INFORMATION TECHNOLOGY ACT 2000 & 2008

A SEMINAR REPORT

Submitted by

P.VISWASA REDDY

In partial fulfillment for the award of the degree

Of

BACHELOR OF ENGINEERING

In

INFORMATION TECHNOLOGY

At

VIVEKANANDA INSTITUTE OF TECHNOLOGY (EAST), JAIPUR RAJASTHAN TECHNICAL UNIVERSITY, KOTA

JANUARY-2012

ABSTRACT

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" which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

ACKNOWLEDGEMENT

it would be insufficient just to say a “word of thanks” for all those people who have been so instrumental in the success of this seminar. However, as a small token of my appreciation I have named hare of all those wonderful people, without whom all this would not have been possible.

I am deeply indebted to my mentor Mr. MANISH SWAMI for allowing me to gain the benefits of this seminar.

P.VISWASA REDDY

BRANCH-I.T.

VIII SEMESTER

CONTENTS

CHAPTER 1

INTRODUCTION TO IT ACTS

" The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb "– National Research Council, U S A "Computers at Risk" (1991)

What is Cyber Law ?Cyber Law is the law governing cyber space.Cyber spaceis a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Cyber law of India encompasses laws relating toCyber CrimesElectronic and Digital SignaturesIntellectual PropertyData Protection and Privacy

What is Cyber Crime?Cyber crime is the latest and perhaps the most complicated problem in the cyber world. Cyber crimes are unlawful acts where computer is used either as a tool; or a target; or both.The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime.

Cybercrimes can be basically divided into three major categories:Cybercrimes against personsCybercrimes against propertyCybercrimes against government

Cyber crime against personsCybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, is one of the most important Cybercrimes known today in genre.

Cyber crime against propertyThese crimes include:Computer vandalism (destruction of others' property);Transmission of harmful programmes; Siphoning of funds from financial institutions; Stealing secret information & data.

Cybercrime against governmentCyber terrorism is one distinct kind of crime in this category. The medium of Cyberspace is used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

Electronic SignatureElectronic Signatures are used to authenticate electronic records. Digital Signatures are one type of electronic signatures. Digital Signatures satisfy three major legal

requirements: Signer authentication; Message authentication; and Message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

Intellectual PropertyIntellectual property refers to creations of the human mind e.g., a story, a song, a painting, a design & etc. The facets of intellectual property that relate to cyber space are covered by Cyber law.

Facets of Intellectual PropertyCopyright law in relation to computer software, source code, websites, cell phone content etc. Licensing in terms of software and source code.Trademark law with relation to domain names, meta tags, mirroring, framing, linking etc.Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts.Patent law in relation to computer hardware and software.

Data Protection & PrivacyData Protection and Privacy Laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

IT Act of India, 2000The primary source of cyber law in India is the Information Technology Act , 2000 (IT Act).The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.Information Technology Act 2000 consisted of 94 sections segregated into 13 chapters. Four schedules form part of the Act.

IT Amendment Act, 2008ITA 2008, as the new version of Information Technology Act 2000 is often referred, has provided additional focus on Information Security. It has added several new sections on offences including Cyber Terrorism and Data Protection.The Information Technology Amendment Act, 2008 (IT Act 2008) has been passed by the parliament on 23rd December 2008 and came into force from October 27, 2009 onwards.

CHAPTER 2

HISTORY

The United Nations General Assembly by resolution A/RES/51/162, dated the 30 January 1997 has adopted the Model Law on Commerce adopted by the United Nations Commission on International Trade Law. This is referred to as the UNCITRAL Model Law on E-Commerce.

Following the UN Resolution India passed the Information Technology Act 2000 in May 2000 and notified it for effectiveness on October 17, 2000.

The Information technology Act 2000 has been substantially amended through the Information Technology Amendment Act 2008 which was passed by the two houses of the Indian Parliament on December 23, and 24, 2008. It got the Presidential assent on February 5, 2009 and was notified for effectiveness on October 27, 2009.

A complete history of how the current version of the Information Technology Act -2008 version evolved over a period of time between 1998 to 2009 is available at the reference link given under external links below.

Information technology Act 2000 consisted of 94 sections segregated into 13 chapters. Four schedules form part of the Act.

In the 2008 version of the Act, there are 124 sections (excluding 5 sections that have been omitted from the earlier version) and 14 chapters. Schedule I and II have been replaced. Schedules III and IV are deleted.

CHAPTER 3

STATEMENT OF OBJECTS AND REASONS INFORMATION TECHNOLOGY ACT 2000

1.The Information Technology Act was enacted in the year 2000 with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

2. With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as a protected system as to restrict its access.

3. A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.

4. The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly of the United Nations by its resolution No. 56/80, dated 12th December, 2001, recommended that all States accord

favourable consideration to the said Model Law on Electronic Signatures. Since the digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonisation with the said Model Law.

CHAPTER 4

Notes on clauses

Clause 1—This clause seeks to substitute the words "digital signatures" by the words "electronic signatures" as provided in the Table thereunder so as to make it technology neutral.

Clause 2—This clause seeks to amend sub-section (4) of section 1 so as to exclude Negotiable Instruments, power of attorney, trust, will and contract from the application of the Act and to empower the Central Government to amend the entries in the First Schedule.

Clause 3—This clause seeks to amend section 2 and to define certain new expressions.

Clause 4—This clause seeks to substitute heading of Chapter II with new heading "DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE' so as to make the Act technology neutral.

Clause 5—This clause seeks to insert a new section 3A which provides for authentication of electronic record by electronic signature or electronic authentication technique. It also empowers the Central Government to insert in the Second Schedule any electronic signature or electronic authentication technique and prescribe the procedure for the purpose of ascertaining the authenticity of electronic signature.

Clause 6—This clause seeks to insert a new section 6A which empowers the Central Government as well as the State Government to authorise the service providers for providing efficient services through electronic means to the public against appropriate service charges. Further the said section empowers the Central Government as well as the State Government to specify the scale of service charges.

Clause 7—This clause seeks to insert a new section 10A to provide for contracts formed through electronic means.

Clause 8—This clause seeks to make amendment in sub-section (1) of section 12 which is of a consequential nature.

Clause 9—This clause seeks to substitute sections 15 and 16 so as to remove certain inconsistencies in the procedures relating to secure electronic signatures and to provide for security procedures andpractices.

Clause 10—This clause provides for omission of section 20 with a view to empower the Certifying Authority under section 30 to act as repository of electronic signatures.

Clause 11—This clause seeks to make amendment in sub-section (1) of section 29 with a view to limit the powers of the Controller in respect of access to any computer system only with reference to the provisions of Chapter VI and not with reference to the provisions of entire Act. The powers with respect to access to any computer system under other provisions of the Act are proposed to be entrusted to the Central Government under section 69.

Clause 12—This clause seeks to amend section 30 with a view to empower the Certifying Authority to be the repository of all Electronic Signature Certificates issued under the Act.

Clause 13—This clause seeks to amend section 34 with a view to make the provisions of that section technology neutral.

Clause 14—This clause seeks to amend section 35 with a view to omit the first proviso to sub-section 94 so as to make the provisions of that section technology neutral.

Clause 15—This clause seeks to amend section 36 so as to add two more representations for issuance of digital signature.

Clause 16—This clause seeks to insert a new section 40A which provides for duties of the subscriber of Electronic Signature Certificate.

Clause 17—This clause seeks to make an amendment in the Chapter heading of Chapter IX with a view to provide for making compensation for damages in respect of various contraventions.

Clause 18—This clause seeks to amend section 43 so as to add certain more contraventions for damaging computer or computer system.

Clause 19—This clause seeks to insert a new section 43A so as to empower the Central Government to provide for reasonable security practices and procedures and the sensitive personal data or information and also to provide for compensation for failure to protect sensitive personal data or information stored in a computer resource.

Clause 20—This clause seeks to make amendment in section 46 with a view to make consequential changes.

Clause 21 and 22&23—These clauses seek to make amendments in the heading of Chapter X and section 48 with a view to suitably modify the same with the title of the Cyber Appellate Tribunal as mentioned in clause (*n*) of sub-section (1) of section 2.

Clause 24—This clause seeks to substitute sections 49 to 52 and insert new sections 52A to 52D. Section 49 provides for the establishment of the Cyber Appellate Tribunal. Sections 50, 51 and 52 provide for qualifications, term of office, conditions of service and salary and allowances of the Chairperson and Members of the said Tribunal. Sections 52A to 52D provide for powers of the Chairperson and distribution of business among the Benches.

Clause 25 to 28—These clauses seek to make amendments in sections 53 to 56 with a view to make the Cyber Appellate Tribunal a multi-member body.

Clause 29—This clause seeks to insert a proviso in section 61 so as to provide jurisdiction to courts in certain cases.

Clause 30—This clause seeks to amend section 64 so as to recover the compensation also as the arrears of land revenue.

Clause 31—This clause seeks to substitute sections 66 and 67 and insert new sections 66A and 67A with a view to make certain more computer related wrong actions punishable and enhance the penalty.

Clause 32—This clause seeks to amend section 68 so as to reduce the quantum of punishment and fine.

Clause 33—This clause seeks to substitute section 69 so as to empower the Central Government to issue directions to an agency for interception or monitoring or decryption of any information transmitted through any computer resource. It also provides for punishment for rendering assistance to such agency.

Clause 34—This clause seeks to amend section 70 so as to enable the Central Government as well as the State Government to declare any computer resource as protected system. It also provides for information security practices and procedures for such protected system.

Clause 35—This clause seeks to insert a new section 70A for empowering Indian Computer Emergency Response Team to serve as a national nodal agency in respect of Critical Information Infrastructure.

Clause 36—This clause seeks to insert a new section 72A which makes the disclosure of information in breach of a lawful contract punishable.

Clause 37—This clause seeks to substitute sections 77 and 78 and to insert new sections 77A and 77B. Section 77 provides that compensation, penalties or confiscation under the Act shall not interfere with the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force. Section 77 provides for certain offences relating to

computer resource as compoundable offences. Section 77B provides that Court shall take cognizance only on a complaint and not otherwise. Section 78 provides for power to investigate offences.

Clause 38—This clause seeks to substitute Chapter XII and to insert a new Chapter XIIA which provides for exemption of intermediaries from liability in certain circumstances and also empowers the Central Government to prescribe guidelines to be observed by intermediaries for providing services. It also empower the Central Government to specify the Examiner of Electronic Evidence.

Clause 39—This clause seeks to omit section 80 of the Act with a view to entrust the powers of search and seizure, etc., to a Police Officer not below the rank of Deputy Superintendent of Police and for that purpose necessary provisions have been included in section 78 by substituting the same *vide* clause 37.

Clause 40—This clause proposes to insert a proviso to section 81 so that the rights conferred under this sections hall be supplementary to and not in derogation of the provisions of the Copyright Act or the Patents Act.

Clause 41—This clause seeks to make amendment in section 82 with a view to declare the Chairperson, Members, officers and employees as public servants.

Clause 42—This clause seeks to amend section 84 with a view to make consequential changes.

Clause 43—This clause seeks to insert three new sections 84A, 84B and 84C with a view to empower the Central Government to prescribe the modes and methods of encryption for secure use of electronic media and for promotion of e-governance and e-commerce applications. Further it provides that abetment of and attempt to commit any offence shall also be punishable.

Clauses 44 and 45—These clauses seek to make amendments in sections 87 and 90 respectively, which are of consequential nature.

Clause 46—This clause seeks to omit sections 91 to 94 for the reason that these provisions have become redundant as necessary modifications have already been carried out in the Indian Penal Code and other related enactments.

Clause 47—This clause seeks to substitute new Schedules for the First Schedule and the Second Schedule so as to provide for documents or transactions to which the provisions of the Act shall not apply. It also enables the list of electronic signature or electronic authentication technique and procedure for affixing such signature to be specified in the Second Schedule.

Clause 48—This clause seeks to omit the Third Schedule and Fourth Schedule as consequential to the omission of provisions of sections 93 and 94.

Clause 49—This clause provides for certain amendments in the Indian Penal Code so as to specify certain offences relating to the computer resources.

Clause 50—This clause provides for certain consequential amendments in the Indian Evidence Act pursuant to the changes proposed in the Act.

Clause 51—This clause provides for amendments in the Code of Criminal Procedure by inserting new section 198B and amending section 320 so as to make certain consequential amendments pursuant to the changes proposed in the Act.

CHAPTER 5

INFORMATION TECHNOLOGY ACT 2000

ACT NO. 21 OF 2000

[9th June, 2000.]

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", which involve the use of alternatives to paper-based meth ds of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Ban of India Act, 1934 and for matters connected therewith or incidental thereto. WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law; AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based method of communication and storage of information; AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:-

5.1 PRELIMINARY

Short title, extent and commencement.

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be c nstrued as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to,- (a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881); (b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882; (c) a trust as defined in section 3 of the Indian Trusts Act, 1882; (d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 (39 of 1925) including any other testamentary disposition by whatever name called; (e) any contract for the sale or conveyance of immovable property or any interest in such property; (f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Definitions.

(1) In this Act, unless the context otherwise requires,- (a) "access" with its grammatical variations and cognate expressions means gaining entry into, instructing 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 LICENSE 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 manipulations of electronic, magnetic or optical impulses, and includes all input, outp t, 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, data, computer data base 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 programme , electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions; (m) "Controller" means the Controller of Certifying Authorities

5.2 DIGITAL SIGNATURE

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 ev ry 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.

5.3 ELECTRONIC GOVERNANCE

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 h ve been satisfied if such information or matter is-

(a) rendered or made available in an electronic form.

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

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 co tained 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 its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" sh ll be construed accordingly.

Use of electronic records and digital signatures in Government and itsagencies.

(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 LICENSE, 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 f rm as may be prescribed by the appropriate Government.

Retention of electronic records.

1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are r tained in the electronic form, if- (a) the information contained therein remains accessible so as to be usable for a subsequent reference; (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; (c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Power to make rules by Central Government in respect of digitalsignature.

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; (c) the manner or procedure which facilitates identification of the person affixing the digital signature; (d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and (e) any other matter which is necessary to give legal effect to digital signatures.

5.4 ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

Attribution of electronic records.

An electronic record shall be attributed to the originator- (a) if it was sent by the originator himself; (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.

Acknowledgement of receipt.

1) 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.

(2) 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.

(3) 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 spe ified 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 ackno ledgment 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.

Time and place of despatch and receipt of electronic record.

1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originato .

(2) 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.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched 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 lace of business.

(4) 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).

(5) For the purposes of this section,- (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.

5.5 SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

Secure electronic record:-

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.

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.

Security procedure:-

The Central Government shall for the purposes 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.

5.6 REGULATION OF CERTIFYING AUTHORITIES

Appointment of Controller and other officers.

1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification app int such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

Functions of Controller

The Controller may perform all or any of the following functions, namely:- (a) exercising supervision over the activities of the Certifying Authorities; (b) certifying public keys of the Certifying Authorities; (c) laying down the standards to be maintained by the Certifying Authorities; (d) specifying the qualifications and experience which employees of the Certifying Authorities should possess; (e) specifying the conditions subject to which the Certifying Authorities shall conduct their business; (f) specifying the contents of written, printed or visual

materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key; (g) specifying the form and content of a Digital Signature Certificate and the key; (h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities; (i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them; (j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems; (k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers; (l) resolving any conflict of interests between the Certifying Authorities and the subscribers; (m) laying down the duties of the Certifying Authorities; (n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

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, r cognise any foreign Certifying Authority as a Certifying Authority for the purposes 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 any 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, by notificati n in the Official Gazette, revoke such recognition.

Controller to act as repository:-

(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall- (a) make use of hardware, software and procedures that are secure from intrusion and misuse; (b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

Application for license

1) Every application for issue of a LICENSE shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a LICENSE shall be accompanied by- (a) a certification practice statement; (b) a statement including the procedures with respect to identification of the applicant; (c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government; (d) such other documents, as may be prescribed by the Central Government.

Renewal of license:-

An application for renewal of a license shall be- (a) in such form; (b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the

Suspension of LICENSE:-

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,- (a) made a statement in, or in relation to, the application for the issue or renewal of the LICENSE, which is incorrect or false in material particulars; (b) failed to

comply with the terms and conditions subject to which the LICENSE was granted; (c) failed to maintain the standards specified under clause (b) of

sub-section (2) of section 20; (d) contravened any provisions of this Act, rule, regulation or order made thereunder, revoke the LICENSE: Provided that no LICENSE shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation. .

Notice of suspension or revocation of LICENSE:-

(1) Where the LICENSE of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories: Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock: Provided further that the Controller may, if he considers necessary, publicise the contents of data base in such electronic or other media, as he may consider appropriate.

Power to delegate:-

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

Power to investigate contraventions:-

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 (43 of 1961) and shall exercise such powers, subject to such li itations laid down under that Act.

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 any contravention of the provisions of this Ac , rules or regulations made thereunder 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 purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge 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.

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

Certifying Authority to ensure compliance of the Act, etc:-

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, egulations and orders made thereunder.

5.7 DIGITAL SIGNATURE CERTIFICATES

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 applicants.

(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 D gital Signature Certificate or for reasons to be recorded in writing, reject the application: Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that- (a) the applicant 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 by the private key 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.

Representations upon issuance of Digital Signature Certificate:-

A Certifying Authority while issuing a Digital Signature Certificate shall certify that- (a) it has complied with the provisions of this Act and the rules and regulations made thereunder; (b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it; (c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate; (d) the subscriber's public key and private key constitute a functioning key pair; (e) the information contained in the Digital Signature Certificate is accurate; and (f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

Revocation of Digital Signature Certificate.

1) A Certifying Authority may revoke a Digital Signature Certificate issued by it- (a) where the subscriber or any other person authorised by him makes a request to that effect; or (b) upon the death of the subscriber; or (c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice

to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that- (a) a material fact represented in the Digital Signature Certificate is false or has been concealed; (b) a requirement for issuance of the Digital Signature Certificate was not satisfied; (c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability; (d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Notice of suspension or revocation.

1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the reposi ory specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

Acceptance of Digital Signature Certificate.

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate- (a) to one or more persons; (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that- (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same; (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true; (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

5.8 PENALTIES AND ADJUDICATION

Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,- (a) accesses or secures access to such computer, computer system or computer network; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Explanation:-For the purposes of this section,- (i) "computer contaminant" means any set of computer instructions that are designed- (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network; (ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer ystem or computer network and are intended for use in a computer, computer system or computer network; (iii) "computer virus" means any computer instruction, information, data or

programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates wh n a programme, data or instruction is executed or some other event takes place in that computer resource; (iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Penalty for failure to furnish information, return

If any person who is required under this Act or any rules or regulations made thereunder to- (a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure; (b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues; (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

5.9 THE CYBER REGULATIONS APPELLATE TRIBUNAL

Establishment of Cyber Appellate Tribunal:-

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification

referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Composition of Cyber Appellate Tribunal:-

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal:-

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he- (a) is, or has been, or is qualified to be, a Judge of a High Court; or (b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

Term of office:-

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

Salary, allowances and other terms and conditions of service ofPresiding Officer. 52. Salary, allowances and other terms and conditions of service of Presiding Officer:-The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed: Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

Filling up of vacancies.

-If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

Resignation and removal:-

(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office: Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly app inted as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings:-

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and n act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

Staff of the Cyber Appellate Tribunal:-

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

Appeal to Cyber Appellate Tribunal:-

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry

of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appea ed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under

sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the ap eal.

Procedure and powers of the Cyber Appellate Tribunal:-

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subj ct to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the foll wing matters, namely:- (a) summoning and enforcing the attendance of any person and examining him on oath; (b) requiring the discovery and production of documents or other electronic records; (c) receiving evidence on affidavits; (d) issuing commissions for the examination of witnesses or documents; (e) reviewing its decisions; (f) dismissing an application for default or deciding it ex parte; (g) any other matter which may be prescribed.

5.10 OFFENCES

Tampering with computer source documents. 65. Tampering with computer source documents:- Whoever knowingly 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, comp ter system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with oth. Explanation:-For the purposes 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.

Hacking with computer system

:-(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes i s 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.

Publishing of information which is obscene in electronic form. 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 t deprave and corrupt persons who are likely, having regard to all relevant circumstances, 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 exte d 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 rup es.

Power of Controller to give directions

:-(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities with the provisions of this Act, rules or any regulations made thereunder. as specified in the order if those are necessary to nsure compliance

(2) Any person who fails to comply with any order under sub-section

(1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Directions of Controller to a subscriber to extend facilities todecrypt information. 69. Directions of Controller to a subscriber to extend facilities to

decrypt information:-(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, riendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under

sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency

referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

Protected system.

70. Protected system:-(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under

sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be l able to fine.

Penalty for misrepresentation:-

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any LICENSE or Digital Signature Certificate, as the case may be, shall be punished ith imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Penalty for breach of confidentiality and privacy:-

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or ot er material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Penalty for publishing Digital Signature Certificate false in certain particulars:-

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that- (a) the Certifying Authority listed in the certificate has not issued it; or (b) the subscriber listed in the certificate has not accepted it; or (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Act to apply for offence or contravention committed outside India. 75. Act to apply for offence or contravention committed outside

India:-(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network lo ated in India.

5.11 NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

Network service providers not to 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 any service as a network service provider shall be liable under this 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. Act, rules or regulations made thereunder for any third party 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;

5.12 MISCELLANEOUS

Power of police officer and other officers to enter, search, etc:-

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Deputy Superintendent of Police, or any other of icer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of commi ting or of being about to commit any offence under this Act. Explanation:-For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

Act to have overriding effect:-

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Controller, Deputy Collector and Assistant Controllers to be public servants:-

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed t be public servants within the meaning of section 21 of the Indian Penal Code (45 of 1860).

Power of State Government to make rules:-

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:- (a) the electronic form in which filing, issue, grant receipt or

payment shall be effected under sub-section (1) of section 6;

(b) for matters specified in sub-section (2) of section 6; (c) any other matter which is required to be provided by rules by the State Government.

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that Hou e.

Amendment of Act 45 of 1860. 91. Amendment of Act 45 of 1860:-The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

Amendment of Act 1 of 1872. 92. Amendment of Act 1 of 1872:-The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

Amendment of Act 18 of 1891. 93. Amendment of Act 18 of 1891:-The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

Amendment of Act 2 of 1934. 94. Amendment of Act 2 of 1934:-The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act:----

CHAPTER -6

The Information Technology Act, 2000
As amended by
The Information Technology (Amendment) Act, 2008

6.1 PRELIMINARY

1.Short Title, Extent, Commencement and Application:-

(1) This Act may be called the Information Technology Act, 2000. [As Amended by Information technology (Amendment) Act 2008]

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision. [Act notified with effect from October 17, 2000. Amendments vide ITAA-2008 notified with effect from....]

(4) (Substituted Vide ITAA-2008) Nothing in this Act shall apply to documents or transactions specified in the First Schedule:Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto.

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

2. Definitions:-

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

(a) "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing 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 adjudicating officer appointed under subsection (1) of section 46;

(d) "Affixing Electronic 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 Electronic 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 Govt;

(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 license to issue a Electronic 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 Electronic Signature Certificates;

"Communication Device" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Inserted Vide ITAA 2008)

(i) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) "Computer Network" means the inter-connection of one or more Computers or Computer systems or Communication device through;
(i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

(k) "Computer Resource" means computer, communication device, computer system, computer network, data, 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 programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48

(na) "Cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

(nb) "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorise d access, use, disclosure, disruption, modification or destruction.

(o) "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;

(r) "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means official Gazette published in the electronic form;

(t) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(ta) "Electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature;

(tb) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate";

(u) "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua) "Indian Computer Emergency Response Team" means an agency established under sub-section (1) of section 70-B;

(v) "Information" includes data, message, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche;

(w) "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes;

(x) "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made there under;

(z) "License" means a license granted to a Certifying Authority under section 24;

(za) "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;

(zb) "Prescribed" means prescribed by rules made under this Act;

(zc) "Private Key" means the key of a key pair used to create a digital signature;

(zd) "Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "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;
(d) adhere to generally accepted security procedures;

(zf) "Security Procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "Subscriber" means a person in whose name the Electronic Signature Certificate is issued;

(zh) "Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether –
(a) the initial electronic record was affixed with the digital signature by the use of private key) corresponding to the public key of the subscriber;
(b) the initial electronic record is retained intact or has been altered since such electronic) record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

6.2 DIGITAL SIGNATURE AND ELECTRONIC 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.

3-A. Electronic Signature

(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section(2), a subscriber nay 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 of no other person;

(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;

(c) Any alteration to the electronic signature made after affixing such signature is detectable;

(d) Any alteration to the information made after its authentication by electronic signature is detectable; and

(e) It fulfills such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of 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

6.4 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 been 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 Electronic Signature:-

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, not withstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

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

6. Use of Electronic Records and Electronic Signature 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 license, 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).

6-A. Delivery of Services by Service Provider –

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorise , by order, any service provider to set up, maintain and upgrade

the computerised facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation - For the purposes of this section, service provider so authorised includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorise any service provider authorised under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (2), the appropriate Government may authorise the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.

7. Retention of Electronic Records -

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if -

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

7-A. Audit of Documents etc in Electronic form -

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

8. Publication of rules, regulation, etc, in Electronic Gazette

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form

9. Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form -

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and

preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to Make Rules by Central Government in respect of Electronic Signature -

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

(a) The type of Electronic Signature;

(b) The manner and format in which the Electronic Signature shall be affixed;

(c) The manner or procedure which facilitates identification of the person affixing the Electronic Signature;

(d) Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) Any other matter which is necessary to give legal effect to Electronic Signature.

10-A. Validity of contracts formed through electronic means:-

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

6.4 ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC RECORDS

11. Attribution of Electronic Records –

An electronic record shall be attributed to the originator, -

(a) if it was sent by the originator himself;

(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.

12. Acknowledgement of Receipt: –

(1) Where the originator has not agreed with stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment maybe 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.

(2) 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.

(3) 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.

13. Time and place of dispatch and receipt of electronic record. –

(1) 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.

(2) 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.

(3) Save as otherwise agreed 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.

(4) The provisions of sub-section (2) shall apply not withstanding 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).

(5) For the purposes of this section -

(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.

6.5 SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC 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 Electronic Signature. –

An electronic signature shall be deemed to be a secure electronic signature if-

(i) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation **-** In case of digital signature, the "signature creation data" means the private key of the subscriber

16. Security procedures and Practices. –

The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices:

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

6.6 REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers. –

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers, other officers and employees as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller. Circumventing

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers other officers and employees shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller. –

The Controller may perform all or any of the following functions, namely

(a) Exercising supervision over the activities of the Certifying Authorities;

(b) Certifying public keys of the Certifying Authorities'

(c) Laying down the standards to be maintained by the Certifying Authorities;

(d) Specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) Specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) Specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;

(g) Specifying the form and content of a Electronic Signature Certificate and the key;

(h) Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) Resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) Laying down the duties of the Certifying Authorities;

(n) Maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

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, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Electronic 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 any 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, by notification in the Official Gazette, revoke such recognition.

20. Controller to act as repository. –

(Omitted by the Information Technology (Amendment) Act, 2008 (10 of 2009), Section 13 (w. e. f. 27-10-2009).

21. License to issue electronic signature certificates:-

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

(2) No license 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 Electronic Signature Certificates as may be prescribed by the Central Government.

(3) A license granted under this section 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.

22. Application for license:-

(1) Every application for issue of a license shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a license shall be accompanied by-

(a) A certification practice statement;

(b) A statement including the procedures with respect to identification of the applicant;

(c) Payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) Such other documents, as may be prescribed by the Central Government.

23. Renewal of license –

An application for renewal of a license shall be –

(a) In such form;

(b) Accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the license:

24. Procedure for grant or rejection of license:-

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.

25. Suspension of License –

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has -

(a) Made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;

(b) Failed to comply with the terms and conditions subject to which the license was granted;

(c) Failed to maintain the standards specified in Section 30 [Substituted for the words "under clause (b) of sub-section (2) of section 20;" vide amendment dated September 19, 2002]

(d) Contravened any provisions of this Act, rule, and regulation or order made there under, revoke the license:

Provided that no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any grounds for revoking a license under sub-section (1), by order suspend such license pending the completion of any enquiry ordered by him:

Provided that no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.

26. Notice of suspension or revocation of license –

(1) Where the license of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data-base maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

Provided that the data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock.

Provided further that the Controller may, if he considers necessary, publicize the contents of the data-base in such electronic or other media, as he may consider appropriate.

27. Power to delegate.

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions. –

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data:-

(1) Without prejudice to the provisions of sub-section (1) of section 68, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter 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 purposes 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 assistant 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 arc reasonably suited to the performance of intended functions;

(c) Adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured;

(ca) be the repository of all Electronic Signature Certificates issued under this Act;

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and

(d) Observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc. –

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

32. Display of license. –

Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carries on its business.

33. Surrender of license:-

(1) Every Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller.

(2) Where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favor a license is issued, shall be guilty of an offense and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure. –

(1) Every Certifying Authority shall disclose in the manner specified by regulations -

(a) Its Electronic Signature Certificate

(b) Any certification practice statement relevant thereto;

(c) Notice of revocation or suspension of its Certifying Authority certificate, if any; and

(d) Any other fact that materially and adversely affects either the reliability of a Electronic Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature Certificate was granted, then, the Certifying Authority shall-

(a) Use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) Act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

6.8 ELECTRONIC SIGNATURE CERTIFICATES

35. Certifying Authority to issue Electronic 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 applicants.

(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 application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate. –

A Certifying Authority while issuing a Digital Signature Certificate shall certify that -

(a) It has complied with the provisions of this Act and the rules and regulations made there under;

(b) It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(ca) the subscriber holds a private key which is capable of creating a digital signature

(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber.

(d) The subscriber's public key and private key constitute a functioning key pair;

(e) The information contained in the Digital Signature Certificate is accurate; and

(f) It has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of Digital Signature Certificate. –

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate -

(a) on receipt of a request to that effect from -

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate. –

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it -

(a) Where the subscriber or any other person authorised by him makes a request to that effect; or

(b) Upon the death of the subscriber; or

(c) Upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that -

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority Shall communicate the same to the subscriber.

39. Notice of suspension or revocation:-

(1)Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for
publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

6.9 DUTIES OF SUBSCRIBERS

40. Generating Key Pair:-

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, (*) the subscriber shall generate pair by applying the security procedure.

40-A. Duties of subscriber of Electronic Signature Certificate:-

In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.

41. Acceptance of Digital Signature Certificate:-

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorise s the publication of a Digital Signature Certificate -

(a) To one or more persons;

(b) In a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that -

(a) The subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) All representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) All information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of Private Key. –

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the r public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation - For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

6.10 PENALTIES, COMPENSATION AND ADJUDICATION

43. Penalty and Compensation for damage to computer, computer system, etc. – \

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, -

(a) Accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under;

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

he shall be liable to pay damages by way of compensation to the person so affected.

Explanation - For the purposes of this section, -

(i) "Computer Contaminant" means any set of computer instructions that are designed -

(a) To modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or

(b) By any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means;

(v) "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

43-A. Compensation for failure to protect data: –

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation: For the purposes of this section,-

(i) "Body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security

practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

(iii) "Sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

44. Penalty for failure to furnish information, return, etc :–

If any person who is required under this Act or any rules or regulations made there under to –

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues;

45. Residuary Penalty:-

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to Adjudicate:-

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section(3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(1-A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees 5 crore

Provided that the jurisdiction in respect of claim for injury or damage exceeding rupees 5 crore shall vest with the competent court.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and Legal or Judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and -

(a) All proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;
(b) Shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.
(c) Shall be deemed to be a Civil Court for purposes of order XXI of the Civil Procedure Code, 1908 (5 of 1908).

47. Factors to be taken into account by the adjudicating officer:-

While adjudging the quantum of compensation under this Chapter the adjudicating officer shall have due regard to the following factors, namely –

(a) The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
(b) The amount of loss caused to any person as a result of the default;

(c) The repetitive nature of the default.

6.11 THE CYBER APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal:-

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal:-

(1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint.

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008 (Inserted Vide ITAA 2008)

(d) The Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction;

(4) Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member
of such Tribunal from one Bench to another Bench.

(5) If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

50. Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal. –

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court;

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than two one years or joint secretary to the Government of India or any equivalent post in the central Government or State Government for a period of not less than seven years.

51. Term of office, conditions of service etc of Chairperson and Members:-

(1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.

(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member.

52. Salary, allowance and other terms and conditions of service of Chairperson and Member:-

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of Cyber Appellate Tribunal shall be such as may be prescribed.

52-A. Powers of superintendence, direction, etc. –

The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

52-B. Distribution of Business among Benches.

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

52-C. Powers of the Chairperson to transfer cases. –

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo moto without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

52-D. Decision by majority:-

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

53. Filling up of vacancies:-

If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding officer Chairperson or Member as the case may be of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal. –

(1) The Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Chairperson or the Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings:-

No order of the Central Government appointing any person as the Chairperson or the Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal:-

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as the Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Chairperson.

(3) The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Regulations Appellate Tribunal:-

(1) Save as provided in sub-section (2), any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

58. Procedure and Powers of the Cyber Appellate Tribunal:-

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -

(a) summoning and enforcing the attendance of any person and examining him on oath;
(b) requiring the discovery and production of documents or other electronic records;
(c) receiving evidence on affidavits;
(d) issuing commissions for the examination of witnesses or documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it *ex parte* ;
(g) any other matter which may be prescribed

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

59. Right to legal representation:-

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal Limitation

60. Limitation:-

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction. –

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High court:-

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of Contravention:-

(1) Any contravention under this Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by

the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation - For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

6.12 OFFENCES

65. Tampering with Computer Source Documents:-

Whoever knowingly 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 program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

66. Computer Related Offences. –

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to 5 lakh rupees or with both.

Explanation: For the purpose of this section,-

a) The word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

b) The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

66–A. Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

a) Any information that is grossly offensive or has menacing character; or

b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device;

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to two three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66-B. Punishment for dishonestly receiving stolen computer resource or communication device:-

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66-C. Punishment for identity theft:-

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66-D. Punishment for cheating by personation by using computer resource:-

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66-E. Punishment for violation of privacy:-

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation:- For the purposes of this section--

(a) "Transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "Capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "Private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "Publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "Under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that-

(i) He or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) Any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66-F. Punishment for cyber terrorism:-

(1) whoever,-

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) Denying or cause the denial of access to any person authorised to access computer resource; or

(ii) Attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) Introducing or causing to introduce any Computer Contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

67. Punishment for publishing or transmitting obscene material in electronic form:-

Whoever publishes or transmits or causes to be published or transmitted 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 circumstances, 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 three years and with fine which may extend to five lakh rupees and in the event of a second or

subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67-A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:-

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct 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 ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

67-B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form:-

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
(d) Facilitates abusing children online; or
(e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67-A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) Which is kept or used for bonafide heritage or religious purposes.

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67-C. Preservation and Retention of information by intermediaries:-

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

68. Power of Controller to give directions:-

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or with both.

69. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource:-

(1) Where the central Government or a State Government or any of its officer specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

69-A. Power to issue directions for blocking for public access of any information through any computer resource:-

(1) Where the Central Government or any of its officer specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2), for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

69-B. Power to authorise to monitor and collect traffic data or information through any computer resource for Cyber Security:-

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43;

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

70. Protected system:-

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

70-A. National nodal agency:-

(1) The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.

(2) The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.
(3) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

70-B. Indian Computer Emergency Response Team to serve as national agency for incident response:-

(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-

(a) collection, analysis and dissemination of information on cyber incidents;
(b) forecast and alerts of cyber security incidents;
(c) emergency measures for handling cyber security incidents;
(d) coordination of cyber incidents response activities;
(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
(f) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.

(7) Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

(8) No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1)

71. Penalty for misrepresentation:-

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished

with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy:-

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72-A. Punishment for Disclosure of information in breach of lawful contract:-

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

73. Penalty for publishing electronic Signature Certificate false in certain particulars:-

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that -

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Publication for fraudulent purpose:-

Whoever knowingly creates publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

75. Act to apply for offence or contraventions committed outside India:-

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation:-

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape

drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

77. Compensation, penalties or confiscation not to interfere with other punishment:-

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77-A. Compounding of Offences:-

(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act. Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

77-B. Offences with three years imprisonment to be cognizable:-

(1) Not withstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

6.13 INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. Exemption from liability of intermediary in certain cases:-

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) The intermediary does not-

(i) initiate the transmission,

(ii) Select the receiver of the transmission, and

(iii) Select or modify the information contained in the transmission;

(c) The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if-

(a) The intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act ;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

6.14 EXAMINER OF ELECTRONIC EVIDENCE

79-A. Central Government to notify Examiner of Electronic Evidence:-

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

***Explanation*:-** For the purpose of this section, "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

6.15 MISCELLANEOUS

80. Power of Police Officer and Other Officers to Enter, Search, etc:-

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

***Explanation* -** For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

81. Act to have Overriding effect:-

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act ,1970 (39 of 1970).

81-A. Application of the Act to Electronic cheque and Truncated cheque: –

(1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

(2) Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under the notification.

82. Chairperson, Members, Officers and Employees to be Public Servants:-

The Chairperson, Members and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be Public Servants within the meaning of section 21 of the Indian Penal Code.

83. Power to Give Directions:-

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made there under.

84. Protection of Action taken in Good Faith:-

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, Adjudicating Officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

84-A. Modes or methods for encryption: –

The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption

84-B. Punishment for abetment of offences:-

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

84-C. Punishment for attempt to commit offences:-

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

85. Offences by Companies:-

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Explanation - For the purposes of this section

(i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and

(ii) "Director", in relation to a firm, means a partner in the firm.

86. Removal of Difficulties:-

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act. (2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules: -

(1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may 2 provide for all or any of the

following matters, namely:-

(a) the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3-A;

(aa) the procedure for ascertaining electronic signature or authentication under sub-section (3) f section 3-A;

(ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5;

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed or issued and the method of payment under sub-section (2) of section 6;

(ca) the manner in which the authorised service provider may collect, retain and appropriate service charges under sub-section (2) of section 6-A;

(d) the matters relating to the type of Electronic Signature, manner and format in which it may be affixed under section 10;

(e) the manner of storing and affixing electronic signature

creation data under section 15;

(ea) the security procedures and practices under section 16;

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers, other officers and employees under section 17;

(g) (omitted vide ITAA-2008)

(h) the requirements which an applicant must fulfill under sub-section (2) of section 21;

(i) the period of validity of license granted under clause (a) of sub-section (3) of section 21;

(j) the form in which an application for license may be made under subsection (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

(l) such other documents which shall accompany an application for license under clause (d) of sub-section (2) of section 22;

(m) the form and the fee for renewal of a license and the fee payable there of under section 23;

(ma) the form of application and fee for issue of Electronic Signature Certificate under section 35;

(n) the form in which application for issue of a Electronic Signature Certificate may be made under sub-section (1) of section 35;

(o) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

88. Constitution of Advisory Committee:-

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber
Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise -

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act;

(4) There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

89. Power of Controller to make Regulations:-

(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made there under to carry out the purposes of this Act

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the
following matters, namely-

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (n) [Substituted for (m) vide amendment dated 19/09/2002] of section 18;

(b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority under sub-section (1) of section 19;

(c) the terms and conditions subject to which a license may be granted under clause (c) of sub-section (3) of section 21;

(d) other standards to be observed by a certifying authority under clause (d) of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section (3) of section 35;

(g) the manner by which a subscriber communicates the compromise of private key to the Certifying Authority under sub-section (2) of section 42;

90. Power of State Government to make rules:-

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely -

(a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;

(b) for matters specified in sub-section (2) of section 6;

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. Amendment of Act 45 of 1860. –

[Omitted by the Information Technology (Amendment) Act, 2008 (10 of 2008), Section 48 (w.e.f. 27-10-2009).].

92. Amendment of Act 1 of 1872. –

[Omitted by the Information Technology (Amendment) Act, 2008 (10 of 2008), Section 48 (w.e.f. 27-10-2009).].

CHAPTER 7

CYBER CRIME

History reveals that the Cyber crime originated even from the year 1820.That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

2. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime

3.0. The term 'cyber crime' has not been defined in any Statute or Act.

3.1. The Oxford Reference Online defines 'cyber crime' as crime committed over the Internet.

3.2. The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of special knowledge or expert use of computer technology. So what exactly is Cyber Crime. Cyber Crime could reasonably include a wide variety of criminal offences and activities.

3.3. CBI Manual defines cyber crime as:

(i) Crimes committed by using computers as a means, including conventional crimes.

(ii) Crimes in which computers are targets.

3.4. A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both".

3.5. The Information Technology Act, 2000, does not define the term 'cyber crime'. Cyber crime can generally defined as a criminal activity in which information technology systems are the means used for the commission of the crime.

4. Based on the United Nations General Assembly resolution of January 30,1997, the Government of India passed the Information Technology Act 2000 (Act No.21 of 2000) and notified it on October 17, 2000. The Information Technology Act, 2000, is the first step taken by the Government of India towards promoting the growth of the E-commerce and it was enacted with a view to provide legal recognition to e-commerce and e-transactions, to facilitate e-governance and prevent computer-based crimes. It is a first historical step.

5. However, the rapid increase in the use of Internet has led to a spate in crime like child pornography, cyber terrorism, publishing sexually explicit content in electronic form and video voyeurism. The need for a comprehensive amendment was consistently felt and after sufficient debate and much deliberation, the I.T. Amendment Act 2008 was passed. The ITAA 2008 got the President's assent in

4.February 2009 and was notified with effect from 27.10.2009. The new IT Amendment Act 2008 has brought a large number of cyber crimes under the ambit of the law. Some of the significant points in the Amendment Act include introduction of corporate responsibility for data protection with the concept of 'reasonable security practices' (Sec.43A), recognition of Computer Emergency Response Team – India (CERT-In) as the national nodal agency empowered to monitor and even block web-sites under specific circumstances, introduction of technological neutrality replacing digital signatures with electronic signatures etc. Besides, the CERT-In will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents.

6. The IT Act provides legal recognition for transactions carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce", involving the use of alternatives to paper-based methods of communication and storage of information. The IT Act facilitates electronic filing of documents with the Government agencies.

7. Cyber Crimes - Three categories :

 Against Property – Financial crimes – cheating on-line – illegal funds transfer.

 Against Persons – On-line harassment, Cyber Stalking, Obscenity.

 Against Nations – Cyber Terrorism – Damaging critical information infrastructures.

NATURE MODUS OPERAND
I. OFFENSIVE MESSAGES

(Messaging, annoying, intimidating, insulting, misleading, defaming)

i. SMS SMS of above nature may be sent using mobile phone of one's own identity or by acquiring a fade identity.

 Such SMS may be forwarded amongst groups and communities (inter/intra) in which case the actual source could not be fixed.

 Few SMSs had been circulated affecting public tranquillity; Eg: False Tsunami warning, false alarm as target of explosion.

ii. MMS □ Multimedia messages often defaming or obscene are Sent among small groups using mobile Phones/Bluetooth

□ If there had been a sharing in many mobile equipments the first source couldn't be fixed. E.g., Arrest of the Managing Director of bazee.com in a school MMS Scandal in Delhi.

□ Often captured in private places unknowingly for future exploitation.

iii. Web based SMS □ SMS can be sent by logging onto sites like way2sms.com by becoming a member of the site typing the message of choice and choosing destination to be sent anywhere in the world by concealing one's identity

□ Way2sms never share the IP logs with law enforcement agencies.

iv. Chat room messages □ Chat room messages in internet relay chats happens by direct connection between each others' machines in which the IP logs are stored neither by Yahoo nor Google and so information shared in Chat rooms may be saved but can never be traced retrospectively to its origin

II OFFENSIVE CALL

(Offender calls either by his/her own name or by acquiring false identity- Landline calls/mobile calls, web based calls, VOIP calls, Skype, Yahoo messenger, Chat room calls,overseas calls etc.)

i. Landline/mobile calls □ Many landlines still have no caller Ids

□ Difficulty if the connection is in a non-existent fictitious address.

ii. Web based calls □ Calls can be made by spoofing the mobile number using the sites like http://www.phonetrick.net/ www.prankdial.com/

iii. Overseas calls

Landline/mobile

□ For overseas landline/mobiles the details of the subscribers are not available without the co-operation of international agencies.

iv. Chat room calls – VOIP

Calls – Skype

□ In VOIP it is difficult to ascertain the source as it passes through various international gateways before it enters the country to get terminated in an Indian operator's subscriber

III Deceptive messages

(Lottery, cheating, job racket)

(*SMS of lottery cheating, emails of prize money, articles, false promise of jobs, false mail for admission to a reputed University)*

 Greed of the victim is the main reason why cyber frauds are successful.

 SMS/Email messages of winning a lottery of prize money or articles, alluring people to deposit money.

 Clues available are email IDs and sometimes few mobile phone numbers.

 Live.com, Yahoo.co.uk domains IP which are frequently used never share the login IPs and it provides a conducive climate for commission of crimes.

 To the extent it was made available, the IP logs invariably had shown some Nigerian, Mediterranean, Middle East and American countries. Hence users details are not available.

 The mobile numbers are often fictitious and seasonal.

 The Bank accounts are invariably bogus and have transient life; sometimes an innocent gets allured for Commission by stating false reasons for the source of money.

 The following awareness messages have been propagated:

Do not believe emails or SMS that say that you have won a million dollar lottery. Be way of strangers who promise to transfer Crores of rupees to your bank account.

 Similar cheating can be for prize of cars, for an employment to a job fetching high income, admission to a course in a reputed university abroad.

 Sometimes Nigerians use the tool of threat of an insider staying inside star hotels waiting for instructions to ignite an explosive if not parted with the ransom money by negotiations.

 Occasionally criminals hide behind proxy servers by concealing their real location of log-ins.

 (Threat to critical infrastructures and vital installations and public places) E-mails of threatening nature often with an intention to mislead or to deceive or to implicate another person by wielding threat to critical infrastructures

IV. DATA THEFT

(Theft of proprietory information causing breach of confidentiality and integrity and thereby altering its utility value. More due to disharmony in employee/employer situations by disgruntled employees.)

 Sensitive information belonging to business organizations is targeted by rivals, criminals and sometimes even by disgruntled employees.

 Disharmony in work place often makes the exemployees to take away the valuable data or design or client information.

 Sometimes they damage it; delete it; or sell it to a competitor.

 Many a times the employers become suspicious about their ex-employees and attribute instances of data theft which the ex-employee was holding in his possession to carryout his official duties at the time of his employment.

 Frequently breach of Non Disclosure of Agreement (NDA) and Memorandum of terms of employment are often attributed to criminal activity by employers which in truth may be a civil violation

V. IDENTITY THEFT

 Identity theft involves fraudulent or dishonest use of someone's electronic signature, password or other unique identification feature.

 It is the first step towards credit card fraud, online share trading scams and e-banking crimes.

VI. INTERNET VIOLATIONS OF COPY RIGHTS

(Internet violation of copyrighted informations like feature films, songs, music etc.IPR theft)

 Posting of features films, part of the films, causing lossto the revenue and criminal violations of Copy Right Act, 1957 often challenges the film industries and law enforcement.

 Uploading happening in Indian servers can be deleted.

 If it is an International server, deletion happens by request. Despite that if persisting, deletion becomes a task of chance and persons behind the activity may not surface at all.

VII. FINANCIAL CRIMES – SPOOFING/PHISHIHG/INTERNET BANKING

(Offender creates/Spoofs, the webpage of a bank or any organization in the guise of enhancing their security or updating the services, collects personal confidential information at various stages and abuses the information for causing wrongful loss, fraudulent transfer of funds in Internet banking)

This is a wide term that includes credit card fraud, online share trading scams and e-banking crimes.

 In today's highly digitalized world, almost everyone is affected by financial crimes.

 Phishing usually involves spoofed emails that contain links to fake websites.

 Spoofing becomes a pre-requisite for causing deceptive belief and it follows phishing of vital information.

 Spoofing of the sites normally happens in bank pages if the intention is for a financial fraud. Other sites get spoofed for misleading the viewer or for causing embarrassment.

 A spoofed page becomes difficult to be distinguished by normal viewers.

 Phishing normally happens for credit card related information or for password details of internet banking.

 Internet Banking requires unique authentication. Forgotten PIN or password option generates new ones if answers to the questions match. New PIN or Passwords reach as mobile SMS, mobile phone security if compromised, criminals then know the precious PIN or Password.

 Fund transfer normally goes to bogus fictitious accounts within the country but far apart in Geography.

 Quick withdrawal happens through short living accounts and the offender manages to open further bogus accounts as a preparation for his future crimes

 Withdrawal happens mostly in ATMs by concealing the identity.

 Banking systems and mobile phone systems provide facilities without proportionate security breeding vulnerabilities.

 The system now is not immune for account opening or for activating a new SIM card by producing forged ID cards and non-existence characters or by impersonation.

 Sheer non-compliance of the KYC norms of RBI and verification norms of TRAI opens wide scope for criminal activities ranging from a disturbance call to a fraudulent fund transfer culminating even as a mean for anti-national activities.

 The following awareness message have been Propagated:

Never respond to unsolicited emails asking for financial information

VIII. WEB PAGE HACKING

(The page gets defaced by altering the content of the file and appearance causing embarrassment and denial of service)

 The primary objective in web page hacking is to deface and embarrass an organization or an institute.

 The intention may extend from causing a denial of service to bringing down a business competitor.

 Government sites get hacked and hackers sometimes claim responsibility for hacking; the intention being to cause defamation and damage to the dignity of the institution.

IX. SPAM / MALWARE / ESPIONAGE

 Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately.

 E-mail spam, known as junk mail, is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

 Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.

 Malware is a wide term that includes viruses, worms, Trojans, rootkits, backdoors, spyware, botnets, keystroke loggers and dialers.

 Cyber espionage is the act of obtaining personal, sensitive proprietary or classified information without permission

 Also known as cyber spying, it involves the use of cracking techniques and malicious software including Trojans and spyware.

X. MOBILE DEVICE ATTACKS

 Threats to the security of mobile devices include unauthorized access, stolen, handsets, data theft, malware, phishing etc.

 Mobile devices are getting more computing power and are becoming increasingly feature rich. This increases the likelihood of attacks against potential vulnerabilities.

XI. DENIAL OF SERVICE

 This involves flooding a computer with more requests than it can handle, causing it to crash.

 In a Distributed Denial of Service (DDoS) attack, the perpetrators are many and are geographically widespread.

XII. SOCIAL ENGINEERING

 A social engineering attack tricks people into revealing passwords or other confidential information by making people believe an unanticipated situation.

 Training the personnel for handling such situations and effectively ensuring the "need to know basis" may be a viable solution.

XIII. VIOLATION OF PRIVACY

(Capturing and publishing the images, pictures and videos of individuals often without the knowledge and concurrence and thereby passing humiliation and embarrassment)

 Normally females victimized in this way by the posting of pictures with an attachment of an unwanted message, often with the phone number to cause incessant disturbance by calls from international strangers.

 Social networking sites like *Orkut* have fairly responded to Police requests by furnishing the IP addresses and log details.

 Face book has proved to be a non-responsive, despite requests not withstanding even if addressed to any of the International organizations like Child Exploitation On-line Protection forums.

 Social networking sites like face book have maintained its unbroken silence if requests for deletion of posted pictures were addressed.

XIV. CYBER TERRORISM

 Cyber terrorism involves the use or threat of disruptive cyber activities for ideological, religious or political objectives

 Cyber terrorism can weaken a country's economy and even make it more vulnerable to military attack.

XV. OBSCENITY & PORNOGRAPHY

(Uploading obscene and lascivious materials in Internet and causing propagation and transmission: abusing children and uploading of images of such abuse)

 International online sharing sites like Rapidshare, megaupload and various sites have provided a nurturing platform for the cultivation, propagation and transmission of the menace of pornography including children.

 Surprisingly sites like Paypal and other online payment sites have been hand in glove with such sites prompting one to infer that there might be a sharing of the proceeds of income by the propagation of pornography.

 Blocking of porno-sites had been a challenge both in technical and legal means because the content can be hosted in a different domain names or in different IP addresses from different geographies of the world.

9. The investigation of cyber crimes is complex. The evidence is often in an intangible form. Its collection, appreciation, analysis and preservation present unique challenges to the Investigator. The increased use of networks and the growth of the Internet have added to this complexity. Using the Internet, it is possible for a person sitting in India to steal a computer resource in Brazil using a computer situated in USA as a launch pad for his attack. Distributed attacks are also not unheard of. The challenges in such cases are not only technological, but also jurisdictional.

10. Of late, we are experiencing more and more of cyber crimes, since many of us have switched over to the fourth mode of communication i.e. Internet from the previous modes viz. gestures, speech and writing. The internet has opened up avenues of commerce, trade and communication like never before. It is the network that deals in billions of transactions each day. These transactions are usually transactions of money, pictures, information and videos. The magnitude of transactions – the sheer volume makes internet not just an easy tool for information exchange, but also an ideal hotbed of crimes.

11. Internet provides anonymity and safety. Unlike other forms of crimes wherein the person undertakes considerable risk, cyber crime provides the criminal with a cover. He leaves no physical foot-prints, finger-prints or other tangible traces making it extremely difficult to track cyber criminals down

12. Cyber crime being technology driven evolves continuously and ingeniously making it difficult for investigators to cope up with changes. Criminals are always one step ahead in the sense that they create technology or come up with technique to perpetrate a particular crime and the law enforcers then counter such techniques or technologies.

13. **Information Technology Act, 2000** & Indian Penal Code

 All cyber crimes do not come under the IT Act.

 Many cyber crimes come under the Indian Penal Code
Sending threatening message by email -Section 506 IPC
Sending defamatory message by email -Section 499 IPC
Sending a mail outraging the modesty -Section 509 IPC

Forgery of electronic records -Section 465 IPC
Bogus websites, cyber frauds, phishing -Section 420 IPC
Email spoofing -Sections 465, 419 IPC
Web-jacking -Section 383 IPC
Criminal breach of trust -Sections 406, 409 IPC

Online sale of Narcotics -NDPS Act

Online sale of Weapons Arms Act

Hacking -Section 66 of IT Act

Pornography -Section 67 of IT Act

Email bombing -Section 66 of IT Act

Denial of Service Attack -Section 43 of IT Act

Virus Attack -Sections 43, 66 of IT Act

PENALTIES AND ADJUDICATION :

The Information Technology (Amendment) Act, 2008, adds 8 offences, 5 of which are added to the Information Technology Act, 2000 and 3 to IPC

15. The new offences are as follow :

Sl.No. Section Description

1 66 As proposed in ITAA, 2008, this Section combines contraventions indicated in Section 43 with penal effect and reduces the punishment from 3 years to 2 years. It also introduces the pre-conditions of "Dishonesty" and "Fraud" to the current Section 66.

2 66 A Punishment for sending offensive messages through communication service, etc.

3 66 B Punishment for dishonestly receiving stolen computer resource or communication device.

4 66 C Punishment for identity theft.

5 66 D Punishment for cheating by personation by using computer resource.

6 66 E Punishment for violation of privacy

7 66 F Punishment for cyber terrorism.

8 67 Punishment for publishing or transmitting obscene material in electronic form.

9 67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

10 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

11 67 C Preservation and retention of information by intermediaries.

12 71 Misrepresentation to the Controller or the Certifying Authority. Making any misrepresentation to or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be.

13 72 Any person who, in pursuance of any of the powers conferred under IT Act, has secured access to any electronic record, book, register, correspondence, information or document without the consen of the person concerned discloses such electronic record, book, register, correspondence, information, document to any other person.

14 73 Publishing Digital Signature Certificate false in certain particulars. Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge that the certifying Authority listed in the certificate has not issued to other subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

15 74 Creation, publication or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose

IMPORTANT SECTIONS OF IT ACT 2000 :

16.1**. Section 44** – Penalty for failure to furnish information, return, etc:- If any person who is required under the Act or any rules or regulations made There under to –

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure,

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations,he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues,

(c) maintain books of account or records fails to maintain the same,he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

16.2. **Section 45** (Residuary penalty) further covers all other offences that may possibly arise under the act. It provides that "whoever contravenes any rules or regulations made under the Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees" to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees

16.3.0. **Section 46** (Power to adjudicate – Adjudicating Officer) empowers the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a Stale Government to be an adjudicating officer for holding an inquiry regarding the commission of the offences laid out in Chapter IX in the manner prescribed by the Central Government.The persons appointed shall possess such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government. Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction. This is also discussed in S.Sekar v. The Principal General Manager (Telecom), (BSNL), MANU/TN/9663/2007**.**

16.3.1. Every adjudicating officer appointed as above shall have the Powers of a civil court which are conferred on the Cyber Appellate Tribunal under

Section 58(2). Further all proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code, 1860 and it shall be deemed to be a civil court for the purposes of **Sections 345** and **346** of the Code of Criminal Procedure, 1973.

16.3.2. The adjudicating officer shall offer the offender a reasonable opportunity for making representation in the matter. If, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of the Act governing such offence

16.4. **Section 47** prescribes the factors to be taken into account by the adjudicating officer while adjudging the quantum of compensation, namely:

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default.

16.5. **Section 65** - Tampering with computer source documents – Who ever knowingly 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 time being in force, shall be punishable with imprisonment up to three years, or

with fine which may extend up to two lakh rupees, or with both. Tampering with computer source documents was discussed in Syed Asifuddin and Ors. v. The State of Andhra Pradesh and Anr., 2005 Cri L J 4314, Jigar Mayurbhai Shah v.State of Gujarat, (2008)2GLR1134, Pootholi Damodaran Nair v. Babu, 2005(2)KLT707, and Ravi Shankar Srivastava v. State of Rajasthan,2005(2)WLC612.

16.6. **Section 66** (Computer related offences)- This Section deals with hacking the Computer System and states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or 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. It further states that whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both. The case of Nirav Navinbhai Shah v. State of Gujarat and Anr., MANU/GJ/8458/2006 involved **Section 66**.

16.7. **Section 67** – Punishment for publishing or transmitting obscene material in electronic form : This Section was in question in Dr. Prakash v. State of Tamil Nadu and Ors., AIR 2002 SC 3533, Fatima Riswana v. State Rep. by A.C.P., Chennai and Ors., (2005) 1 SCC 582, Assistant Commissioner of Police, Crime Record Bureau, Inspector of Police v. Saravanan and others, MANU/TN/1776/2003, Avnish Bajaj v. State (N.C.T.) of Delhi, (2005) 3 Comp L J364(Del), M.Saravanan v. State of Tamilnadu, MANU/TN/8296/2006, and Maqbool Fida Husain v. Raj Kumar Pandey, MANU/DE/0757/2008

16.8. **Sections 76, 68(2), 69** and **70** have been amended by the Information Technology Amendment Act 2008, Also See Firos v. State of Kerala,AIR 2006 Ker 279.

16.9. **Section 71** (Penalty for misrepresentation) This Section prescribes a penalty for any misrepresentation or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate. It states that such cases shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

16.10. **Section 72** (Penalty for breach of confidentiality and privacy)Again if any person who, in pursuance of any of the powers conferred under the Act,rules or regulations made thereunder, has secured access to any electronic record,book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished under **Section 72** with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

16.11**. Section 73** (Penalty for publishing (Electronic Signature) Certificate false in certain particulars) If a Digital Signature Certificate that is false in certain particulars is published or made available by a person to any other person with the knowledge that the Certifying Authority listed in the certificate has not issued it, or the subscriber listed in the certificate has not accepted it, or the certificate has been revoked or suspended, then such person shall be punished under Section 73 with imprisonment for a term which may extend to two years, or with fine which may

extend to one lakh rupees, or with both. A publication that is for the purpose of verifying a digital signature created prior to such suspension or revocation, is not penalized under this Section.

16.12. **Section 74** (Publication for fraudulent purpose). This Section states that whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

16.13. **Section 75** (Act to apply for offences or contravention committed outside India). This Section accords extra territorial application to the Act and states that the provisions of the Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. The Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. As per **Section**

76, any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of the Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation.

16.14. **Section 77** (Compensation, penalties or confiscation not to interfere with other punishment). This Section states that in addition to the penalties prescribed by the IT Act, imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force may also be made. The Act as amended gives a police officer not below the rank of Inspector the power to investigate any offence under the Act.

16.15. **Section 79** (Exemption from liability of intermediary in certain cases)- This Section declares that no person providing any service as a network service provider shall be liable under the 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. This issue was also discussed in the case of Sanjay Kumar Kedia v. Narcotics Control Bureau and Anr., (2008)2 SCC 294.

16.16. The Amendments brought about by the Information technology Act in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 came up for consideration in State of Punjab and Ors. v. Amritsar Beverages Ltd. and Ors., (2006) (7) SCC 7, In Re: Sr. Abaya 2006 Cri.L.J. 3843, SICOM Ltd v. Harjindersingh and Ors., AIR 2004 Bom 337, Vishal Paper Tech India Ltd. And Ors. v. State of A.P. and Anr., 2005Cri L J 1838, Sri. P. Padmanabh v. Syndicate Bank Limited, AIR 2008 Kant 42, Steel Tubes of India v. Steel Authority of India, 2006 Cri L J 1988, V.K. Soman Achari v.: Sabu Jacob and Anr., 2007 Cri L J 1042,
Indira Priyadarshini Forum v. State of Kerala, 2001 Cri L J 2652.

Cyber crimes in India :

17.1. Cyber Crimes have emerged as a serious global threat, forcing governments, police departments and intelligence units to adopt counter measures.

17.2. The CERT (Computer Emergency Response Team), the apex cyber security division under the ministry of information technology of India, found that cyber crime in the country has accelerated about 50 times since 2004.

17.3. The agency recorded just 23 cyber crime incidents in 2004 in contrast to a huge 1,237 in 2007. These primarily included phishing attacks distribution of viruses/malicious code and illegal infiltration to computer networks.

17.4. A high ranking official from the IT ministry told DNA on April 8,2008 that phishing is a kind of fraud in which an online criminal tricks the user and grabs his/her secret online banking details such as account number, or security codes like password to access those accounts.

17.5. Further, according to annual report for 2007 of CERT, there were 392 incidents of phishing, 358 cases of virus proliferation and 223 cases of network infiltration recorded in 2007. Compared to this, there were only 3 phishing attacks, 5 cases of virus proliferation and 11 incidents of network infiltration reported in 2004.

17.6. These statistics from CERT are, however, only indicative without giving the actual picture of cyber crime in India. The agency merely maintains records of cases that are notified to it.

17.7. Furthermore, a data of the government revealed that in January 2008, 87 security related incidents were recorded in contrast to 45 in December 2007. Of these, 47% involved phishing, 25% related to worm/virus under the malware category, 21% to unauthorized scanning, and 7% to technical help under separate categories.

18.0. Tamil Nadu State :

18.1. As far as Tamil Nadu State is concerned, Tamil Nadu Police formed two Cyber Crime Cells in the year 2002 – one in the Central Crime Branch, Egmore for Chennai City and the another in the CBCID Headquarters, Chennai, for the entire state of Tamilnadu. Recently another Cyber Crime cell has been sanctioned for Coimbatore city. It is learnt that Dr.M.Sudhakar, Additional Deputy Commissioner of Police, Central Crime Branch, Chennai, is rendering commendable service in respect of registration of cases in cyber crime as well as its investigation.

18.2. Year wise reported cases Reporting of cases to Cyber Crime Cell has increased due to awareness spread among the Net users regarding the existence of separate investigation agency and a special Act. In particular, cases of Identity theft and cheating through Internet have increased.

Investigation and Computer Forensics :

19.1. In cyber crime cases, the investigator's challenge is to establish the crime beyond reasonable doubt using digital evidence that exist in cyber space. This requires Computer or Cyber Forensics special skills, equipments, lab and capabilities far different from conventional crime detection.

19.2. Computer forensics is extremely important to track and establish proof in all computer related offences. According to **Section 79A** of the Information Technology Act, 2000, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines The computer forensic field has developed techniques to improve the detection, connection, and classification of digital information. Thus the field includes a multitude of systems to extract useful information from computer media and involves the application of varied tools.

The stages in computer forensic investigation are usually as follows:

1. Identifying the doer of the crime.

2. Locating the means and equipment through which the crime was committed

3. Collection and extraction of the physical evidence

4. Correlating the evidence to the crime and facilitating the arrest of the Wrong doer. Chain-of-custody is one of the controls used by courts to satisfy admissibility standards. Chain-of-custody is a process consisting of methodical checklists and procedures during the collection, preservation and analysis of evidence for the purpose of establishing authenticity and reliability of evidence. In other words, the evidence offeror tries to prove the chain-of-custody in order to rebut or minimize charges that evidence may be tainted or altered.

19.4. Thus the authenticity of physical evidence is shown by accounting for who, what, when, where and how a given piece of evidence was transferred from its initial discovery, through its collection, access, handling, storage and eventual presentation at trial. Chain-of-custody has been institutionalized as a procedure for the seizure of physical evidence by law enforcement, as well as for the handling of digital evidence by computer forensic examiners as a measure of evidence integrity.

19.5. The Cyber Crime Investigating Officers are enhancing their technical knowledge by undergoing periodical training organized by Central Bureau of Investigation Academy (CBI), Chaziabad, Tamil Nadu Police Academy (TNPA),Chennai, (Tamil Nadu Police Officers), Government Examiner of Questioned Documents (GEQD), Hyderabad, Centre for Development of Advanced Computing (C-DAC), Thiruvananthapuram, National Association of Software and

Services Companies (NASSCOM), Chennai, Anna University, Chennai and Computer Emergency Response Team-India (CERT-IN), New Delhi.

PREVENTION METHODS

2.1 PREVENTIVE STEPS FOR INDIVIDUALS

2.1.1. CHILDREN:

Children should not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not give photographs to anyone on the Net without first checking or informing parents guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to –face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

2.1.2 PARENTS:

Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol. There is also software to establish time controls for use of limpets (for example blocking usage after a particulars time) and allowing parents to see which site item children have visited. Use this software to keep track of the type of activities of children.

2.1.3. GENERAL INFORMATION:

Don't delete harmful communications (emails, chats etc). They will provide vital information about system and address of the person behind these.

 Try not to panic.

 If you feel any immediate physical danger contact your local police.

 Avoid getting into huge arguments online during chat and discussions with other users.

 Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful.

 Be extremely careful about how you share personal information about yourself online.

 Choose your chatting nickname carefully so as others.

 Do not share personal information in public space online; do not give it to strangers.

 Be extremely cautious about meeting online introduced person. If you choose to meet, do so in a public place along with a friend.

 If a situation online becomes hostile, log off and if a situation places you in fear, contact local police.

 Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

2.2 PREVENTIVE STEPS FOR ORGANISATIONS AND GOVERNMENT

2.2.1 PHYSICAL SECURITY:

Physical security is most sensitive component, as prevention from cyber crime Computer network should be protected from the access of unauthorized persons.

2.2.2 ACCESS CONTROL:

Access Control system is generally implemented using firewalls, which provide a centralized point from which to permit or allow access. Firewalls allow only authorized communications between the internal and external network.

2.2.3 PASSWORD:

Proof of identity is an essential component to identify intruder. The use of passwords in the most common security for network system including servers, routers and firewalls. Mostly all the systems are programmed to ask for username and password for access to computer system. This provides the verification of user. Password should be charged with regular interval of time and it should be alpha numeric and should be difficult to judge.

2.2.4 USING ENCRYPTION: - Encryption is able to transform data into a form that makes it almost impossible to read it without the right key. This key is used to allow controlled access to the information to selected people. The information can be passed on to any one but only the people with the right key are able to see the information. Encryption allows sending confidential documents by E-mail or save confidential information on laptop computers without having to fear that if someone steals it the data will become public. With the right encryption/decryption software installed, it will hook up to mail program and encrypt/decrypt messages automatically without user interaction.

2.2.5 FINDING THE HOLES IN NETWORK:

System managers should track down the holes before the intruders do. Many networking product manufactures are not particularly aware with the information about security holes in their products. So organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed.

2.2.6 USING NETWORK SCANNING PROGRAMS:

There is a security administration's tool called UNIX, which is freely available on Internet. This utility scans and gathers information about any host on a network, regardless of which operating system or services the hosts were running. It checks the known vulnerabilities include bugs, security weakness, inadequate password protection and so on. There is another product available called COPS (Computer Oracle and Password System). It scans for poor passwords, dangerous file permissions, and dates of key files compared to dates of CERT security advisories.

3.0 DETECTION: Cyber crime is the latest and perhaps the most specialized and dynamic field in cyber laws. Some of the Cyber Crimes like network Intrusion are difficult to detect and investigation even though most of crimes against individual like cyber stalking, cyber defamation, cyber pornography can be detected and investigated through following steps:

After receiving such type of mail

(1) Give command to computer to show full header of mail.

(2) In full header find out the IP number and time of delivery of number and this IP number always different for every mail. From this IP number we can know who was the Internet service provider for that system from which the mail had come.

(3) To know about Internet Service Provider from IP number take the service of search engine like nic.com, macffvisualroute. Com, apnic.com, arin.com.

(4) After opening the website of any of above mentioned search engine, feed the IP number and after some time name of ISP can be obtained.

(5) After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender.

(6) ISP will provide the address and phone number of the system, which was used to send the mail with bad intention.

After Knowing the address and phone number criminal can be apprehended by using conventional police methods.

4.O CYBER LAW

India has enacted the first I.T.Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United Nations. Chapter XI of this Act deals with offences/crimes along with certain other provisions scattered in this Acts .The various offences which are provided under this chapter are shown in the following table: -

Un-authorised access to protected system Sec.70 Breach of Confidentiality and Privacy Sec.72

Publishing false digital signature certificates Sec.73

NOTE: Sec.78 of I.T.Act empowers Deputy Supdt. Of Police to investigate cases falling under this Act.

4.2 Computer Related Crimes Covered under IPC and Special Laws
Offence Section

Sending threatening messages by email Sec 503 IPC

Sending defamatory messages by email Sec 499 IPC

Forgery of electronic records Sec 463 IPC
Bogus websites, cyber frauds Sec 420 IPC
Email spoofing Sec 463 IPC
Web-Jacking Sec. 383 IPC
E-Mail Abuse Sec.500 IPC
Online sale of Drugs NDPS Act
Online sale of Arms Arms Act

5.0 ELEMENTARY PROBLEMS ASSOCIATED WITH CYBER-CRIMES:

One of the greatest lacunae in the field of Cyber Crime is the absence of comprehensive law any where in the World. The problem is further aggravated due to disproportional growth ratio of Internet and cyber laws. Though a beginning has been made by the enactment of I.T. Act and amendments made to Indian Penal Code, problems associated with cyber crimes continue to persist.

1. Jurisdiction is the highly debatable issue as to the maintainability of any suits, which has been filed. Today with the growing arms of cyber space the territorial boundaries seem to vanish. Thus the concept of territorial jurisdiction as envisaged under S.16 of Cr.P.C. and S.2.of the I.P.C. will have to give way to alternative method of dispute resolution.
2. Loss of evidence is a very common & expected problem as all the data are routinely destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.
3. Cyber Army: There is also an imperative need to build a high technology crime & investigation infrastructure, with highly technical staff at the other end.
4. A law regulating the cyber-space, which India has done.
5. Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provision recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.
6. Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such case, which needs appreciation, is the P.I.L. (Public Interest Litigation), which the Kerala High Court has accepted through an email.

'Perfect' is a relative term. Nothing in this world is perfect. The persons who legislate the laws and by-laws also are not perfect. The laws therefore enacted by them cannot be perfect. The cyber law has emerged from the womb of globalisation. It is at the threshold of development. In due course of exposure through varied and complicated issues it will grow to be a piece of its time legislation.

CHAPTER 8

Case Study

It is not so easy and possible to eliminate cyber crime once for all in view of the latest scientific development. However, it is quite possible to combat and check the cyber crimes. To achieve that object, the first and foremost requirement is the awareness among the public about the cyber crimes and the precautions to prevent the same.

20.1. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advises the five "P" mantras for online security, viz., Precaution, Prevention, Protection, Preservation and Perseverance. A Citizen should keep in mind the following things :-

1.to prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.

2.always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

3.always use latest and up date anti virus software to guard against virus Attacks

4.always keep back up volumes so that one may not suffer data loss in case of virus contamination

5.never send your credit card number to any site that is not secured, to guard against frauds.

6.always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

7.it is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

8.web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

9.use of firewalls may be beneficial.

10. web servers running public sites must be physically separate protected from internal corporate network.

20.2. In respect of using mobile phones, the public should not be carried away by S.M.S. messages offering attractive gifts and thereby inducing to part with huge amounts. Recently in a case at Chennai, a woman having been attracted by a S.M.S. message incurred a loss of Rs.57/- lakh as she was promised a huge sum of money. It is better to record the following news item

"Woman falls for SMS offer, loses Rs. 57 lakh

S. Vijay Kumar *She was promised a huge prize money Gang operated from India and abroad*

CHENNAI: A woman who responded to an SMS was relieved of Rs.57 lakh by a gang that operated from India and abroad.

The 52-year-old graduate of Mylapore, who was promised a huge prize money as part of the 'World Cup Promotion Draw,' deposited the money in different bank accounts over a period of one month, starting third week of May. After realizing the fraud, she lodged a complaint with the police.

According to police sources, the woman received an SMS in May second week, stating that she had won a cash prize worth a few crores of Indian currency. She responded to the email account that was mentioned in the SMS.

Days later, the complainant received an email in which the accused persons said the money would be delivered in India after obtaining necessary clearance from different agencies, including the United Nations and the Reserve Bank of India. They communicated the movement of the person bringing the cash box and asked her to deposit her money in various bank accounts for obtaining clearance from the immigration and customs authorities. A majority of the accounts into which the woman deposited money, ranging between Rs. 87,000 to Rs. 7.5 lakh, were opened in ICICI Bank. When there was no trace of the prize money even after depositing Rs.57 lakh, the victim lodged a complaint with Commissioner of Police T. Rajendran last week who directed the Central Crime Branch to form a special team and investigate the case.

"A major portion of the money was deposited in the accounts of Zulfikar

Zariar, Javed Khan and Imran Zari. We have written to ICICI Bank to share the details

of these account holders. The money was drawn from ATMs across the country including New Delhi and Mumbai. Video footage recorded by cameras in ATM

machines could provide a clue to the identity of the suspects," an investigator told The

Hindu.

"One of the accounts from which emails were sent was

ukembassyact@yahoo.com. When contacted, Yahoo asked us to get in touch with lawenforcing

agencies in the United States to get the user details," he said. Police suspect

that the accused used fictitious names and documents to open bank accounts."

20.3. The above case is only a tip of the iceberg. Therefore, the public

should not only be aware about the effective functioning of the cyber crime cells,

but they should also be vigilant in preventing such cases.

At 20,Sunny solved 15 cases of Cyber Crimes of Ahmedabad Crime Branch like Phishing Cases, Biggest Data Theft Case, Espionage Case, Credit Card Fraud Case, Several Orkut Fake Profile Impersonation Cases, Email Hacking Cases, SMS Spoofing Cases, Cyber Pornography Case,Cyber Terrorism Case, Several 419 Nigerian Fraud Case,**etc.**

Ahmedabad Blast Case Study
Sunny Vaghela helped Crime Branch, Ahmedabad to Trace origin of the Terror Mails sent during Ahmedabad Serial Bomb Blasts. Following are the details.

First Mail was sent on 26th Jully,2008 from Email Id alarbi_gujarat@yahoo.com from IP Address. 210.211.133.200 which traced to Kenneth Hawood's House at Navi Bombay.His Unsecured WIFI router was misused by terrorists to send terror mail from his router.As log system is disabled, we were unable to find out the details of the MAC address of the culprit.

Second Mail was sent on 31st July,2008 from alarbi_gujarat@yahoo.com from IP Address: 202.160.162.179 which traced out to Mediacal College at Vaghodiya,Baroda,Gujarat India. It

was little bit difficult to trace this mail as the mail has been sent using proxy server & fake mail script but finally I traced out the original IP address.\

Third Mail was sent on 23rd August,2008 from alarbi.alhindi@gmail.com from IP address: 121.243.206.151 which traced to Khalsa College at Bombay. Again Unsecured WIFI router was misused to send an email.

Forth Mail was sent on 13th September,2008 from al_arbi_delhi@yahoo.com which traced to Kamran Power Limited at Bombay. In this case also WIFI router was misused to send the threatning mail.

:Some Points to be noted for WIFI users while surfing Internet:

Don't Configure WIFI Router as Unsecured Connection, It can be misused by someone.

ISP configure your phone number/mobile number as default Network Key in Router in normal case. one should change it as soon as possible if so.

If router is configured as an Unsecured Connection then enable the logging system. This helps you to get MAC (Media Access Control) address of the machines which uses your wifi router.

If router is Configured as an Unsecured Connection then kindly install packet capturing software or WLAN analyzing software so that you can keep eye on machines which gets an unauthorize your wifi router.

If router is configured as an Unsecured Connection then bind your MAC address with the router. This will only allow your laptops to get connected to router.

Protect Your SSIDS & Dont use WEP while configuring your router.

Dont ever use viral networks like "Free internet" Or "wifi" Network because those networks are designed to steal your data from laptop.
Maintain All types of Logs for atleast 6 months.

:Some Points to be noted by ISPs:

ISP should maintain Event Log, Security Log & Surfing Activity logs for atleast 6 months so that activities of any registered subscriber can be traced out within seconds.

ISP should verify the customer information when anyone register for internet service. In many Cyber Crime Cases we found internet connection registered on fake identities/proofs.

Some ISPs have installed WIFI hotspots at Restaurants/Coffee shops/Shopping Malls/Hotels. One can buy prepaid internet card to use the service without submitting any proof or documents. ISP should asked for some photo identity proof before issuing prepaid card.

ISP should give an access to Govt. Authority & Investigation agencies to their real time dynamic IP address database so that it can be traced out within seconds.

ISP should put filtering mechanisms in their event logs for words being used like ‘al arbi’,’jihad’,’indian mujahideen’ . Govt agencies must be alerted when someone register email id with combination of any of above key words. Email Service Providers also take this into consideration.

Mumbai Blasts Case

After Mumbai Bombings, he had successfully accomplished task of getting confidential information on the banned organization **JAMAT ud DAWAH** for **One of the investigating agencies.** He was also appreciated for the same.

Phishing Case Study

One Doctor from Dehgam,Gujarat had registered a crime stating that some persons (“perpetrators”) have perpetrated certain acts through misleading emails ostensibly emanating from ICICI Bank’s email ID. Such acts have been perpetrated with an intent to defraud the Customers.

The investigation was carried out with the help of the mail received by the customer, bank account IP details & domain IP information, the place of offence at Merrut was searched for evidence.

The case was registered under section 406,419,420 of IPC & 65,66, of IT Act,2000 at D.C.B Police station which attract imprisonment of upto 3 years of jail & 2 lakh of fine which accused never thought of.

Data Theft Case Study

It could well be biggest DATA THEFT case in the country. Florida(USA) based Firm has registered crime stating that Ahmedabad based BPO had theft database from their server & illegally selling to company’s clients & competitors .They also claimed that IT company owner had taken this step in response to cancellation of business contract of development & maintenance of the company’s one of the portals.

The investigation was carried out by Sunny Vaghela with the help of mail received by company’s competitors & server of US based firm. All digital evidence was collected by Sunny & ACP, Crime Branch, Ahmedabad.

The place of offence was raided & accused had been arrested. Accused contacted more than 20 clients to sell the database. Finally all computers & media disks had been seized from him.

The case was registered under section 406,420 of IPC & 65,66,72 of IT Act,2000 at D.C.B Police station, Ahmedabad.

Cyber Stalking Case

Sunny Vaghela traced out origin of the email sent to Mr.Narendra modi,Chief Minister,Gujarat on 17th January,2009.

Orkut Profile Impersonation Case

Four girls from well known Engineering Institute of Gujarat has registered crime with Crime Branch,Ahmedabad stating that their fake profile was made on orkut & porn pics are also posted. they also stated that the person was adding their friends & using abusive language on the Internet.

The investigation was carried out by Sunny Vaghela.The case has been registered under section 419(a) & 67 of IT Act,2000 at D.C.B Police Station, Ahmedabad.

SMS Spoofing Case

One Guy named Ankit was getting SMS from his fiancée's Number for atlease 5 times a day.

The Investigation was carried out by Sunny Vaghela .IP address of the culprit was traced out within one day.The accused was found to be neighbor of Ankita.

The case was registered under section 419A ,66(a),72 of It act at D.C.B Police station
Detailed Case Study of the Biggest data Theft Case,Credit Card Fraud Case,Call forging Case, NIgerian Fraud case,job fraud case will be uploaded soon..Thanks for visiting..Please check back this page soon.

Insulting Images of Warrior Shivaji on Google – Orkut

An Indian posts ‘insulting images’ of respected warrior-saint Shivaji on Google’s Orkut. Indian police come knocking at Google’s gilded door demanding the IP address (IP uniquely identifies every computer in the world) which is the source of this negative image. Google, India hands over the IP address.

No such incident in India would be complete without a few administrative slip-ups. The computer with that IP address is using Airtel, India as the ISP to connect to the internet and Orkut. Airtel gives police the name of an innocent person using a different IP address. How two IP addresses could be mixed-up in a sensitive police case is anyone’s guess.

An innocent Indian, Lakshmana Kailash K, is arrested in Bangalore and thrown in jail for 3 weeks. Eventually, his innocence is proved and he is released in Oct, 2007.

A number of news media report this incident. American citizen and India lover Christopher Soghoian (home page http://www.dubfire.net/chris/) studies Informatics at Indiana University and researches/writes about security, privacy and computer crime. Christopher does an excellent article on this topic for the blogs at respected tech media group CNET.

Like all good writers, Christopher Soghoian, gives Google, India a list of questions so that he can give a balanced perspective to the millions of CNET readers.

How does Google, India respond?

The only comment was: "Google has very high standards for user privacy and a clear privacy policy, and authorities are required to follow legal process to get information. In compliance with Indian legal process, we provided Indian law enforcement authorities with IP address information of an Orkut user."

Not surprisingly, Google is a keen to play this down as Yahoo is being hauled over the coals by US Congress for handing over an IP addresses and emails to the Chinese Government which resulted in a Chinese democracy activist being jailed.

Techgoss contacted Christopher and asked him for a list of the questions he had put to Google. The following were the questions that Christopher put to Google which were never answered. Sometimes what you do not say says more about what you have done.

1. Can Google speak at all to the specifics of this incident?

2. If so, can Google confirm if they released ip addresses or any other log information to the Indian police regarding this incident.

3. If Google did hand over log information, did the Indian police have a warrant/court order, or did they merely request it?

4. Does Google feel in any way responsible for the man's accidental arrest and jailing?

5. Speaking more generally, without going into the specifics of this incident...Has Google ever in the past handed over user information (including logs) to Indian law enforcement/authorities without a court order/search warrant?

6. In this case, the crime the man was accused of (defaming a 300 year old historical figure) does not exist in the US. Will Google conform to the laws of each country it does business in, or will it defer to American concepts of freedom of speech and the press?

7. Does Google reveal information to other countries for "crimes" that would not normally be an illegal in the US? For example, the ip addresses of people in Saudi Arabia and other conservative Muslim countries who search for adult, consensual pornography?

8. Is the log data for Orkut stored in India, or is it stored elsewhere? If the data is not stored in India, is Google still responsible for giving it to the Indian authorities?

How does it Airtel react to rectify its mistake?

Firstly, with an immediate, unqualified apology. In itself, a positive first step.

Techgoss (techgoss.com) had heard rumors about Airtel also offering monetary compensation to the person wrongly jailed. But Airtel is being coy about possible financial compensation. An Airtel spokesperson issued the following statement to techgoss.com

"Airtel are aware of this incident and deeply distressed by the severe inconvenience caused to the customer. We are fully cooperating with the authorities to provide all information in this regard and we are in touch with the customer. We have robust internal processes, which we review frequently to make them more stringent. We have conducted a thorough investigation of the matter and will take appropriate action".

Does this mean the customer will get compensation? It is not clear either way. Let's wait and see. It is interesting to see that despite the arrest he is still with Airtel. Now that's loyalty to your telecom company.

CHAPTER 9

COMPARISON OF I.T. ACT INDIA WITH U.K

If we want to compare the law of developed countries and Indian law gives a clear picture that the Indian laws need to be analysed and reviewed in order to maintain law and regulations. It is clear that UK has its Data Protection Act of 1998 wherein the Act is basically designed to provide protection and privacy to the personal data of the individuals residing in UK . According to the Data Protection Act, the people and Organizations involved in storing personal data should register with the information commissioner, who is been appointed by the government as an official of the government in order to keep a check on the rules and regulations provided by the Act. The Act has certain restriction in the collection of personal data. Any personal data can be demanded only for one or more lawful purposes and cannot be further processed or used apart from the task/tasks that it was needed for. The personal data should not be excessive and should be relevant and correct and adequate for the purpose/purposes it is needed and to be processed. It is quite evident that the European Union and U.S try to protect the Personal data of their citizens as the Data Protection Act is much sophisticated and moreover they keep on trying to enhance their system. Though US have a different methodology from what the European Union follows for the Data Protection and Privacy. US follow the sectoral approach that consists of mixed legislation and regulations and self regulations also. Data is grouped in several classes on the basis of their utility in US. Hence a different law structure is followed for each class of data. While the provision in the Indian IT Act deals with extraction of data, destroying the data etc. which means that companies don't get protection of data which forces them to lead towards separate private contracts to keep their data secured. The European Union follows and forces the Protection of personal data on all its countries and the US also complies with the European Union as by the Safe Harbour Agreement can business be facilitated from the European Union countries. Hence it is very necessary for India to comply with the European Union. Though efforts have been made to have a Data Protection Act in India still the

legislature is unable to frame the Bill. The Bill is a complete draft of the UK data protection Act but according to the today's requirement more comprehensive Act is needed. Thus the US approach of

data protection can be also being followed to get fully equipped with today's requirements. The IT act protects credit data which is one of the personal data aspects. Hence unauthorised use or transfer of data or information should only be used to identify the credit worthiness of the customer and should be processed further. Any part of legislation is not sufficient and hence a comprehensive and complete data protection Act is needed in India where information Technology Act, 2000 is not a data or privacy related act as it does not have all the principles of the data protection and privacy. The IT Act, 2000 is a generic Act which has concentrates on things like the digital signatures, cyber contraventions and offences, e-governance, confidentiality. It is mistaken and is wrongly compared to the European Directive on Data Protection (EC/95/ 46), OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data and the Safe Harbour Approach of the US. The fact is that the IT Act, 2000 deals with the issue of the Data Protection and privacy in a partial way. There is a lack of actual framework in the IT Act, 2000 wherein the Data Protection Authority and quality and transparency of the data are considered. Even if the IT Act, 2000 adopts some new amendments still there would be a lack of the actual framework for data protection and privacy that should match the EU directive, OECD Guidelines or the Safe Harbour Principles. The absence of Data Protection Law in India is a heavy loss to the outsourcing industry as though it is a flourishing industry in India but does not have a proper Data Protection Act. The customers in the US and European Union are protected by the comprehensive privacy directive which requires that the personal data cannot be transferred to countries which do not have adequate protection policy. As a result the European trade Union finds that data protection is a major issue which has to be taken into consideration in these international out-sourcing companies. Hence this may lead to a block in the out- sourcing industry in India. Hence India needs to handle this situation tactfully and should consider the importance for the need of a Data Protection Act.

CHAPTER 10

REFERENCES

1. Mohammed Nyamathulla Khan, 2009, Does India have a Data Protection Law Available from website: [Online]

http://www.legalserviceindia.com/article/l406-Does-India-have-a-Data-Protection-law.html

[Accessed on 28th June 2011]

2. CRID – University of Namur, 2005, Section 43. Penalty for damage to computer, computer system, etc., pg 31 Available from website:

[Online]

http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf [Accessed on 11th Julyl 2011]

3. CRID – University of Namur, 2005, Section 65 Tampering with source document, pg 31-32 Available from website: [Online]

http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf [Accessed on 15th July 2011]