Information technology act

We have new remissions like cyber world, entities, e-transaction, e-banking, e-return and e- contracts. Apart from positive side of e-revolution there is seamy side also as computer; internet and CIT in the hands of criminals has become weapon of offence. Accordingly a new branch of Jurisprudence emerged to tackle the problems of cyber crimes in cyber space I. E. Cyber Law or Cyber Space Law or Information Technology Law. For the first time, a Model Law on E-commerce was adopted in 1996 by United Nations Commission on International Trade and Law (UNCRITICAL).

It was further adopted by the General Assembly of the United Nations by passing a solution on 31st January, 1997. Further, India was also a signatory to this Model Law and had to revise its national laws as per the said model law. Therefore, in May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on the 9th June, 2000 and came to be known as the Information Technology Act, 2000. 1. 1 Reasons for enactment of IT act: National: a.

Increasing use of Sits in conducting business transactions and entering into contracts, because it was easier, faster and cheaper to store, transact and monomaniac electronic information than the traditional paper documents. B. Business people were aware of these advantages but were reluctant to interact electronically because there was no legal protection under the existing laws. International reasons: a. International trade through electronic means was growing tremendously and many countries had switched over from traditional paper based commerce to e-commerce. . The United Nations Commission on International Trade Law (UNCRITICAL) had adopted a Model Law on Electronic Commerce in 1996, so as to bring uniformity in laws

governing e-commerce across the globe. . India, being a signatory to UNCRITICAL, had to revise its national laws as per the said model law. Therefore, India also enacted the IT Act, 2000. D. Because the World Trade Organization (WTFO) was also likely to conduct its transactions only in electronic medium in future. 1. 2 Objectives of IT Act: 1 .

To provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means commonly referred to as “ electronic commerce”, which involves the use of alternatives to paper- based methods of communication and storage of information. . To provide legal recognition of electronic records and digital signatures. 3. To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (DEED’) and other means of electronic communication. . To provide legal recognition to business contacts and creation of rights and obligations through electronic media. 5. To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates. 6. To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions. . To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies.

This would also make the citizen-government interaction more hassle free. 8. To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions. 9. To amend the Reserve Bank of India Act, 1934 so as to

facilitate electronic fund transfers between the financial institutions. 10. To amend the Banker’s Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks. . 3 structure of ‘ ATA 2008 act: 1. I. T Act totally has 13 chapters and 90 sections. 2. The Act begins with preliminary and definitions and from there the chapters that follow deal with authentication of digital signatures, electronic records, electronic signatures etc. 3. The civil offence of data theft and the process of adjudication and appellate procedures have been described. 4. Elaborate procedures for certifying authorities (for digital certificates as per IT Act -2000 and nice replaced by electronic signatures in the IOTA -2008) have been spelt out. . Then the Act describes some of the well-known cyber crimes and lays down the punishments thereof. 6. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described. 7. Rules and procedures mentioned in the Act have also been laid down in a phased manner, with the latest one on the definition of private and sensitive personal data and the role of intermediaries, due diligence etc, being defined as recently as April 2011. . 4 Terminologies with reference to IT act: Computer: ‘ 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.

Computer System: “ computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not regrettable and capable of being used in conjunction with external files, which contain computer programmer, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions; Communication Devices: Similarly the word ‘ communication devices’ inserted in the IOTA-2008 has been given an inclusive definition, taking into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc like what was later being marketed as I Pad or other similar devices on WI-FL and cellular models.

Communication Network: The word Communication Network as defined in IOTA-2008 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 (it) Terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained Intermediary: 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 NY service with respect to that record and includes telecoms service providers, network service providers, internet service providers, hobnobbing service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes Information: Information includes data, text, images, sound, voice, codes, computer programmer, software and databases or

micro film or computer generated micro fiche. Data: Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. 1. 5 Need for amendment: TIT, 2000 was an Act of extensive debates, elaborate reviews and detailed criticisms.

Further, a rapid increase in the use of computer and Internet gave rise to new forms of crimes like, sending offensive emails and multimedia messages, child pornography, cyber terrorism, publishing sexually explicit materials in electronic arm, breach of confidentiality and leakage of data by intermediary, e-commerce frauds like cheating by perspiration – commonly known as pushing, identity theft, frauds on online auction sites, etc. So, penal provisions were required to be included in the Information Technology Act, 2000. Also, the Act needed to be technology- neutral to provide for alternative technology of electronic signature for bringing harmonistic with Model Law on Electronic Signatures adopted by United Nations Commission on International Trade Law (UNCRITICAL) Thus the need for an amendment – a detailed one – was felt for the I. T. Act. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I. T. Act and comparing it with similar legislations in other nations and to suggest recommendations.

Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures; the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008. This Amendment Act got the President assent on 5 Feb. 2009 and was made effective from 27 October 2009. 2. SOME IMPORTANT TERMS: 2. 1 Digital signature: The Information Technology Act, 2000 validates " DIGITAL SIGNATURE" and provides for enabling a person to use it Just like the traditional signature. Digital signature is a secure method of binding the identity of the signer with electronic record or message.

The basic function of digital signature is to authenticate the document, to identify the person and to make the contents of the document binding on person putting digital signature. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in arrant. It is a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means you know who created the document and you know that it has not been altered in any way. Digital Signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.

Authentication is the process of verifying that information is coming from a trusted source. These two processes work in tandem for digital signatures. There are several ways to authenticate a person or information on a

computer: 1 . A Digital Signature authenticates electronic documents in a similar manner a handwritten signature authenticates printed documents. For example in the US, the budget, public and private laws that are printed by the Government printing Post have digital signatures which verifies that indeed they are prepared by the GPO. 2. This signature cannot be forged and it asserts that a named person wrote or otherwise agreed to the document to which the signature is attached. 3.

Digital signature enables the " authentication" and " non-repudiation" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message. Legal provisions relating to digital signature: The IT Act, 2000 contains following provisions relating to digital signature: a. Authentication of electronic records Any subscriber may authenticate an electronic record by affixing his digital signature. B. Authentication by use of asymmetric crypto system and hash function The authentication of electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record onto another electronic record. C.

Verification of electronic record Any person by the use of public key of the subscriber can verify the electronic record. The private key and the public key are unique to the subscriber and constitute a functioning key pair. For Example: 2. 2 Electronic signature: Electronic signature is a wide term and it refers to various methods by which one can sign an electronic record. It may take many forms and could be created by different technologies. It can be as basic as a typed name or a digitized image off handwritten signature. Consequently, e-signatures are very problematic with regards o maintaining

integrity and security, as nothing prevents one individual from typing another individual’s name.

Due to this reality, an electronic signature that does not incorporate additional measures of security (the way digital signatures do, as described above) is considered an insecure way of signing documentation. The term “ electronic signature” is defined under section 2(TA) of the IT Act 2000 (as inserted by Information Technology Amendment Act 2008 (IOTA) as follows : “ Electronic signature” means authentication of any electronic record by a subscriber by means f the electronic technique specified in the second schedule and includes digital signature”. Major amendments of IT act include adoption of electronic signatures as a legally valid mode of executing signatures.

This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone. Thus, if you simply write your name and say “ l sign” that will be sufficient to constitute electronic signature but obviously it is not at all safe or secure. The person can always say that some other person typed his name in the document without his consent or knowledge. Here, the digital signature plays an important role as the same is secure and the person cannot be allowed to deny that he did not sign unless he prove with clear evidence that it was put without his consent or knowledge. 2. 3 E-Governance: Chapter 3 of the IT Act, 2000 (Sections 4-AAA) deals with e-governance.

E-governance is the application of Sits to the processes of government functioning so as to have simple, accountable, speedy, responsive and transparent governance. The word electronic” in the term e-Governance implies technology driven governance. E- Governance is the application of information and communication technology (ACT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between Government-to-citizens (GIG), Government-to-Business(GAB), Government-to- Government(GIG) as well as back office processes and interactions within the entire government frame work. Through the e-Governance, the government services will be made available to the citizens in a convenient, efficient and transparent manner.

The here main target groups that can be distinguished in governance concepts are Government, citizens and businesses/interest groups. In e-Governance there are no distinct boundaries. Generally four basic models are available-Government to Customer (Citizen), Government to employees, Government to Government and Government to Business. The act provides for legal recognitions of electronic records and digital signatures in Government and its agencies. The essence of E-governance is to reach the beneficiary and ensure that the services intended to reach the desired individual has been met with. The main objective of e-governance is to simplify and improve governance and enable people’s participation in governance through mail and internet.

E-governance is not only providing information about the various activities of the government to its citizens and other organizations but it involves citizens

to communicate with government and participate in government decision-making. E-governance is applied in following ways: a. Putting government laws and legislations online. B. Putting information relating to government plans, budgets, expenditures and performances online. C. Putting online key Judicial decisions like environment decisions etc. Which are important to citizens and create precedence for future actions. D. Making available contact addresses of local, regional, national and international officials e. Making available the reports of enquiry committees or commissions online.

For example: Guardroom (Restaurants): This project was developed in Debra Rampart (near Jasper) and it provides various online facilities to the villagers, like Sambaing (copies of land records), Shakiest online, Grammar (rural e-mail account), Mindanao (online rates), Grammar (village bazaar), Vivacity (matrimonial service), Pedantry (application for driving license), ann. loans and ration cards and Pram Patria (issuance of domicile for caste, income certificate) etc. 2. 4 Certifying Authority: According to section 24 under Information Technology Act 2000 “ Certifying Authority” means a person who has been granted a license to issue Digital Signature Certificates. A Certifying Authority is a trusted body whose central responsibility is to issue, renew and provide directories of Digital Certificates. In real meaning, the function of a Certifying Authority is equivalent to that of the passport issuing office in the Government. A passport is a citizen’s secure document (a “ paper identity”), sued by an appropriate authority, certifying that the citizen is who he or she claims to be.

Similar to a passport, a user’s certificate is issued and signed by a Certifying Authority and acts as a proof. Anyone trusting the Certifying Authority can

also trust the user’s certificate. The IT Act 2000 gives details of who can act as a CA. Accordingly a prospective CA has to establish the required infrastructure, get it audited by the auditors appointed by the office of Controller of Certifying Authorities, and only based on complete compliance of the requirements, a license to operate as a Certifying Authority can be obtained. The license is issued by the Controller of Certifying Authority, Ministry of Information Technology, Government of India. 3. CYBER CRIMES: 3. Introduction The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provided equal opportunities to all the people to access any information, data storage, analyses etc. With the use of high technology. Due to increase in the number of cybernetics, misuse of technology in the cyberspace was clutching up which gave birth to cybercafés at the domestic and international level as well. Cyber Crime is not defined officially in IT Act or in any other legislation. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and related legislations. Hence, the concept of cyber crime is Just a combination of crime and computer. Cyber Crime is “ unlawful acts wherein the computer is either a tool or target or both”.

Cyber crime may be defined as a criminal offense on the Web, a criminal offense regarding the Internet, a violation of law on the Internet, an illegality committed with regard to the Internet, breach of law on the Internet, computer crime, contravention through the Web, irruption regarding Internet, criminal activity on the Internet, disrupting operations through malevolent programs on the Internet, stalking victims on the Internet, theft

of identify on the Internet. Most cybercafé is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. Cybercafés also includes criminal activities done with the use of computers which further perpetuates crimes I. Financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc. 3. 2 Types of cyber crimes: Amongst many different types of cyber crimes such as cracking, e-mail spoofing, carding, cyber defamation, cyber squatting etc. Two are explained here in detail. 1. Hacking: It is the act of gaining unauthorized access to a computer system or network and in mom cases making unauthorized use of this access. Any person who trespasses any computer, computer system, computer network or any part thereof, knowingly, with malicious intentions to gain access or use or makes an attempt to access or use is said to have committed a crime Malicious purpose may include: Money laundering, obtaining money, theft.

Fraudulent pretences or representations Formulating and executing any fraudulent scheme For example: Using the computer as a distribution point for spam, downloading files from the computer, stealing account info for various services, putting a virus on someone’s PC, smart phone etc. When a person X gains unauthorized access to the gamma account of Y and denies access to Y. In this case X is the hacker. 2. Pushing: Pushing is a form of

social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by camouflaging as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message.