by a person occupying a responsible official position in relation to the operation or management of the relevant activities. Such statement shall be evidence of the matter stated in the certificate. It should be sufficient for this purpose that the
statement is made to the best of knowledge and behalf of the person making it.\textsuperscript{72}

For the purpose of Section 65B information shall be taken to be supplied to a computer, if it is done in any appropriate form whether this is done directly with or without human intervention by means of any appropriate equipment, or if the information is supplied by any official in the course of his activities with a view to storing or processing the information even if the computer is being operated outside those activities.\textsuperscript{73}

\textbf{Section 67A}

This is a newly inserted section, it talks about proof as to digital signature. It declares that, except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.

\textbf{Section 73A}

Again a new section is introduced after Section 73 namely Section 73A.\textsuperscript{74} For the purpose of ascertaining whether a digital signature is that of the person by whom it purports to have been affixed, the court may direct that person or the controller or the certifying authority have to produce the

\textsuperscript{72}Section 65B of Indian Evidence Act, 1872
\textsuperscript{73}An explanation to the Section 65B declares that for the purpose of this section any reference to information being deprived from other information is to be taken to mean derived by calculation, comparison or any other process.
\textsuperscript{74}Section 73A of the Indian Evidence Act, 1872 says, in order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—
\hspace{10pt} a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
\hspace{10pt} b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.
digital signature certificate. The court may also direct any other person to apply the public key listed in the digital signature certificate and verify the digital signature purported to have been affixed by that person. For this purpose the ‘controller’ means the controller appointed under Section 17(1) of the Information Technology Act, 2000.

Section 81A

As per Section 81A the court has to presume the genuineness of any electronic record purporting to be the Official Gazette or purporting to be the electronic record direct by law to be kept by a person. It is necessary that the electronic record is substantially kept in accordance with the form required by the law and is produced from proper custody.

Section 85A

Under this section presumption is available to the court that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

Section 85B

In any proceeding involving a secure electronic record, the court has to presume, unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

Sub-section (2) provides that in any proceeding involving secure digital signature, the court has to presume unless the contrary is shown, that the secure electronic signature was affixed by the subscriber with the intention of signing or approving the electronic record. This presumption is to be
confined only to secure electronic record or to secure electronic signature. Sub-section (2) says that except in the case of a secure electronic record or a secure electronic signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature. Secure system is defined in Section 2(ze) of the IT Act.\(^7\)

**Section 85C**

Another presumption is available to court that, unless contrary is proved, that the information listed in an Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

**Section 88A**

The section provides that the court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

The explanation to the section explains the meaning of the terms ‘addressee’ and ‘originator’. It says that these terms will have the same

\(^7\) Section 2(ze) of the Information Technology Act, 2000 says, “secure system” means computer hardware, software, and procedure that—

a) are reasonably secure from unauthorised access and misuse;

b) provide a reasonable level of reliability and correct operation;

c) are reasonably suited to performing the intended functions; and

d) adhere to generally accepted security procedures;
meaning as is assigned to them in clauses (b)\textsuperscript{76} and (za)\textsuperscript{77} of Section 2(1) of the Information Technology Act, 2000.

**Section 90A**

Where an electronic record purports to be or is proved to be five years old and is produced from any proper custody which the court considers proper in the particular case, the court may presume that the electronic signature which purports to be the electronic signature of any person was so affixed by him or by any person authorized by him in the behalf.

Defining the expression ‘proper custody’ the explanation to the section says that electronic records are said to be in proper custody if they are in the place in which and under the care of the person with whom they would naturally be; but that no custody is improper if it is proved to have had a legitimate origin or the circumstances of the particular case are such as to render such an origin probable.\textsuperscript{78}

**Section 131**

This section has been substituted for the purpose of accommodating electronic records along with documents. The new section says that no one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to

---

\textsuperscript{76}Section 2(b) of the Information Technology Act, 2000 says, ‘addressee’ means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

\textsuperscript{77}Section 2(za) of the Information Technology Act, 2000 says, ‘originator’ means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

\textsuperscript{78}This explanation also applies to the presumption under Section 88A of the Evidence Act.
refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.

Persons normally in possession of documents on behalf of other are generally agents, attorneys, mortgagees, trustees, etc. This section is extends to these persons the same protection which the Section 130 provides for a witness who is not party to a suit.

To end with, it can be said that electronic contracts are almost same as other hard copy contracts as far as its evidentiary value is concerned and in case of any discrepancy there are certain prerequisites that fill the lacunae. All electronic contracts are valid contracts as they are legalized by the Information Technology Act and one could be made liable if there is any infringement with the terms and conditions. Subsequently many amendments have been brought, in order to attain conceptual clarity.

7.3.2. ONLINE CONTRACTING & IMPEDIMENTS TO JUDICIARY

Judiciary is one of the pillars of democracy. It is the judiciary which interprets the law. It is the judiciary which declares vires of legislations. Law relating to e-contract is of recent origin, it is more or less techno-legal in nature. Present judicial system works under settled legal environment. Therefore courts require assistance from experts on all technical issues. Further Section 45 of Indian Evidence Act, 1872 speaks about expert opinion. It is read as under,

When the Court has to form an opinion upon a point of foreign law, or of science, or art, or as to identity of handwriting or finger impressions, the opinions upon that point of persons specially skilled in such foreign law, science or art, or in questions as to identity of handwriting or finger impressions are relevant facts. Such persons are called experts.
Therefore Courts can certainly take expert opinion from person who is well versed in computer and internet. It is the well settled principle of law that the expert opinion is not binding on courts. Even if courts take any opinion from expert still it has to come to its own independent conclusion. This sort of situations would cause some impediments in adjudicating process.

Order XIII of Code of Civil Procedure, 1908 seeks marking of documents. In e-contract there are no documents. As per Evidence Act one has to submit primary document. Courts in India decide almost all civil cases on the basis of primary documents. As we don’t find primary documents in e-contract, so it is bit difficult for judiciary to decide cases relating to online contracts.

Although legislatures have enacted IT Act, 2002, it is substantive law. IT Act is of its own kind which includes both legal and technical provisions. To tackle techno-legal issues we need well establish procedural law to support substantive law. IT Act is substantive law which deals with rights and liabilities of parties, whereas not such law is enacted so as to deal with procedure. By not enacting procedural law for IT Act the legislators have created hurdle for enforcement of IT Act. Even this hurdle applies to judiciary too. Without clear procedure it is difficult for judiciary to interpret law upto the mark. We have CPC for civil law and CrPC for criminal, then why not ITPC i.e. “Information Technology Procedure Code”.

As disputes pertaining to e-contract are techno-legal issues, it is difficult for a Judge or an adjudicator to be expert in these matters. The modern day judges are not so well acquainted with all these issues. Hence, they require training so as to update and upgrade their skill and knowledge pertaining to realm of cyber law.
Apart from above stated things there must also be special provisions for training of courts staff and advocates about the intriguing issues of e-contract and cyber law. Further in disputes pertaining to e-contract most of the data would be in electronic format, special provision must also be made for saving, retaining and retrieving e-data when it is presented before the Court.

**7.3.3. LEGISLATIVE SETBACKS**

It is been almost a decade since IT Act was enacted. There have been infinite changes in field of technology and there have been new developments in e-commerce. Further it is almost 140 years since Indian Contract was enacted, it is worth enough to mention, that this enactment has been amended on only few occasions. It is cardinal principle of law that, with changing society, law should also be changed. If law remains static it is difficult for the enforcing machinery to enforce.

The IT Act enacted in India is total verbatim of UNCITRAL Model Law. In IT Act there is nowhere reference about the contract. Whole of IT Act is enacted keeping in mind about cybercrimes. The legislators while enacting did not consider e-commerce as important aspect. Sections 11-13 deal bit about dispatch and receipt of e-document, which are applied to contracts. As such there is no specific chapter in IT Act which states law relating to contract. The UNCITRAL Model Law is holds good for developed countries. As India being developing country the UNCITRAL Model Law doesn’t suits to its needs.

Further it can be said that while dealing with online contracts one has to consider both IT Act and Contract Act. It is already made clear that the Contract Act is a very old law; it was enacted in an era wherein inventions like, mobile, telephone or internet were not available. It is the opinion of
most of the jurists that traditional principles of contract law are applicable to e-contract. For certain extent this opinion can be accepted, but now time has changed and now there is need for change in existing law of contract. In UK, since enactment of first law on contract many changes have been brought in to contract law, and from time to time they have changed their laws. Whenever necessary they have re-enacted law relating to contract. At the latest in UK, there is a new enactment for liability of third parties in contract. When we look at the Indian conditions, it is regretful to say that the legislators have failed in updating contract with changing conditions, i.e. technological development.

Not only Indian Contract Act alone which was not amended while enacting IT Act, but also the allied legislations to Contract Act, such as, Specific Relief Act, Sale of Goods Act, Carriage of Goods Act, Partnership Act, Consumer Protection Act, Insurance Act, Code of Civil Procedure and Evidence were not amended.

Sale of Goods Act, deals about the sale of movable goods. In this internet era, online shopping has become fashion. People like to do shopping online sitting at their homes. It is necessary to mention here that normally people never intend to shop online, but while surfing they shop just for fun, without understanding the consequences of such transactions. In most of the cases, people will be shopping without intention. There are issues involving in these types of contracts, firstly, these retail contracts are based on standard form of contracts, which are unilateral in themselves. These agreements are one sided boilerplate drafted by the seller. Secondly, there will be a separate contract with a remote manufacturer, that consumers are provided opportunity to see their goods only after receipt or delivery of same. Thirdly, there are likely chances of getting deceived in these types of retail contracts. Fourthly, the seller will
be always including disclaimer clause in his agreement. For these forms of techno-legal issues the Sale Goods Act, doesn’t provide any answer. So there is high need for bringing changes to current Sale of Goods Act, 1930.

It is suggested here that contract law in India requires amendment on par with technological development. The legislatures should learn lessons from the developed countries, because those countries will be updating their laws with changing trends.

7.3.4. MISCELLANEOUS ISSUES

7.3.4.1. JURISDICTION

A. PLACE OF FORMATION

For determining the jurisdiction of the Court in a dispute between the contracting parties, it is necessary to know where the contract in question was concluded. The place of formation of the contract determines the jurisdiction of the court where breach of contract gives rise to cause of action. It is well settled principle that contract concludes, (a) where letter of acceptance is posted in case of postal communication and (b) where letter of acceptance is received where instantaneous means of communication has been used.

Quite different from the above two rules, the IT Act lays down rules for place of dispatch and receipt of electronic records which may not necessarily by the actual place of dispatch or receipt of the electronic record. Furthermore, it is quite possible that a contract may be actually concluded at a place different from that where the electronic record is deemed to be received. The IT Act has laid down an objective test which is the place of business of the originator or that of the addressee where an electronic record is deemed to have been dispatched or received as the
case may be. The location of the computer resource is not a determining factor. In a given situation the computer resource of the originator or addressee used for the dispatch or receipt of the electronic record, may be located in a jurisdiction other than that in which the originator or addressee has a place of business. Further, parties may not be aware of the location of the computer resource used for dispatch or receipt of the electronic record. To address this uncertainty, precise test has been laid down which takes into account pace of business, regardless of the location of the computer resource. However, contracting parties are free to agree on a different rule.

The Courts in India will be called to determine the compatibility of the above provision with Section 20 of the Civil Procedure Code. It appears that the scope of ‘cause of action’ as a possible ground for filing a suit in a particular court has been reduced. Section 20 of the Civil Procedure Code, inter alia, provides that every suit shall be instituted in a court within the local limits of whose jurisdiction defendant(s) carries on business or where cause of action wholly or partly arises. The breach of contract gives rise to a cause of action and suit in such case may be instituted under Section 20 of CPC either in place where contract is formed or where defendant carries on business. But the IT Act fuses place of formation of the contract with the place of business and lays down that the place of business shall be deemed as the place of dispatch or receipt of the electronic record as the case may be. This means that the place of business shall be a place where a case has to be instituted in case of breach of contract which may not be necessarily the place where the contract has been concluded.

B. JURISDICTION

A cyberspace transaction knows no national or international boundaries, and is not analogous to three dimensional world in which Common Law
principles developed. From the beginning of internet, the issue of jurisdiction has continued to challenge legal minds, societies and nations in the context of the peculiarly inherent character of internet. Different principles were being evolved in different national jurisdictions in this regard.

The e-commerce applications of internet are limitless and the jurisdictional issues spawned by it are many and diverse. However, it is not the end, once e-commerce applications of internet are unfolded to its potential, jurisdictional issues likely to emerge may not be forceable at present. It is quite possible that the supplier and customer may be residing in two different countries. The questions which are likely to arise are: which country has the jurisdiction in case of dispute? Whether the laws of the country in which customer resides or the laws of the country in which supplier resides, apply? How to enforce judgment?

Considering the entire issue of jurisdiction from the Indian perspective, there is, by far, no established principle. Section 19 of the Code of Civil Procedure is a provision under the Indian context which clarifies the position in case of domestic level multiple jurisdictions.

Section 19 provides that, ‘where a suit for compensation for wrong done to the person or to moveable done to the person or to moveable done to the person or to moveable property, if the wrong was done within the local limits of the jurisdiction of one court and definition resides, or carries on business, or personally works for gain, within the local limits of jurisdiction of another court, the suit may be instituted at the option of the plaintiff in either of the said courts’

There is nothing harm in applying above principle to internet contracts. As it is already discussed jurisdictional issues in India are determined either
by the place of residence or place of business or cause of action. The first is an objective one and easy to determine. The ‘cause of action’ jurisdiction to pose serious issue in e-commerce disputes. The cause of action jurisdiction is a subjective and is most likely debated in e-commerce cases.

It appears that Section 13 of the IT Act is not in harmony with Section 11 of the Consumer Protection Act, 1986. Section 13 of IT Act provides that where the originator (offeror here) or the addressee (offeree here) has more than one place of business, then principle place of business shall be deemed as the place where the electronic record has been dispatched or received as the case may be. The place of business will determine the jurisdiction of the court and in case there is dispute between the parties involving contract formed electronically, then the suit shall be in the court within the local limits of whose jurisdiction, inter alia, principal place of business of the opposite party is situated.

Against this, the Consumer Protection Act provide that a consumer can file a complaint against the opposite party in a District Forum within the local limits of whose jurisdiction the opposite party inter alia, has a branch office. There is an apparent conflict between the two provisions and rule incorporated in Section 13 is likely to cause inconvenience to the consumers especially where the opposite party has principle office outside India—an inconvenience which the Consumer Protection (Amendment) Act, 1993 removed by incorporating the present rule. 79

79 The present rule was incorporated in the Consumer Protection Act after the decision of the National Commission in Indian Airlines Corporation v. Consumer Education and Research Society, Ahmadabad, (1991) 3 Comp. LJ 166 (NCDRC), where it was laid down that a complaint cannot be filed in a district forum within the local limits of whose jurisdiction opposite party has only branch office. The amendment was suggested in the report submitted by the Working Group to make necessary amendments to Consumer Protection Act and MRTP Act, 1969
The above mentioned possible conflict could be avoided if the expression, ‘the place of business is that which has the closest relationship to the underlying transactions,’ incorporated in the IT Act along with expression ‘principle place of business’, presently provided.80

Next question arises, whether access to website give rise to the cause of action and consequent jurisdiction to the court within the local limits of whose jurisdiction website has been accessed?

The cause of action means every fact that it would be necessary for the plaintiff to prove, if transverse, in order to support his right to judgment of the court.81 It does not include every piece of evidence which is necessary to prove each fact, but every fact which is necessary to be proved. Even an infinitesimal fraction of a cause of action will be a part of cause of action and will confer jurisdiction on the court within the territorial limits of which that little occurs.82

It has been made clearly by the judicial gloss that the formation of the contract is a part of the cause of action and where suit is for damages for breach of the contract, it can lie at any place where the contract was made, notwithstanding that the place where the contract was to be performed and the place where the breach alleged in the plaint occurred, are both outside such jurisdiction.83 The place where a contract is concluded will be either the place where acceptance is posted or where a contract is concluded will be either the place where acceptance is posted or where acceptance is received depending upon the medium of communication

80 Farooq Ahmad, Cyber Law In India, 2nd Ed, New Era Law Publications, Delhi, 2005, p. 236
81 S.S. Mittal v. Bar Council of India, AIR 1974 HP 32
82 Lijjal v. Netai Chand, AIR 1969 Cal 224
83 A.B.C. Laminant v. A.P. Agencies, AIR 1989 SC 1239
used. However, as already discussed, in case of e-contracts, place of business or place of residence, as the cases may be, will be deemed as a place of contract formation, notwithstanding that the contract may actually be concluded at a different place.

After the initial disagreement expressed by the courts regarding the offer forming part of the cause of action, the controversy has been now set at rest by the Apex Court in *A.B.C. Laminant v. A.P. Agencies*,84 wherein it was laid down that making of an offer on a particular place does not form cause of action in a suit for damages for breach of contract. Ordinarily, acceptance of an offer and its intimation to the offeror results in a contract and hence a suit can be filed at the place where the contract should have been performed or its performance completed. If the contract is to be performed at the place where it is made, the suit on the contract is to be filed there and nowhere else.

Answering to the issue whether an access to website can give rise to a cause of action can be found on the basis of above discussion. There is near consensus to regard information available on the internet as an invitation to offer unless contrary intention may be inferred. The court, as stated above, has declined to consider offers as a part of the cause of action. Invitation to treat is much less in degree that the offer. If offer does not give rise to the cause of action, the question of invitation to treat forming part of the cause of action does not arise. Thus, whether information on website is construed offer or invitation to treat, mere access to web site cannot give rise to the cause of action. However, it should be differentiated from a situation where information itself gives rise to the cause of action.

84 AIR 1989 SC 1239
As mentioned already, the transaction of business over internet is possible beyond the national borders. Can a person domiciled in India file which arises within India and can a person domiciled in India file a suit against a non-resident foreigner who is carrying business through his agent in India on a cause of action that arises outside India?

As regards the first question the Allahabad High Court has in *Gaekwar Baroda State Rly v. Habibullah*, made it clear that the language of Section 20 of the Civil Procedure Code is wide and flexible enough to cover the cases of non-resident foreigners whose cause of action arose within India and there is nothing which makes an exception as regards them. However, the Court cautioned that the sanctity of the discussion in a foreign country should not be confused that with the actual legal position.

The apprehension of the Court regarding the enforcement of the decision in another country proved true in *Bachchan v. Indian Abroad Publication Inc.* wherein Indian national got a favourable judgment in the United Kingdom but could not get judgment enforced in New York. The Court held that the UK Law applicable to the case is not harmony with the US Law and therefore, the decision cannot be recognised as enforceable in the US. This issue of enforcement of the court decision in a jurisdiction other than that where the decision was pronounced is likely to be faced by the courts frequently in e-commerce disputes.

The second issues raised before the Privy Council in *Annameli v. Muruges*, but was left undecided. This issue has become much important than it was before the birth of Multinational Corporations and the present economic liberalization undertaken by Government of India.

---

85 AIR 1934 All 340  
86 585 NYS 2d 661 (Sup. 1992)  
87 LLR 26 Mad. 544
The solution to this problem can be found by giving wide interpretation to the expression ‘carries on business’ used in Section 20 of the CPC so as to include ‘any business carried on by himself or through an agent’. This interpretation is supported by the fact the expression ‘carries on business’ has been used in addition to the expression ‘personally works for gain’. The two expressions are quite distinct from each other and one of the distinctions is the physical involvement of the person concerned. Thus, the person who is not carrying on business in India personally but through an agent or any other instrumentality may be considered as carrying on business for the purposes of Section 20 of CPC.

The issues of jurisdiction are more intriguing at the international level where not only the jurisdiction of the courts but also the applicable law will have to determined. The problem becomes complicated because of the diversity of the laws. For instance, comparative advertising is prohibited in Germany but not in America or India. Similarly advertising aimed at children is forbidden in Scandinavian countries but not in India. Thus, it is quite possible that any business activity executed over website may be perfectly legal in one country but may not be so in another.

**Judicial Trends and Jurisdiction**

At this juncture, it is prudent to examine some of the foreign legal precedents on the evolving subject of jurisdiction over the net.

In *Burgere King Crop. v. Rudezuitiz*, the US Supreme Court asserted jurisdiction on the grounds of accessibility of internet. The court asserted that when a defendant has purposefully directed its activities to a forum

---

88 471 US 462 (1985)
state caused injury to an individual or entity, the state’s invocation of jurisdiction comport with its Due process obligations.

However, this principle was not carried very far. In *Bensusan Restaurant Corp. v. King*[^89^], the US Court observed that “the issue....is whether existence of a ‘sit’ on the world wide web... without anything more, is sufficient to vest this court with personal jurisdiction over defendant”. The court answered the question in the negative, holding that the exercise of jurisdiction in such circumstances would run afoul of the Due process clause of the US Constitution.

The same principle was carried forward in *Hearst Corp. v. Goldberger*.[^90^] The court in this case held that it lacked personal jurisdiction over the definition. The court observed that “finding of personal jurisdiction... based on the mere availability of an internet Website would mean that there would be nationwide (indeed, worldwide) jurisdiction over anyone and everyone who establishes an internet website. Such nationwide jurisdiction is neither consistent with traditional personal jurisdiction case law nor acceptable to the court as a matter of policy.”

In *Maritz, Inc. v. Cybergold, Inc.*,[^91^] the court held that actively soliciting customer for mailing list created sufficient contacts to arrest jurisdiction over anon-resident definition in a trademark infringement action.

The famous case of *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*[^92^] gave the test of ‘sliding scale’ of interactivity under which the validity of

[^91^]: 947 F. Supp. ED No. 1996
jurisdiction depends on the ‘level of interactivity and commercial nature of the exchange of information’ of the defendant’s website.

In the Zippo case, the court analysed the jurisdictional issue in the contest of Internet and observed as follows:

The internet makes it possible to conduct business throughout the world entirely from a desktop. With this global revolution looming on the horizon, the development of the law concerning the permissible scope of personal jurisdiction based on internet use is in its infant stages. The cases are scant. Nevertheless, our review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the internet. The sliding scale is consistent with well-developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the internet personal jurisdiction is proper... At the opposite end are situations where a defendant has simply posted information on an internet website that is accessible to users in foreign jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. *Bensu san Restaurant Corp. v. King*, the court refused to exercise jurisdiction based on the website alone, reasoning that it did not rise to the level of purposeful availment of that jurisdiction’s laws. The middle ground is occupied by interactive web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website.
The Zippo Court asserted that when an entity intentionally engages in business with foreign jurisdiction, a ‘different result should not be reached simply because business is conducted over the internet’.93

In the case of *Panavision Int’l, L.P. v. Toeppen*,94 it was held,

There are two types of jurisdiction, general jurisdiction and personal jurisdiction. General jurisdiction exists when the defendant is domicile in the forum state or has substantial, systematic and continuous activities with the forum state. Specific jurisdiction is determined by three-part test. First, the defendant must do some act or enter into a transaction with the forum by which he purposely avails himself of the privilege of conducting activities in the forum. Second, the litigation must arise out of the act or transaction. Third, the exercise of jurisdiction must be reasonable under the circumstances. The requirement of purposeful availment is satisfied when the non-resident takes deliberate action toward the forum state. In tort cases, jurisdiction attaches over a non-resident tortfeasor who commits an act outside the forum state, directed at the forum state and causes harm to a resident of the forum state. This mechanism is called the ‘effects doctrine’.

The case of *Calder v. Jones* established the important ‘foreign effects’ test used in later cases, notably *Panavision* case. Conduct in one state having a tortuous effect in another state can established the necessary ‘minimum contracts’ to support the exercise of jurisdiction over non-resident defendants.

93 The American Courts have for the purposes of the jurisdiction classified websites into three categories:

**Active Website:** It facilitate establishing of contractual relationships and acts as a ‘window shop’ for the defendant to do actual business on the internet.

**Interactive Website:** These enable users to exchange information with the host computer.

**Passive Website:** These make only information available and do nothing more.

94 (1999) 72 Cal. App. 4th 104 (JDO)
The year 2001 saw a further redefining of the principles of the important subject of jurisdiction. In the case entitled *Clarence Bell Jr., v. Imperial Palace Hotel/Casino Inc.*, decided by the US District Court, the principles enunciated by the Zippo case got further refined.

The court held that to support specific personal jurisdiction, it is not enough for plaintiffs simply to allege the existence of an ‘interactive website’. The nature of the website, its use in the forum, and the relation of that use to the litigation are critical in assessing personal jurisdiction.

In the celebrated case of *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L’Antisémitisme*, the judicial thinking on jurisdiction got further refined.

This case has a peculiar history. Two groups in France La Ligue Contre Le Racisme et L’Antisémitisme (LICRA) and L’Union des Etudiants Juifs France (UEJF), complained to the court that Yahoo! France’s auction websites sold Nazi memorabilia and Third Reich related goods, which is banned under French Law. They consequently requested the court to take stringent action. Yahoo! Took up the plea that is was a company incorporated in the USA and that the French Laws did not bind it. It was further contended that technologically speaking, it was not possible for Yahoo! to block access to all Nazi memorabilia.

The French Court ordered Yahoo! France to remove all Nazi memorabilia and content from its website, failing which it would have to pay a fine of 100,000 francs for each day of non-compliance. Yahoo! complied with the order of the French judge and removed almost all of the Nazi memorabilia links on its auction sites.

95 2001 US Dist. LEXIS 18378 (ND Cal. 2001)
However, Yahoo! also moved an American court for a declaration that the directions given by the French judge were not enforceable in US and that Yahoo! being an American company was not bound by the decision of the French court.

In a historical judgment, the court in Yahoo! has taken the foreign effects test to its ultimate conclusion. One of the issues before the court was whether the State of California had jurisdiction over French citizens who attempted to enforce an order of a French requiring Yahoo!, a California resident to comply with that order by modifying its computer hardware and software systems. Answering the same in the affirmative, the court held that the California long arm state permits California courts to assert jurisdiction over non-residents consistent with the due process clause of the US Constitution. Jurisdiction may be premised on general jurisdiction requiring systematic and continuous contacts or specific jurisdiction requiring express aiming at the forum. The District Court of California further held that the directions of the French judge could not be enforced in the USA, as the same were violative of the First Amendment to the US Constitution. The Judge further held that though the American court respected the French judgment, yet the fact was that the French judgment was passed in the peculiar facts relating to France and that such judgment would not be applicable in American Law on American citizens and legal entities.

This judgment has far reaching significance and consequences on the entire subject of jurisdiction. Till now, the courts anywhere in the world could assume and were assuming jurisdiction on internet transactions and websites that were located outside the country. But this decision removed all doubts.
It is evident that the courts are looking into the totality of the circumstances when determining whether to exercise jurisdiction over individuals involved in internet related activities.

However, the coming of the Zippo Case in the US changed the legal principles concerning assuming of jurisdiction. In this case, the American court decided that there must be ‘something more’ than mere internet access in order to enable the court to assume jurisdiction.

C. CHOICE OF FORUM

In India parties are free to make choice of forum by making a contract to that effect where two or more courts have jurisdiction and that contract will not be hit by Section 28 of the Indian Contract Act. But it is not open to the parties to confer jurisdiction on a court, by agreement, which it does not possess under CPC.

7.3.4.2. CHOICE OF LAW

At the outset, it is important to make clear there is a distinction between choice of law and jurisdiction. While jurisdiction deals with issues of forum, applicable law deals with the legal rules and principles that need to

96 Section 28 of Indian Contract Act, 1872 read as, every agreement, by which any party thereto is restricted absolutely from enforcing his rights under or in respect of any contract, by the usual legal proceedings in the ordinary tribunals, or which limits the time within which he may thus enforce his rights, is void to the extent.

Exception 1 : Saving of contract to refer to arbitration dispute that may arise. This section shall not render illegal contract, by which two or more persons agree that any dispute which may arise between them in respect of any subject or class of subject shall be referred to arbitration, and that only and amount awarded in such arbitration shall be recoverable in respect of the dispute so referred.

Exception 2: Saving of contract to refer question that have already arisen - Nor shall this section render illegal any contract in writing, by which two or more persons agree to refer to arbitration any question between them which has already arisen, or affect any provision of any law in force for the time being as to reference to arbitration.
be applied. The choice of law is crucial in a contractual dispute because it defines the rules and principles by which the court can interpret the contract, its breach and enforceability. Applicable law governs issues of the validity of the material and such areas as mistake, representation, and contract formation with reference to which rule of acceptance may be applied. It also indicates the public policy and the formal validity of the contract regarding the capacity of the parties to the contract, illegality, performance and breach of contract. Further, applicable law governs presumptions of law and the burden of proof.97

The choice of applicable law that is to govern a transaction may be either express or implied. An express choice of law is indicated by a statement such as ‘this Agreement shall be governed by, construed and interpreted in accordance with the laws within the territory of India’. An implied choice may concur where previous dealings exist between the parties to the contract and where references to a specific country’ legal system has been made.

In India, the parties do not have choice in case applicable law because the Central Acts are almost applicable throughout India.98 This choice of law is available to the parties leaving in different countries, e.g. Aakash a party to online contract resides in India, the other party Amazon.com resides in the USA.

Further in America this choice of law is available for the citizens, because of the diversity of the state laws and is also available to the citizens of

98 Se Se Oil v. Gorakhram, (1962) 64 Bom LR 113; Societa Anonima Lucchesse Olii E vini Lucca v. Gorakhram, AIR 1964 Mad 532
different countries of European Union by virtue of Rome Convention of 1980\textsuperscript{99}.

In America, three tests have been laid down to determine the validity of a clause in a contract incorporating choice of law. These are (a) the chosen law must have a substantial relationship to either party or transaction,\textsuperscript{100} (b) the chosen law should not be contrary to the fundamental policy of the legal system which would apply in absence of a choice of law clause,\textsuperscript{101} (c) the particular state has a greater interest than the chosen state to determine the relevant issue.\textsuperscript{102}

The Rome Convention gives parties of the contracting state, a free hand to make choice of law which will govern their contract. The only requirement is that the choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. By their choice, the parties can select the law applicable to the whole or only to a part of the Contract.\textsuperscript{103} It is only the absence of such choice that the contract will be governed by the law of the country with which it is mostly closely connected.\textsuperscript{104}

\textbf{7.3.4.3. IDENTITY OF PARTIES}

Internet based e-commerce has besides, great advantages, posed many threats because of its being what is popularly called, ‘faceless and borderless’. For instance, sending an e-mail message does not require

\textsuperscript{99} EC Convention on the Law Applicable to Contractual Obligations (Rome 1980)
\textsuperscript{100} Seeman v. Philadelphia Warehouse Co., 274 US 403
\textsuperscript{101} Restatement second Conflict of Laws 187 (2) (a)
\textsuperscript{102} Ibid.
\textsuperscript{103} Davis v. Jointless Fire Brick Co., 300 Fed 1, 4 (1924)
\textsuperscript{104} Article 3 of the EC Convention on the Law Applicable to Contractual Obligations (Rome 1980)
\textsuperscript{104} Article 4 of the EC Convention on the Law Applicable to Contractual Obligations (Rome 1980)
disclosure of the identity of the sender, nor can a recipient ordinarily be able to know the sender. Furthermore, e-mail messages being like a post card can be interpreted at any place on line, modified, altered, changed and even made to appear to have come from a person other than the actual sender. Similarly a business can set up its own website over which goods or services can be offered without revealing its identity. Again businesses can set up a website in one country but appear to have premises in another country.

These apprehensions are now no mere hypothetical and have started surfacing in the countries where e-commerce has gathered momentum. There are chances of getting defrauded from the sham websites. In market there are many fake website, which are created for deceiving people.

If the disclosure of the identity of the contracting parties over internet is so possible, then many of the fundamental principles of the common law for contract formation will be either inapplicable or simply irrelevant. Whether in a physical environment where parties are at distance or in cyberspace, before executing a contract, the contracting parties must be sure about the (1) party sending or receiving the communication as the case may be (2) communication and (3) time of communication. If A and B communicate offer and acceptance for executing a contract over internet; B must be sure that the: (a) offer received by him is the offer sent by A, (b) offer received by him is the sent to him by A. In other words, offer has not been corrupted in transit, (c) of dispatch of offer, (d) offer received is meant for his. Similarly A must have the same surety when he receives acceptance from B.

The technology which produces many risks for the parties interested in making contract over internet provides solution also. However, the IT Act provides no alternative for the parties except to adopt asymmetrical
cryptosystem and hash function.\textsuperscript{105} This asymmetrical cryptosystem is also called public key encryption and is based on an Algorithm known as RSA.\textsuperscript{106}

The asymmetric cryptosystem, as the name suggests, has two different but mathematically related keys called the private key and the public key. The private key is also known as secret key and must be known only to the person holding the key pair. The public key is meant for public use. This key pair works in two ways. A message encrypted by the private key can be decrypted by the public key and the message encrypted by the public key can be decrypted by the private key. This key pair is unique to the person holding it. So a person using public key for decrypting a message will be sure that the message is of the person having its related private key because mathematically related keys can decrypt a message. If a person knows the private key holder, he will be sure that the message has come from that person.

Asymmetric public cryptosystem based on RSA is slow and is seldom used alone. To save time, RSA is used in combination with another cryptographic algorithm such as hash function. This hash function when applied to a message of any length creates short fixed value which is known as message digest or hash value. It is unique to the message and the given private key. The hash function produces the same hash value each time when applied to the same message. It is also called one way process because it is computationally infeasible to reconstruct the same message from its value. The chances of two messages producing the same hash value are insignificantly small. If there is a slight change in the

\textsuperscript{105} Section 3(2) of the Information Technology Act, 2000
\textsuperscript{106} RSA was invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adeleman on the ideas of White Field Diffie and Martim. Hellman is a person who developed public key cryptography in the mid 1970 at Stanford.
message contents, entirely different hash result will be produced. Once the hash result of the message is computed by the signer’s software it is then transformed into what is known as digital signature by the signer's private key. This works as follows:

Suppose A is interested in making an offer to B. A, instead of encrypting the whole message, will apply the hash function to produce a hash result. The hash result will be transformed into what is technically known as a digital signature by the private key of A. Then he will send that offer to B along with its electronic signature. B will apply the same hash function to the offer to get its hash value. Then using the public key of A and the hash value thus produced, B will verify (1) whether the electronic signature was created using the corresponding private key (2) whether the hash value produced by him matches the hash value sent to him by A which was transformed into the electronic signature.

This technology ensures the integrity of the message but does not prevent impersonation. In the above example, suppose B does not know A. Applying asymmetric cryptosystem even with a hash function will not enable B to know A. Anyone can generate a key pair by impersonating another. In order to prevent this, there must be a trusted third party who will independently confirm the identity of the parties, their location and legal status. The IT Act has assigned this job to certifying authorities who must be licensees. These certifying authorities will be supervised by the controller who will be appointed by the Central Government. The certifying authority is empowered to issue an electronic signature certificate in favour of a person who makes application to that effect and satisfies conditions laid down in the IT Act. The person in whose favour the electronic signature certificate is issued is called a subscriber. The subscriber may publish his digital signature certificate on his own or
through any other person or may make it available in the repository of the certifying authority so that anyone interested in establishing legal relationship with the subscriber can confirm his credentials.107

7.3.4.4. THIRD PARTY LIABILITY

It is the cardinal principle of contract law that one who is not a party to a contract cannot acquire rights under it. Now the question arises whether third party is having duty toward the parties to a contract. This question can be answered by giving an illustration.

Illustration: Anil is having internet connection of BSNL, while surfing he purchases a mobile phone on www. ebay.com. While making online payment of mobile phone his internet connection gets disconnected. At that time he assumes that his order got accomplished. He waits for the delivery of mobile, but he doesn’t receive the same for long time. On enquiry he finds that the payment of mobile is not done. On further enquiry to his shock he finds that the amount from his bank account is deducted as payment of mobile, but is not credited with the ebay.com. In this situation, a question arises before us who is liable is it whether ebay.com or BSNL.

In above example question arises, what is the liability of services provider in contract. Here, it can be said that the liability of internet service provider is same as that of postal department for the loss of letter. The internet service provider is can be made liable under the tort and consumer protection law. But he cannot be made liable under the contract, because internet service provider is mere postman and not party to the contract.

107 Sections 36(b) and 41(1) of the Information Technology Act, 2000
So it can be said that the internet service provider is liable under the tort for negligence. No way third party can be made liable under the contract.

These missing contracts are one of the most difficult parts of e-contracts. This would pose a challenge to judicial systems, till law is rightly corrected in this regard.

Having so far discussed about Information Technology Act, 2000 from the perspective of e-contracts, and other related issues, we now move ahead and have a look at international conventions regarding e-contracts.