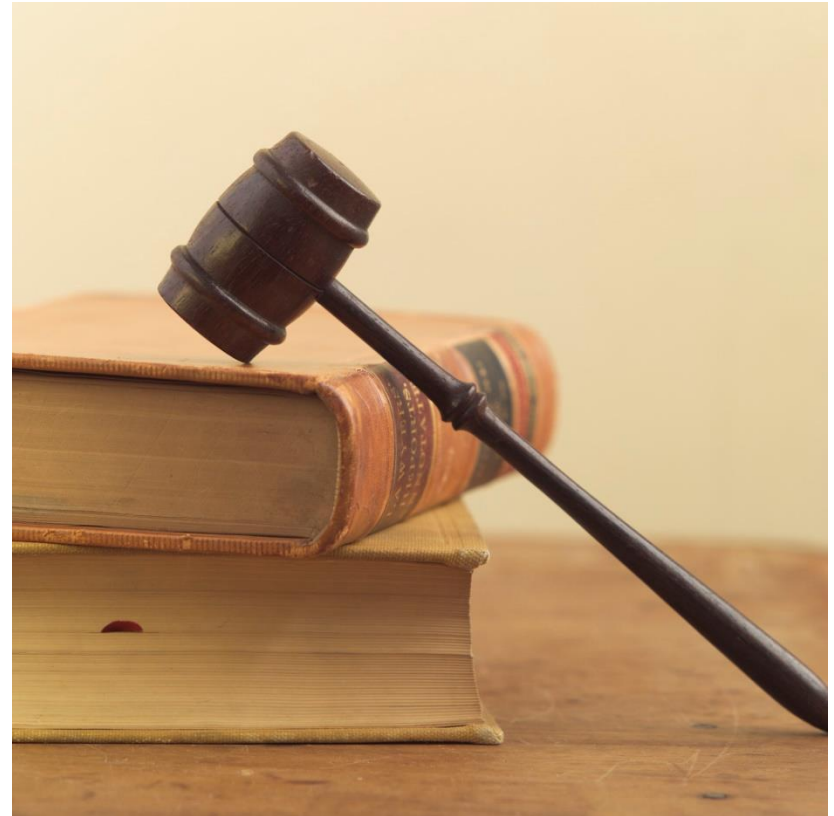




Information Technology Act 2000 - An overview

IT Act, 2000

- Enacted on 17th May 2000- India is 12th nation in the world to adopt cyber laws
- IT Act is based on Model law on e-commerce adopted by UNCITRAL



Objectives of the IT 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"
- To facilitate electronic filing of documents with Government agencies and E-Payments
- To amend the Indian Penal Code, Indian Evidence Act, 1872, the Banker's Books Evidence Act 1891, Reserve Bank of India Act, 1934

Extent of application

- Extends to whole of India and also applies to any offence or contravention there under committed outside India by any person {section 1 (2)} read with Section 75- Act applies to offence or contravention committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India
- Section 2 (1) (a) – “Access” means gaining entry into ,instructing or communicating with the logical, arithmetic or memory function resources of a computer, computer resource or network

Definitions (section 2)

- "computer" means 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 relates to the computer in a computer system or computer network;
- "computer network" means the inter-connection 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;

Definitions (section 2)

- "**computer system**" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
- "**data**" means a representation of information, knowledge, facts, concepts or instruction 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.

Definitions (section 2)

- "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;
- "secure system" means computer hardware, software, and procedure that-
 - (a) are reasonably secure from unauthorized access and misuse;
 - (b) provide a reasonable level of reliability and correct operation;
 - (c) are reasonably suited to performing the intended function; and
 - (d) adhere to generally accepted security procedures
- "security procedure" means the security procedure prescribed by the Central Government under the IT Act, 2000.
- 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

Act is in applicable to...

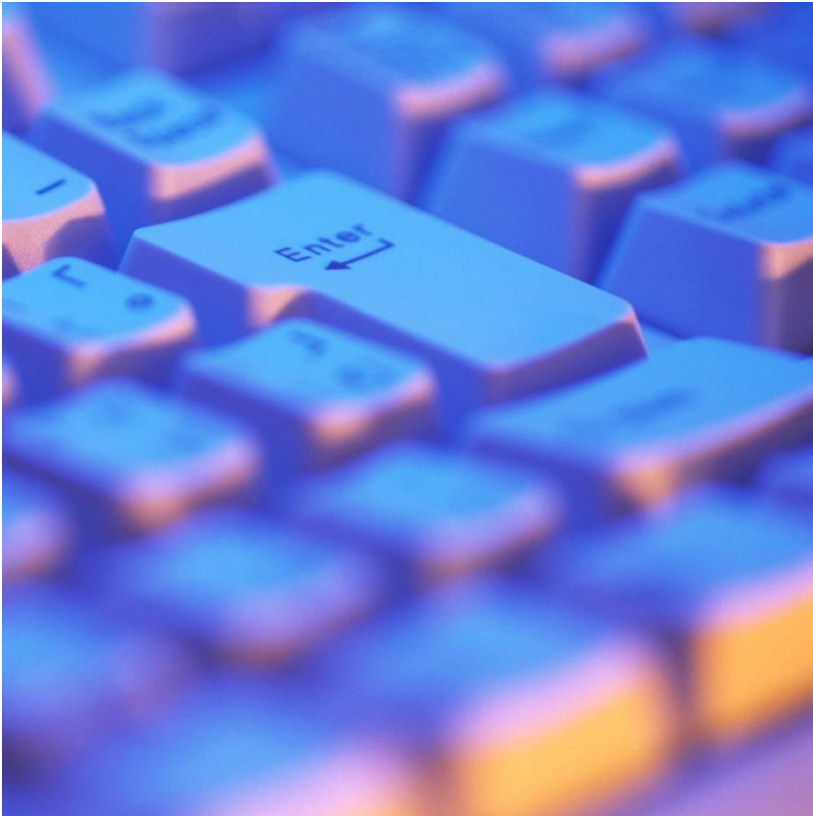
- *(a) a negotiable instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;*
- *(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;*
- *(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;*



Act is in applicable to...

- *(d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition*
- *(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*

E-Commerce



- Universal Internet access
- Total Internet economy in 2004
 - US \$ 4.48 trillion
- E-Commerce spending in 2004
 - US \$ 2.5 trillion
- E-Commerce in India in 2005
 - Rs. 1,95,000 Crore
- E-Commerce in Asia in 2005
 - 28% of world total

Electronic Commerce

- EC transactions over the Internet include
 - Formation of Contracts
 - Delivery of Information and Services
 - Delivery of Content
- Future of Electronic Commerce depends on
 - “the trust that the transacting parties place in the security of the transmission and content of their communications”*



Electronic World

- Electronic document produced by a computer. Stored in digital form, and cannot be perceived without using a computer
 - It can be deleted, modified and rewritten without leaving a mark
 - Integrity of an electronic document is “genetically” impossible to verify
 - A copy is indistinguishable from the original
 - It can't be sealed in the traditional way, where the author affixes his signature
- The functions of identification, declaration, proof of electronic documents carried out using a digital signature based on cryptography.





Electronic World

- Digital signatures created and verified using cryptography
- Public key System based on Asymmetric keys
 - An algorithm generates two different and related keys
 - Public key
 - Private Key
 - Private key used to digitally sign.
 - Public key used to verify.



Public Key Infrastructure

- Allow parties to have free access to the signer's public key
- This assures that the public key corresponds to the signer's private key
 - Trust between parties as if they know one another
- Parties with no trading partner agreements, operating on open networks, need to have highest level of trust in one another



Role of the Government

- Government has to provide the definition of
 - the structure of PKI
 - the number of levels of authority and their juridical form (public or private certification)
 - which authorities are allowed to issue key pairs
 - the extent to which the use of cryptography should be authorised for confidentiality purposes
 - whether the Central Authority should have access to the encrypted information; when and how
 - the key length, its security standard and its time validity



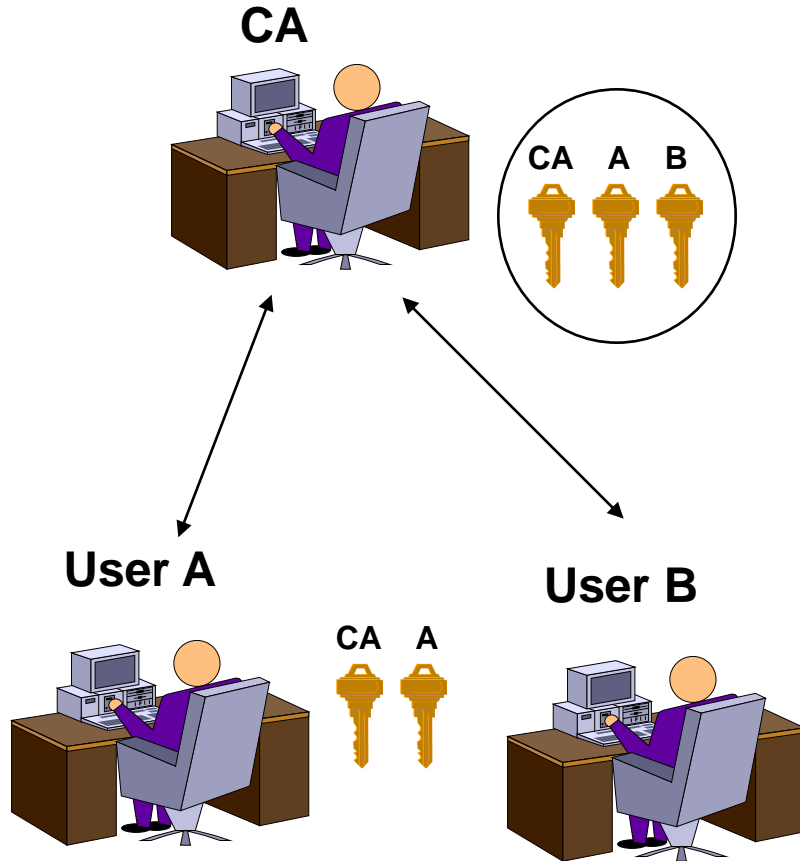
Section 3 Defines Digital Signatures

- The authentication to be affected by use of asymmetric crypto system and hash function
- The private key and the public key are unique to the subscriber and constitute functioning key pair
- Verification of electronic record possible

Secure digital signature-S.15

- 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

Certificate based Key Management



- Operated by trusted-third party - CA
- Provides Trading Partners Certificates
- Notarises the relationship between a public key and its owner



Essential steps of the digital signature process

- **STEP 1** The signatory is the authorized holder a unique cryptographic key pair;
- **STEP 2** The signatory prepares a data message (for example, in the form of an electronic mail message) on a computer;
- **STEP 3** The signatory prepares a “message digest”, using a secure hash algorithm. Digital signature creation uses a hash result derived from and unique to the signed message;
- **STEP 4** The signatory encrypts the message digest with the private key. The private key is applied to the message digest text using a mathematical algorithm. The digital signature consists of the encrypted message digest,
- **STEP 5** The signatory typically attaches or appends its digital signature to the message;
- **STEP 6** The signatory sends the digital signature and the (unencrypted or encrypted) message to the relying party electronically;



Essential steps of the digital signature process

- **STEP 7** The relying party uses the signatory's public key to verify the signatory's digital signature. Verification using the signatory's public key provides a level of technical assurance that the message came exclusively from the signatory;
- **STEP 8** The relying party also creates a "message digest" of the message, using the same secure hash algorithm;
- **STEP 9** The relying party compares the two message digests. If they are the same, then the relying party knows that the message has not been altered after it was signed. Even if one bit in the message has been altered after the message has been digitally signed, the message digest created by the relying party will be different from the message digest created by the signatory;
- **STEP 10** Where the certification process is resorted to, the relying party obtains a certificate from the certification service provider (including through the signatory or otherwise), which confirms the digital signature on the signatory's message. The certificate contains the public key and name of the signatory (and possibly additional information), digitally signed by the certification service provider.



Section 4- Legal recognition of Electronic Records

- If any information is required in printed or written form under any law the Information provided in electronic form, which is accessible so as to be usable for subsequent use, shall be deemed to satisfy the requirement of presenting the document in writing or printed form.



Sections 5, 6 & 7

- Legal recognition of Digital Signatures
 - Use of Electronic Records in Government & Its Agencies
 - Publications of rules and regulations in the Electronic Gazette.
-
- Retention of Electronic Records
 - Accessibility of information, same format, particulars of dispatch, origin, destination, time stamp ,etc

CCA has to regulate the functioning of CAs in the country by-

- Licensing Certifying Authorities (CAs) under section 21 of the IT Act and exercising supervision over their activities.
- Certifying the public keys of the CAs, i.e. their Digital Signature Certificates more commonly known as Public Key Certificates (PKCs).
- Laying down the standards to be maintained by the CAs,
- Addressing the issues related to the licensing process

The licensing process

- Examining the application and accompanying documents as provided in sections 21 to 24 of the IT Act, and all the Rules and Regulations there- under;
- Approving the Certification Practice Statement(CPS);
- Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.



Audit Process

- Adequacy of security policies and implementation thereof;
- Existence of adequate physical security;
- Evaluation of functionalities in technology as it supports CA operations;
- CA's services administration processes and procedures;
- Compliance to relevant CPS as approved and provided by the Controller;
- Adequacy to contracts/agreements for all outsourced CA operations;
- Adherence to Information Technology Act 2000, the rules and regulations thereunder, and guidelines issued by the Controller from time-to-time



Auditors Panel

- M/s Deloitte Haskins & Sells
- M/s Sysman Computers (P) Ltd.
- M/s Price Water House
- M/s Cyber Q Consultancy Pvt.
- M/s Mahindra-British Telecom Ltd.
- M/s Hexaware Technologies Ltd.
- M/s eSecureB2B.com Ltd.
- M/s Covansys Ltd.
- M/s Arthur Anderson
- M/s Wipro Infotech Solutions & Services
- M/s Tata Consultancy Services
- M/s Ernst & Young Pvt. Ltd.
- M/s S.R. Batliboi & Co.



PKI Standards

Public Key Cryptography

- RSA - Asymmetric Cryptosystem
- Diffie-Hellman - Asymmetric Cryptosystem
- Elliptic Curve Discrete Logarithm Cryptosystem

Digital Signature Standards

- RSA, DSA and EC Signature Algorithms
- MD5, SHA-1 - Hashing Algorithms

Directory Services (LDAP ver 3)

- X.500 for publication of Public Key Certificates and Certificate Revocation Lists
- X.509 version 3 Public Key Certificates
- X.509 version 2 Certificate Revocation Lists

PKCS family of standards for Public Key Cryptography from RSA

- PKCS#1 – PKCS#13

Federal Information Processing Standards (FIPS)

- FIPS 140-1 level 3 and above for Security Requirement of Cryptographic Modules



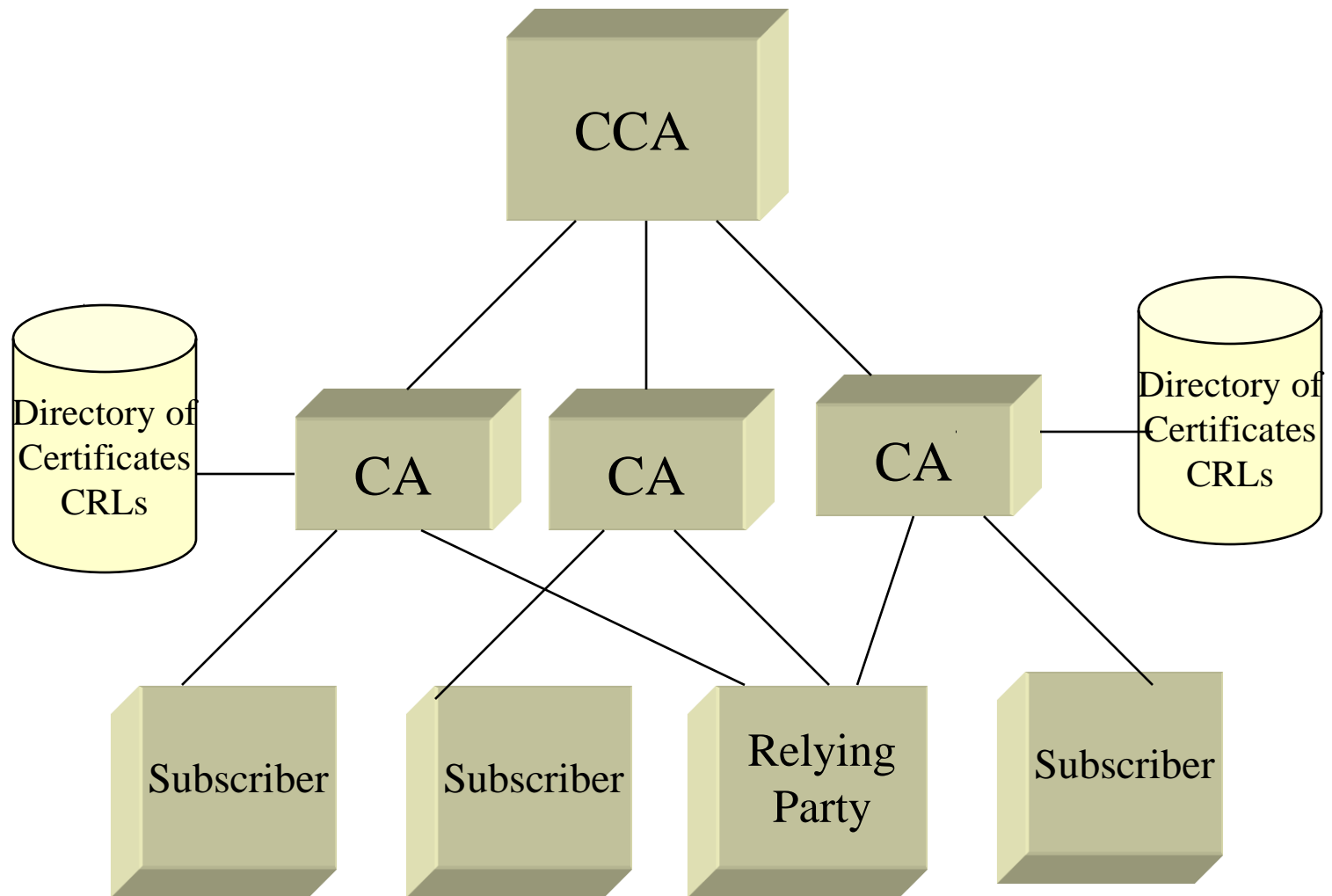
Key Size mandated by the CCA

- CA
 - 2048-bit RSA-key
- User
 - 1024-bit RSA-key

Licensed Certifying Authorities

- Provides services to its subscribers and relying parties as per its certification practice statement (CPS) which is approved by the CCA as part of the licensing procedure.
 - ☐ Identification and authentication
 - ☐ Certificate issuance
 - ☐ Certificate suspension and revocation
 - ☐ Certificate renewal
 - ☐ Notification of certificate-related information
 - ☐ Display of all these on its website
 - ☐ Time-stamping

PKI Hierarchy





Securing communications...

- CCA in position : Root of trust, National Repository
- Licensed CAs
- Digital signatures for signing documents
- Certificates, CRLs for access by relying parties
- PKI operational
- Other provisions of the IT Act – Cybercrimes not to go unpunished

Section 15- Secure Digital Signatures

- If Digital signatures are applied in such a manner that if ER was altered the Digital Signatures would be invalidated then it is called Secured Digital signatures
- Unique to subscriber
- Identifies the subscriber



Regulation of Certifying Authorities [Chapter IV]

- The Central Government may appoint a Controller of Certifying Authority who shall exercise supervision over the activities of Certifying Authorities.
- Certifying Authority means a person who has been granted a licence to issue a Digital Signature Certificate. The Controller of Certifying Authority shall have powers to lay down rules, regulations, duties, responsibilities and functions of the Certifying Authority issuing Digital Signature Certificates. The Certifying Authority empowered to issue a Digital Signature Certificate shall have to procure a license from the Controller of Certifying Authority to issue Digital Signature Certificates. The Controller of Certifying Authority has prescribed detailed rules and regulations in the Act, as to the application for license, suspension of license and procedure for grant or rejection of license.



Digital Signature Certificate

[Chapter VII]

- Any person may make an application to the Certifying Authority for issue of Digital Signature Certificate. The Certifying Authority while issuing such certificate shall certify that it has complied with the provisions of the Act.
- The Certifying Authority has to ensure that the subscriber (i.e., a person in whose name the Digital Signature Certificate is issued) holds the private key corresponding to the public key listed in the Digital Signature Certificate and such public and private keys constitute a functioning key pair. The Certifying Authority has the power to suspend or revoke Digital Signature Certificate.



IT Act –overview of other relevant provisions

- Section 16- Central Government to prescribe security procedures
- Sec 17 to 34- Appointment and Regulation of Controller and certifying authority
- Sec 35 to 39- Obtaining DSC
- Sec 40 to 42- Duties of Subscriber of DSC- exercise due care to retain the private key



Section 12- Acknowledgement of Receipt

- If Originator has not specified particular method- Any communication automated or otherwise or conduct to indicate the receipt
- If specified that the receipt is necessary- Then unless acknowledgement has been received Electronic Record shall be deemed to have been never sent
- Where ack. not received within time specified or within reasonable time the originator may give notice to treat the Electronic record as though never sent



Section 13- Dispatch of Electronic record

- Unless otherwise agreed dispatch occurs when ER enters resource outside the control of originator
- If addressee has a designated computer resource , receipt occurs at time ER enters the designated computer, if electronic record is sent to a computer resource of addressee that is not designated , receipt occurs when ER is retrieved by addressee
- If no Computer Resource designated- when ER enters Computer Resource of Addressee.
- Shall be deemed to be dispatched and received where originator has their principal place of business otherwise at his usual place of residence

Civil Wrongs under IT Act

- Chapter IX of IT Act, Section 43
- Whoever without permission of owner of the computer
 - Secures access (mere U/A access)
 - Not necessarily through a network
 - Downloads, copies, extracts any data
 - Introduces or causes to be introduced any viruses or contaminant
 - Damages or causes to be damaged any computer resource
 - Destroy, alter, delete, add, modify or rearrange
 - Change the format of a file
 - Disrupts or causes disruption of any computer resource
 - Preventing normal continuance of computer

Civil Wrongs under IT Act (Contd.)

- Denies or causes denial of access by any means
 - Denial of service attacks
- Assists any person to do any thing above
 - Rogue Websites, Search Engines, Insiders providing vulnerabilities
- Charges the services availed by a person to the account of another person by tampering or manipulating any computer resource
 - Credit card frauds, Internet time thefts
- Liable to pay damages not exceeding Rs. One crore to the affected party
- Investigation by
- ADJUDICATING OFFICER
- Powers of a civil court



Data diddling: changing data prior or during input into a computer

- Section 66 and 43(d) of the I.T. Act covers the offence of data diddling
- Penalty: Not exceeding Rs. 1 crore

Case in point :

NDMC Electricity Billing Fraud Case: A private contractor who was to deal with receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in his bank who misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

Section 46 IT Act

- *Section 46* of the IT Act states that an adjudicating officer shall be adjudging whether a person has committed a contravention of any of the provisions of the said Act, by holding an inquiry. Principles of Audi alterum partum and natural justice are enshrined in the said section which stipulates that a reasonable opportunity of making a representation shall be granted to the concerned person who is alleged to have violated the provisions of the IT Act. The said Act stipulates that the inquiry will be carried out in the manner as prescribed by the Central Government
- All proceedings before him are deemed to be judicial proceedings, every Adjudicating Officer has all powers conferred on civil courts
- Appeal to cyber Appellate Tribunal- from decision of Controller, Adjudicating Officer {section 57 IT Act}

Section 47, IT Act

- Section 47 of the Act lays down that while adjudging the quantum of compensation under this Act, 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

Cybercrime provisions under IT Act, 2000

Offences & Relevant Sections under IT Act

Tampering with Computer source documents
Sec.65

Hacking with Computer systems, Data alteration
Sec.66

Publishing obscene information
Sec.67

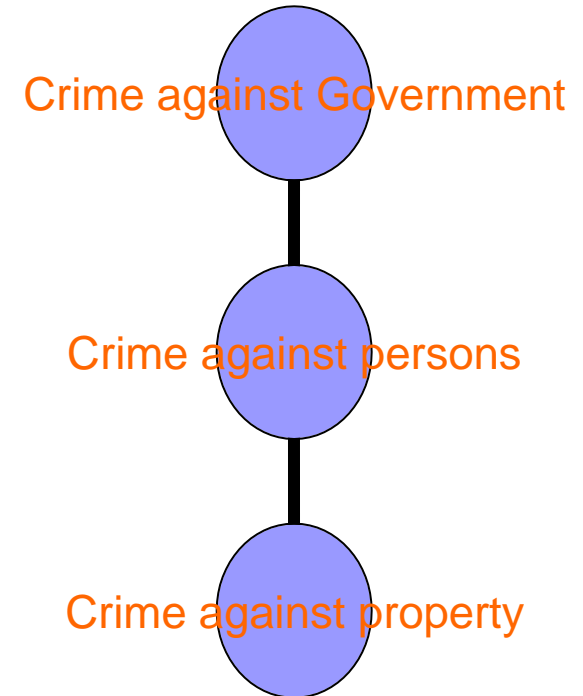
Un-authorized access to protected system
Sec.70

Breach of Confidentiality and Privacy
Sec.72

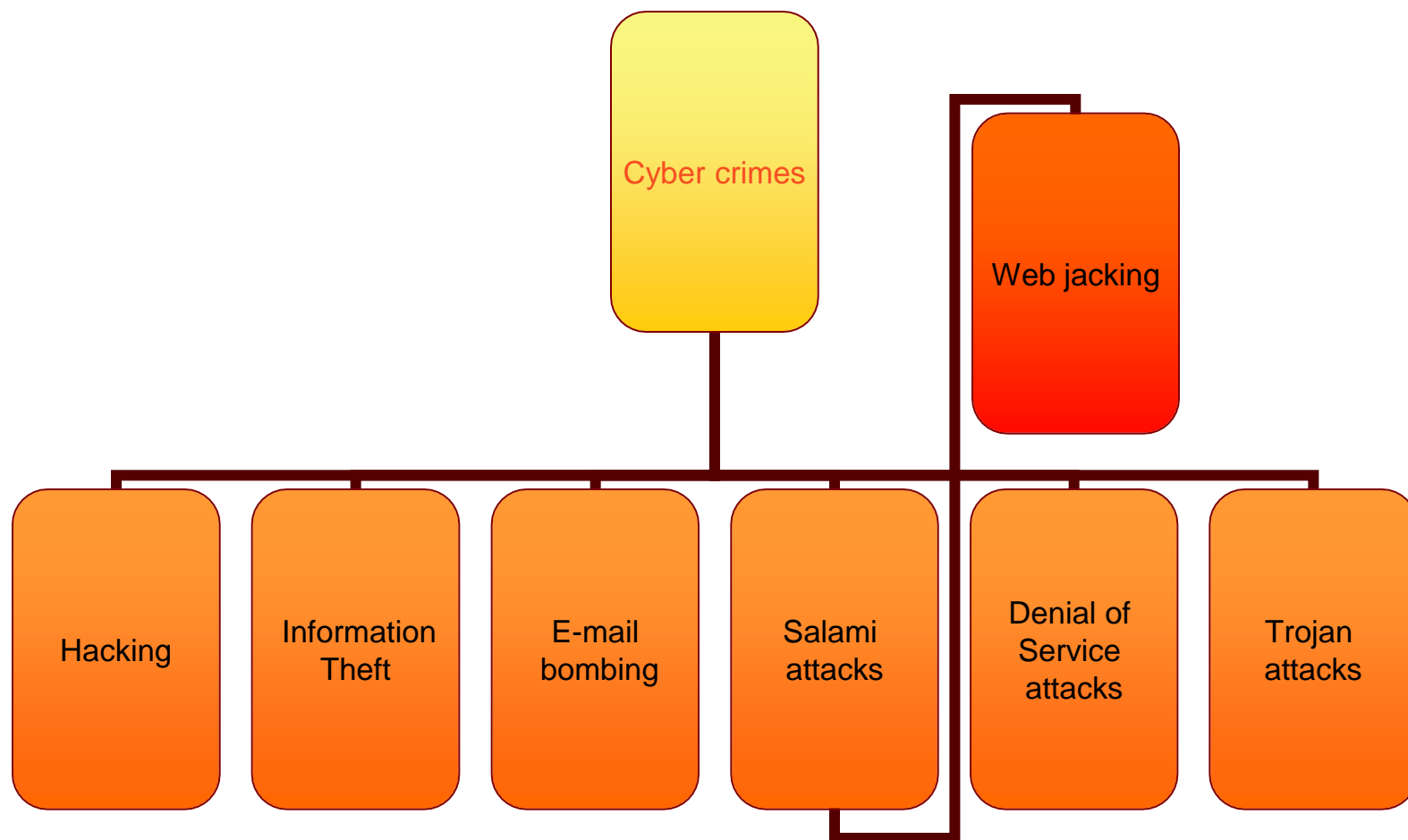
Publishing false digital signature certificates
Sec.73

TYPES OF CYBER CRIMES

- Cyber terrorism
- Cyber pornography
- Defamation
- Cyber stalking (section 509 IPC)
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Phising
- Credit card frauds



TYPES OF CYBER CRIMES



Frequency of reporting Cybercrime in India

- During the year 2005, 179 cases were registered under IT Act as compared to 68 cases during 2004 21.2% cases reported from Karnataka, followed by Maharashtra(26) , Tamil Nadu(22) and Chhattisgarh and Rajasthan (18 each) out of 179 cases, 50% were related to Section 67 IT Act.,125 persons were arrested. 74 cases of hacking were reported wherein 41 were arrested.

Section 65: Source Code

- Most important asset of software companies
- “Computer Source Code” means the listing of programmes, computer commands, design and layout
- Ingredients
 - Knowledge or intention
 - Concealment, destruction, alteration
 - computer source code required to be kept or maintained by law
- Punishment
 - imprisonment up to three years and / or
 - fine up to Rs. 2 lakh

Section 66: Hacking

- **Ingredients**
 - **Intention or Knowledge to cause wrongful loss or damage to the public or any person**
 - **Destruction, deletion, alteration, diminishing value or utility or injuriously affecting information residing in a computer resource**
- **Punishment**
 - **imprisonment up to three years, and / or**
 - **fine up to Rs. 2 lakh**
- **Cognizable, Non Bailable,**

Section 66 covers data theft as well as data alteration

Sec. 67. Pornography

- Ingredients
 - Publishing or transmitting or causing to be published
 - in the electronic form,
 - Obscene material
- Punishment
 - On first conviction
 - imprisonment of either description up to five years and
 - fine up to Rs. 1 lakh
 - On subsequent conviction
 - imprisonment of either description up to ten years and
 - fine up to Rs. 2 lakh
- Section covers
 - Internet Service Providers,
 - Search engines,
 - Pornographic websites
- Cognizable, Non-Bailable, JMFC/ Court of Sessions



Cyber Pornography Cases

- DPS mms case
- Air Force Bal bharati School case
- Miss Jammu mms case

State of *Tamil Nadu Vs Suhas Katti* Conviction within 7 months

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

The accused is found guilty and convicted for offences under section 469, 509 IPC and 67 of IT Act 2000 . This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

The verdict extract...

“ The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.”

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

Sec 69: Decryption of information

■ Ingredients

- Controller issues order to Government agency to intercept any information transmitted through any computer resource.
- Order is issued in the interest of the
 - sovereignty or integrity of India,
 - the security of the State,
 - friendly relations with foreign States,
 - public order or
 - preventing incitement for commission of a cognizable offence
- Person in charge of the computer resource fails to extend all facilities and technical assistance to decrypt the information-punishment up to 7 years.

Sec 70 Protected System

■ Ingredients

- ☐ Securing unauthorised access or attempting to secure unauthorised access
- ☐ to 'protected system'

■ Acts covered by this section:

- ☐ Switching computer on / off
- ☐ Using installed software / hardware
- ☐ Installing software / hardware
- ☐ Port scanning

■ Punishment

- ☐ Imprisonment up to 10 years and fine

■ Cognizable, Non-Bailable, Court of Sessions

Sections 71 & 72

- **Section – 71:**

- **Offence Name** - Misrepresentation to the Controller or the Certifying Authority
- **Description** - Making any misrepresentation to, or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be.
- **Penalty** - Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both

- **section – 72:**

- **Offence Name** - Penalty for breach of confidentiality and privacy
- **Description** - 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 consent of the person concerned discloses such electronic record, book., register, correspondence, information, document to any other person.
- **Penalty** - Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.

Sections 73 & 74

■ **Section – 73:**

- **Offence Name** - Publishing Digital Signature Certificate false in certain particulars
- **Description** - 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 it or the 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.
- **Penalty** - Imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh Rupees.

■ **Section – 74:**

- **Offence Name** - Publication for fraudulent purpose
- **Description** - Creation, publication or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose
- **Penalty** - Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both. .

Cyber crimes punishable under various Indian laws

- Sending pornographic or **obscene emails** are punishable under Section 67 of the IT Act. An offence under this section is punishable on first conviction with imprisonment for a term, which may extend to five years and with fine, which may extend to One lakh rupees.

In the event of a second or subsequent conviction the recommended punishment is imprisonment for a term, which may extend to ten years and also with fine which may extend to Two lakh rupees.

- **Emails that are defamatory** in nature are punishable under Section 500 of the Indian Penal Code (IPC), which recommends an imprisonment of upto two years or a fine or both.
- **Threatening emails** are punishable under the provisions of the IPC pertaining to criminal intimidation, insult and annoyance (Chapter XXII), extortion (Chapter XVII)
- **Email spoofing**
Email spoofing is covered under provisions of the IPC relating to fraud, cheating by personation (Chapter XVII), forgery (Chapter XVIII)

Computer Related Crimes under IPC and Special Laws

Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forgery of electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Online sale of Drugs	NDPS Act
Web - Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

Some more offences dealt with under IPC...

- Criminal breach of trust/Fraud- Sec. 405,406,408,409 IPC
- Destruction of electronic evidence- Sec.204,477 IPC
- False electronic evidence-Sec.193 IPC
- Offences by or against public servant- Sec.167,172,173,175 IPC

Cognizability and Bailability

- **Not mentioned in the Act**

- **Rely on Part II of Schedule I of CrPC**

- If punishable with death, imprisonment for life or imprisonment for more than 7 years: cognizable, Non- Bailable, Court of Session
 - If punishable with imprisonment for 3 years and upwards but not more than 7 years: Cognizable, Non-Bailable, Magistrate of First Class
 - If punishable with imprisonment of less than 3 years: Non-Cognizable, Bailable, Any Magistrate (or Controller of CAs)

Power of Police to Investigate

- Section 156 Cr.P.C. : Power to investigate cognizable offences.
- Section 155 Cr.P.C. : Power to investigate non cognizable offences.
- Section 91 Cr.P.C. : Summon to produce documents.
- Section 160 Cr.P.C. : Summon to require attendance of witnesses.



Power of Police to investigate (contd.)

- Section 165 Cr.P.C. : Search by police officer.
- Section 93 Cr.P.C : General provision as to search warrants.
- Section 47 Cr.P.C. : Search to arrest the accused.
- Section 78 of IT Act, 2000 : Power to investigate offences-not below rank of DSP.
- Section 80 of IT Act, 2000 : Power of police officer to enter any public place and search & arrest.

Email spoofing:

- Pranab Mitra , former executive of Gujarat Ambuja Cement posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe an Abu Dhabi businessmen . After long cyber relationship and emotional massages Mitra sent an e-mail that “she would commit suicide” if Ninawe ended the relationship. He also gave him “another friend Ruchira Sengupta’s” e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died and police is searching Ninawe. Mitra extorted few lacs Rupees as advocate fees etc. Mitra even sent e-mails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case.

Legal provisions to counter identity theft

- The IT Act 2000 in its present form does not have any specific provision to deal with identity theft. However, the Expert Committee on Amendments to the IT Act 2000 (whose report is presently under consideration by the government for adoption) has recommended amending the Indian Penal Code (IPC) by inserting in it two new sections:
- section 417A which prescribes punishment of up to 3 years imprisonment and fine for 'cheating by using any unique identification feature of any other person'; and
- section 419A that prescribes punishment of up to 5 years imprisonment and fine for 'cheating by impersonation' using a network or computer resource.

Forgery

■ Andhra Pradesh Tax Case

In the explanation of the Rs. 22 Crore which was recovered from the house of the owner of a plastic firm by the sleuths of vigilance department, the accused person submitted 6000 vouchers to legitimize the amount recovered, but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted . All vouchers were fake computerized vouchers.

Cyber stalking

- Ritu Kohli (first lady to register the cyber stalking case) is a victim of cyber-stalking. A friend of her husband gave her phone number and name on a chat site for immoral purposes. A computer expert, Kohli was able to trace the culprit. Now, the latter is being tried for "outraging the modesty of a woman", under Section 509 of IPC.

Cyber defamation

- ***SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra***: India's first case of cyber defamation was reported when a company's employee (defendant) started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the plaintiff company.

The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

Online gambling: virtual casinos, Cases of money laundering

- **Cyber lotto case:** In Andhra Pradesh one Kola Mohan created a website and an email address on the Internet with the address 'eurolottery@usa.net.' which shows his own name as beneficiary of 12.5 million pound in Euro lottery. After getting confirmation with the email address a telugu newspaper published this as news.

He gathered huge sums from the public as well as from some banks. The fraud came to light only when a cheque amounting Rs 1.73 million discounted by him with Andhra bank got dishonored.

Case Study- BPO Data Theft

- The recently reported case of a Bank Fraud in Pune in which some ex employees of BPO arm of MPhasis Ltd MsourceE, defrauded US Customers of Citi Bank to the tune of RS 1.5 crores has raised concerns of many kinds including the role of "Data Protection".
- The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

BPO data theft -Case Study (contd.)


- ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust" etc are therefore applicable in the above case in addition to section in ITA-2000.
- Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damage to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

BPO data theft -Case Study (contd.)

- The BPO is liable for lack of security that enabled the commission of the fraud as well as because of the **vicarious responsibility** for the ex-employee's involvement. The process of getting the PIN number was during the tenure of the persons as "Employees" and hence the organization is responsible for the crime.
- Some of the persons who have assisted others in the commission of the crime even though they may not be directly involved as beneficiaries will also be liable under Section 43 of ITA-2000.
- Under Section 79 and Section 85 of ITA-2000, vicarious responsibilities are indicated both for the BPO and the Bank on the grounds of "Lack of Due Diligence".
- At the same time, if the crime is investigated in India under ITA-2000, then the fact that the Bank was not using digital signatures for authenticating the customer instructions is a matter which would amount to gross negligence on the part of the Bank.

Case Study- Case of Extortion of Money Through Internet

- The complainant has received a threatening email and demanded protection from unknown person claiming to be the member of Halala Gang, Dubai. Police registered a case u/s. 384/506/511 IPC.
- The sender of the email used the email ID xyz@yahoo.com & abc@yahoo.com and signed as Chengez Babar.



Case of Extortion of Money Through Internet - Case Study (contd.)

- Both the email accounts were tracked, details collected from ISP's & locations were identified.
- The Cyber cafes from which the emails has been made were monitored and the accused person was nabbed red handed.

FIR NO 76/02 PS PARLIAMENT STREET

- **Mrs. SONIA GANDHI RECEIVED THREATING E-MAILS**
- **E- MAIL FROM**
 - missionrevenge84@khalsa.com
 - missionrevenge84@hotmail.com
- **THE CASE WAS REFERRED**
- **ACCUSED PERSON LOST HIS PARENTS DURING 1984 RIOTS**

Other important provisions of the IT Act, 2000

- **Sec 48 to 64-** prescribes for establishment of Appellate tribunals etc and compounding of contraventions, Appeal to High court within 60 days from decision of Cyber appellate tribunal .
- **Net work service provider** -Section 79- provides for non liability of network service provider in certain cases if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention
- *Explanation.*—For the purposes of this section, —
 - (a) "network service provider" means an intermediary;
 - (b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary
- **Section 85-** corporate responsibility-offences by companies —directors managers liable unless 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

Amendments- Indian Evidence Act 1872



- Section 3 of the Evidence Act amended to take care of admissibility of ER as evidence along with the paper based records as part of the documents which can be produced before the court for inspection.



Presumptions in law

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



Presumptions in law

- The law also presumes that in any proceedings, involving secure digital signature, the court shall presume, unless the contrary is proved, that the secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record




Societe Des products Nestle SA case 2006 (33)

PTC 469 & State v Mohd Afzal,

2003 (7) AD (Delhi)1

- **By virtue of provision of Section 65A, the contents of electronic records may be proved in evidence by parties in accordance with provision of 65B.**

- **Held-** Sub section (1) of section 65b makes admissible as a document, paper print out of electronic records stored in optical or magnetic media produced by a computer subject to fulfillment of conditions specified in subsection 2 of Section 65B .
 - a) The computer from which the record is generated was regularly used to store or process information in respect of activity regularly carried on by person having lawful control over the period, and relates to the period over which the computer was regularly used.
 - b) Information was fed in the computer in the ordinary course of the activities of the person having lawful control over the computer.
 - c) The computer was operating properly, and if not, was not such as to affect the electronic record or its accuracy.
 - d) Information reproduced is such as is fed into computer in the ordinary course of activity.



Important issues to ponder..IT Act is incomplete??

- DS Should not be technology specific but technology neutral- namely asymmetric crypto system and hash function
- Domain Names and rights of domain name owners and squatting
- IPR issues not addressed
- SPAM issues

Is IT Act incomplete?

- New forms of cyber crimes
- Internet Banking, E-fund transfer and e-payments laws.
- Cyber Taxation issues:-
 - Jurisdictional problems
 - PE- issues whether a website a PE
 - Problem of jurisdiction and extraterritorial jurisdiction
 - *India TV, Independent News Service Pvt Ltd v India Broadcast live LLC, 2007(145)DL 521*
 - Privacy concerns



Report of the Expert Committee Proposed Amendments to Information Technology Act 2000 *SUMMARY* -August 2005

- Proposal to add Sec. 43(2) related to handling of sensitive personal data or information with reasonable security practices and procedures thereto
- (ii) Gradation of severity of computer related offences under Section 66, committed dishonestly or fraudulently and punishment thereof
- (iii) Proposed additional Section 72 (2) for breach of confidentiality with intent to cause injury to a subscriber.
- A new section on Section 67 (2) has been added to address child pornography with higher punishment, a globally accepted offense

Suggestions from Report of the Expert Committee (contd..)

- A new phenomenon of video voyeurism has emerged in recent times where images of private area of an individual are captured without his knowledge and then transmitted widely without his consent thus violating privacy rights. This has been specifically addressed in a new proposed sub-section 72(3).
- Section 79 has been revised to bring-out explicitly the extent of liability of intermediary in certain cases. EU Directive on E-Commerce 2000/31/EC issued on June 8th 2000 has been used as guiding principles. Power to make rules w.r.t the functioning of the “Intermediary” including “Cyber Cafes” has been provided for under Section 87.

POSITIVE INITIATIVES & RECOMMENDATIONS

- Mumbai Cyber lab is a joint initiative of Mumbai police and NASSCOM has been set up.
- Suggested amendments to the IT Act,2000-new provisions for child pornography, etc.
- *Stricter provisions for online offences required as compared to offline mode since qualitative impact of online offences is much more than offline offences and punishments need to be commensurate with negative impact suffered by victim .*
- More Public awareness campaigns
- Training of police officers to effectively combat cyber crimes-In a public-private partnership, public sector Canara Bank, the Karnataka Police department and NASSCOM have jointly set up the lab, which would train 1,000 officials every year. The trained officers would be able to analyse and scrutinise data on hard disks, track e-mails, extract evidence using internet and mobile phones and cyber crime-related legislation.



POSITIVE INITIATIVES & RECOMMENDATIONS (Contd.)

- More Cyber crime police cells set up across the country
- Effective E-surveillance
- Websites aid in creating awareness and encouraging reporting of cyber crime cases.
- Specialized Training of forensic investigators and experts
- Active coordination between police and other law enforcement agencies and authorities is required.
- NASSCOM, in association with the Chandigarh administration, inaugurated a state- of-the-art Regional Cyber Security and Research Centre (RCSRC) at Chandigarh.