
Implication of IT ACT for Corporate Businesses Mumbai

Agenda

- ◆ **IT Act, 2000**
- ◆ **IT Amendment Act 2008**

IT Act Genesis

- ◆ **The UN on 30 January 1997 adopted UNCITRAL Model Law on E-Commerce**
- ◆ **IT Act was passed in year 2000. Main focus was**
 - Legal Recognition of Electronic Documents
 - Legal Recognition of Digital Signatures
 - Offenses and Contraventions
 - Justice Dispensation Systems

IT Act 2000- Salient Points

- ◆ **Electronic Contract**
 - Provided recognition
 - Digital Signatures
- ◆ **Support for ecommerce**
- ◆ **PKI regime**
 - Certifying authorities
 - Registering authorities

Where it Lacked

- ◆ **Data Protection was not adequately addressed**
- ◆ **Privacy of information not emphasised**
- ◆ **Third party intermediaries were being booked**
 - Orkut case where CEO was booked

Data Protection

- ◆ **Section 43A: Compensation for failure to protect data**

- ▶ *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.*

Data Protection

- ◆ **"body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities**
- ◆ **"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.
- ◆ **"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.**

Data Protection

- ◆ **The definition of Reasonable Security Practice is to be determined in the following order.**
 - As defined in a mutual contract between the vendor and the processor of data or a data subject and the data processor
 - Compliance to HIPAA, GLBA, Data Protection Act
 - As specified in any law for the time being in force
 - To be specified by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Personal Privacy

- ◆ **Section 72 A: Punishment for Disclosure of information in breach of lawful contract**
 - ◆ 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**

- ◆ This section uses the term “personal information” and not “sensitive personal information” as in section 43A. Hence it could apply to any information which is obtained in order to deliver services. Hence in some ways broadens the definition of information

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 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.
 - Very wide

Coverage

- ◆ includes "Telecom Companies" such as AirTel or Reliance Infocomm or Tata Indicom. It includes Google, Rediff, Sify, Ebay.in, cyber cafes etc. It includes many BPOs who operate as back office service providers, Data Centers, HR service providers, etc.

Email, Theft

- ◆ **66 A- Punishment for sending offensive messages through communication service, etc**
 - Offensive emails- causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient
- ◆ **66 B Punishment for dishonestly receiving stolen computer resource or communication device**

Identity Theft, Phishing

◆ Section 66 C- Identity Theft

- It states: 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 that extends upto three years and shall also be liable to fine which may extend to rupees one lakh

◆ Section 66 D- Cheating by Personation

- 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.

Violation of Privacy

◆ 66 E-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 persons, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees or with both.

Cyber Terrorism

◆ Section 66 F

- knowingly or intentionally penetrates or accesses a computer resource
 - without authorisation or
 - exceeding authorised access, and by
 - means of such conduct obtains access to information,
 - data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that
- such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State,, commits the offence of cyber terrorism.

Provision for Privacy

- ◆ **Section 67C: Preservation and Retention of information by intermediaries.**
 - *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”. Any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to 3 years and shall also be liable to fine.*
 - The notifications on time for preservation etc. are not yet released. However since this is a “cognizable” offence any police inspector can start investigations against the CEO of a company

Lack of Privacy

- ◆ **Section 69-monitor, intercept and decrypt**
 - Any Government official or policeman will be able to listen in to all your phone calls, read your SMSs and emails, and monitor the websites you visit. And he will not require any warrant from a magistrate to do so.
 - Indian telegraph Act 1885 mentioned tapping of lines and was clarified by SC that it can be done for Public safety or public exigency, this has been dropped in the present IT Act
 - Unlimited powers
- ◆ **Offences with 3 years or more of punishment – cognizable and liable for arrest and search in public places without warrant**

Intermediary Liability

- ◆ **Section 79, Intermediary Liability doesn't exist except when**
 - initiate the transmission,
 - select the receiver of the transmission, and
 - select or modify the information contained in the transmission

Liabilities

- ◆ **Section 85, the liabilities that fall on a company under this section will extend to any officer in charge of business or director etc unless "Due Diligence" is proved.**

Dilutions

- ◆ **All offences made bailable**
- ◆ **Punishment in certain cases reduced to three years from earlier five years**

Omissions

- ◆ **Jurisdictional issues**

- ◆ jurisdiction over data and information impacting India

- ◆ **Spam**

- ◆ Not mentioned- India ranked 10th highest spam generating country

Thank You