National Seminar on Enforcement of Cyberlaw

IT Act, 2000 vs 2008-Implémentation, challenges & Role of Adjudicating Authority

Karnika Seth, New Delhi, 8 May 2010

Presentation plan

- Discuss the major changes brought about by the IT (Amendment) Act,2008
- Comment on the recent amendments & its effectiveness
- Challenges posed by the amended Act
- Discuss existing lacunae/clarifications required in the amended Act
- Recommend Strategies for effective enforcement of the Act

IT Act,2000

- The Act was passed in India in 2000
- based on Model law of e-commerce adopted by UNCITRAL in 1996
- Three fold objectives in Preamble-
- Legal recognition for e-transactions
- Facilitate electronic filing of documents with govt agencies
- To amend certain acts such as IPC,1860, Evidence Act,1872,etc

Main Features of IT Act,2000

- Conferred legal validity and recognition to electronic documents & digital signatures
- Legal recognition to e-contracts
- Set up Regulatory regime to supervise Certifying Authorities
- Laid down civil and criminal liabilities for contravention of provisions of IT Act,2000
- Created the office of Adjudicating Authority to adjudge contraventions

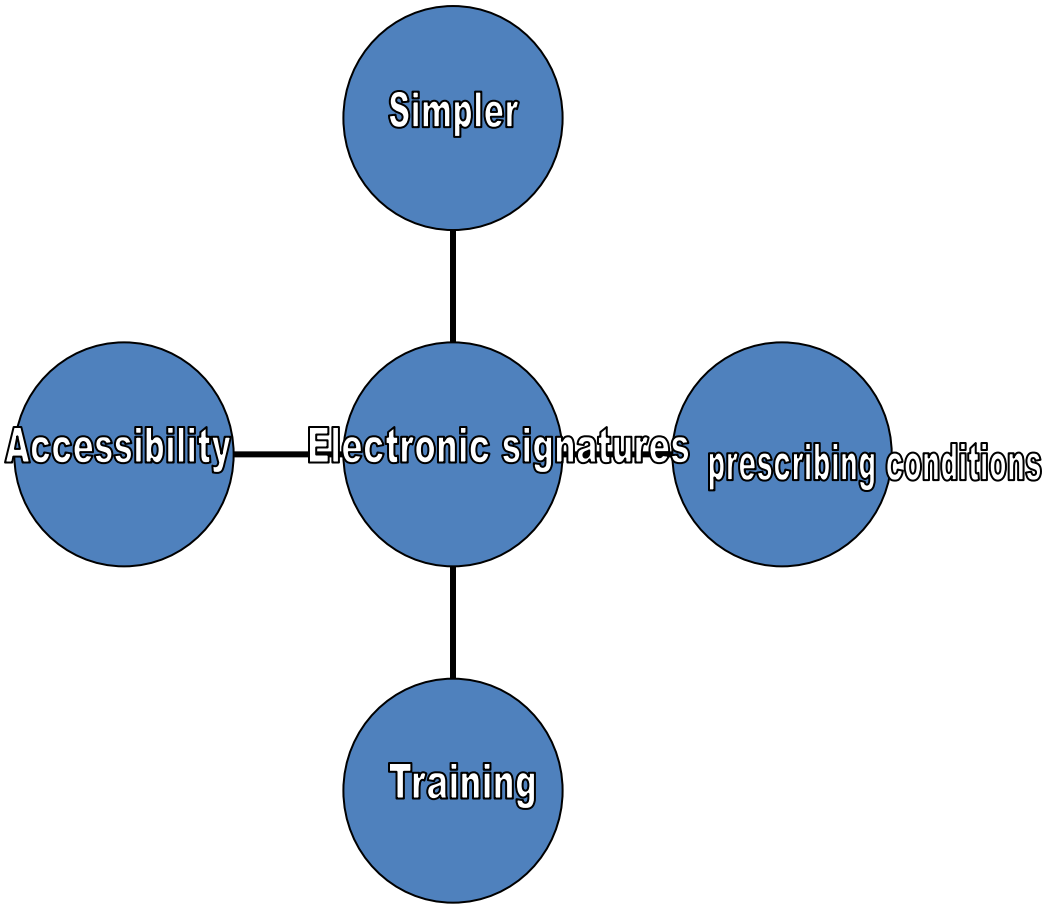
Need for amendments

- Diversifying nature of cybercrimes –all were not dealt with under IT Act,2000-cyber terrorism, spamming, MMS attacks,etc
- Use of wireless technology had no mention in definition of “computer network” in S2(j)
- Digital signatures only for authentication .
- Definition of ‘intermediary’ and their liability required clarification.
- Grey areas-Power of execution- Adjudicating authority
- No appointed statutorily authority for supervising cyber security of protected systems
- Power to investigate offences –only DSP and above
- Power to intercept & decrypt information limited under Section 69

Important definitions added in amended Act

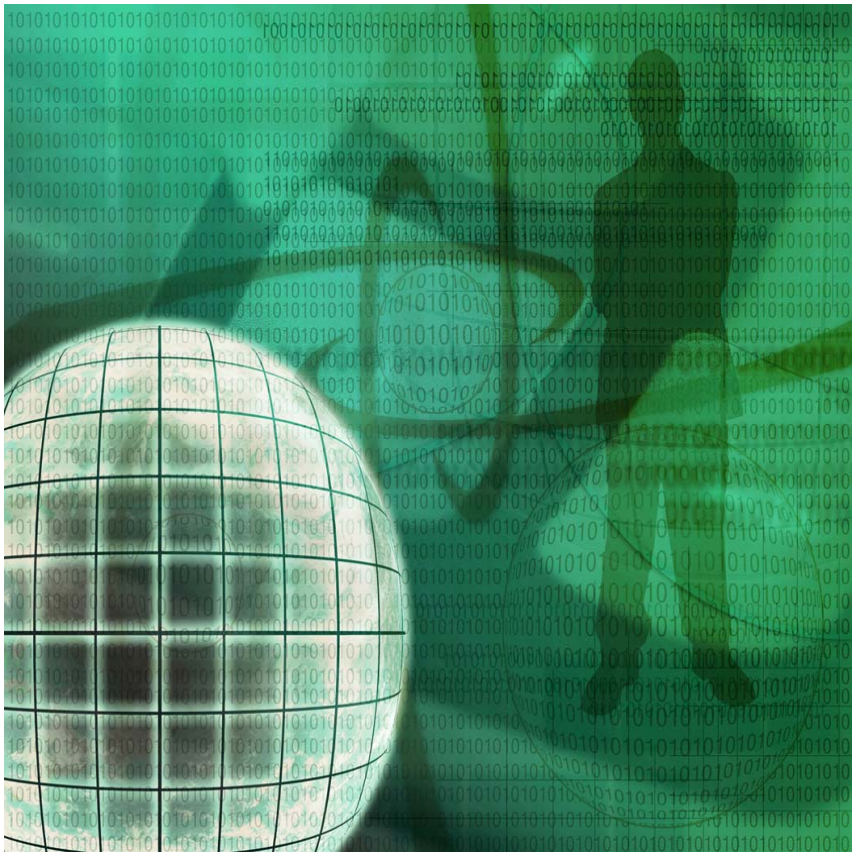
- Section 2 (ha)- communication device- includes cell phones, PDA,etc
- Section 2 (j) computer network – interconnection through wireless added
- Section 2 (na) cybercafe
- Section 2(w)- intermediary- includes search engines, web hosting service providers, online auction sites,telecom service providers etc

IT Act ,2000 v 2008- Electronic Signatures



Corporate Responsibility introduced in Section 43A

- Applies to Corporate bodies handling sensitive personal information or data in a computer resource
- Need for data protection fulfilled- no limit to compensation claim
- Challenge is to define ‘reasonable security practices’ & ‘sensitive personal information’
- Will help combat data theft, credit card and IP frauds
- To be r/w Section 85 IT Act,2000



Section 43A

- To protect from unauthorized access, damage,use,modification,disclosure,or impairment
- ‘Reasonable security practices’ as may be specified by agreement between parties
- Or Specified by any law
- Or Prescribed by Central Govt in consultation with professional bodies

Amended Section 43 –cyber contraventions

- Earlier Section 43 –contraventions-actus reus and Section 66-mens rea +actus reus
- Amended Section 43 , insertion of Section 43 (i) and (j)- requirement of mens rea with actus reus
- Section 43(j) uses words "*stealing*" and "*intention to cause damage*". Same acts when committed 'dishonestly' or 'fraudulently' are placed under Section 66.
- Intent is to punish under section 66 and compensate for loss for same acts in S.43.Amended Section 43 removed ceiling limit for compensation

Amended Section 43 (j)

- *If any person without permission of the owner or any other person who is incharge of a computer,computer system or computer network….steal, 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.*

New cybercrimes

Hacking –Section 66	Sending of offensive false messages(s.66A)	Identity theft (s. 66C)
Cheating by personation (s.66D)	Violation of privacy (s.66E)	Cyber terrorism (s.66F)
Publishing sexually explicit content(s. 67A)	Child pornography (s.67B)	Stolen computer resource(s.66B)
Attempt to commit an offence (s.84C)	Abetment to commit an offence(s.84B)	

Cognisability & bailability

- Most offences introduced by the 2008 amendments prescribe punishment of upto 3 yrs , fine of one lac/2 lac
- For hacking term of imprisonment remains upto 3yrs but fine increased from 2 lakhs to 5 lacs
- In S.67 imprisonment term reduced from 5 yrs to three yrs. Fine increased from one lac to 5 lacs.
- Most Offences are cognisable but bailable
- This is a new challenge for cyberlaw enforcement authorities- need quick action by trained investigators to collect and preserve evidence as probability of tampering increases .

Collection of evidence streamlined

- **Section 67C-** Intermediaries bound to preserve and retain such information as Central govt prescribes, for prescribed duration- contravention punishable with upto 2yrs imprisonment ,upto one lac fine or both
- Accountability of service providers increased- **Section 72A** added-disclosure of information in breach of lawful contract-punishment upto 3 years , fine upto 5 lakh or both

Collection of evidence streamlined

- **Section 69** -Power of Central Govt to intercept, monitor, decrypt information
- IT (procedure and safeguards for interception, monitoring and decryption of Information) Rules, 2009.
- Non-cooperating Subscriber or intermediary -liable to punishment of upto 7 yrs imprisonment and fine is added by amendment.
- Maintenance of confidentiality, due authorisation process, exercise power with caution.

Collection of evidence streamlined

- **Section 69 B** added- confers power on central govt to appoint any agency to monitor and collect traffic data or information generated,transmitted,received,or stored in any computer resource
- Use in order to enhance cyber security& identification,analysis and prevention of intrusion or spread of computer contaminant

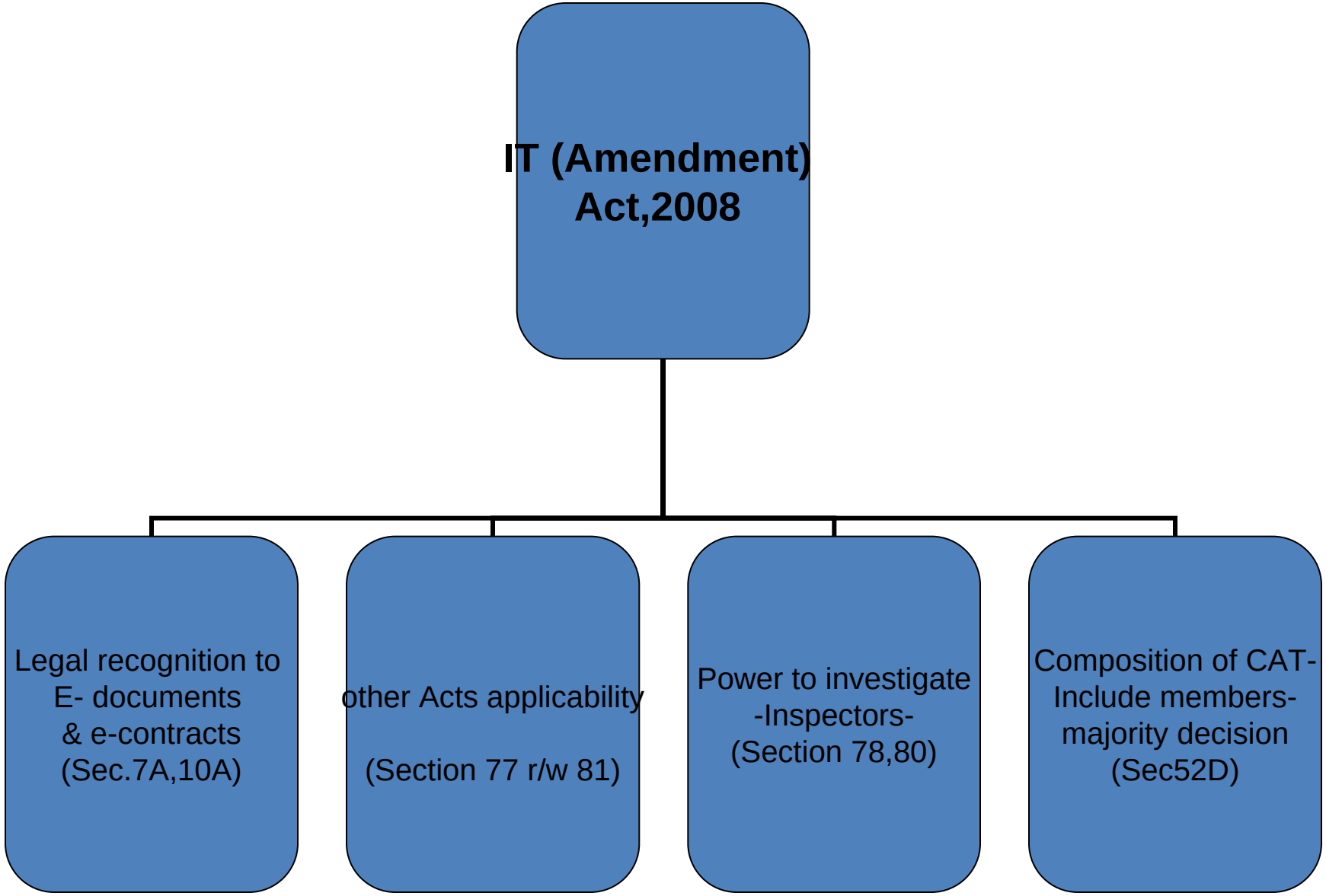
- IT (procedure and safeguards for monitoring and collecting traffic data or information) Rules ,2009
- Responsibility to maintain confidentiality-intermediaries.
- Authorisation procedures laid down
- Review committee provision,destruction of records
- Non cooperating intermediary-liable to punishment –term upto 3 yrs and fine.
- Helpful in curbing cyber terrorism cases –power exercise with caution-right to privacy may be affected.

EEE's role

- Examiner of Electronic Evidence created in section 79A-
- Central Government empowered to appoint this agency
- To provide expert opinion on electronic form of evidence.
- "electronic form evidence" –inclusive definition- computer evidence, digital audio, digital video, cellphone, fax machines-information stored, transmitted in electronic form
- One EEE should be set up/appointed in every State

Strengthening India's cyber security

- Section 70- protected systems- takes within its cover the 'Critical Information Infrastructure'
- Computer resource, incapacitation or destruction of which has debilitating impact on national security,economy,public health, safety.
- CERT appointed as Nodal Agency for incident response- Section 70B
- Multiple roles- alert system ,response team, issuing guidelines ,reporting incidents
- Non cooperating service providers, intermediaries,etc punishable with term upto one year or fine upto one lac or both
- Excludes jurisdiction of court


IT (Amendment) Act,2008
Legal recognition to E- documents & e-contracts (Sec.7A,10A)
other Acts applicability
(Section 77 r/w 81)
Power to investigate -Inspectors-
(Section 78,80)
Composition of CAT- Include members- majority decision
(Sec52D)

New Challenges

- Controller no more to act as **repository** of digital signatures
- Role assigned to Certifying Authority in Section 30.
- Concerns of ensuring secrecy and privacy of electronic signatures is maintained
- Need to strengthen security infrastructure
- Publishing information wrt electronic signatures & regular updation

New challenges

- Blocking of unlawful websites –**Section 69A**
- Power lies with Central Govt or any authorised officer
- Grounds for blocking fairly wide- issue of censorship vs free flow of information
- Information Technology (procedure and safeguards for blocking for access of information by public) Rules 2009
- Websites containing hate speech, defamatory matter, slander, promoting gambling, racism ,violence, terrorism, pornography, can be reasonably blocked
- Blocking of websites also possible by court order
- Calls for cooperation from intermediary-non cooperation-punishable offence-term 7 yrs, fine

Recent amendments & Role of Adjudicating Authority

- The Subject matter of its jurisdiction is widened –adjudging more contraventions under Section 43,43A
- Power to impose penalty & award compensation both
- Excludes jurisdiction from matters where compensation claimed is more than 5 crores
- Quantum of compensation –discretion of adjudicating officer-
- objective criteria laid down for guidance maintained-Amount of unfair advantage gained, amount of loss, repetitive nature of default
- IT (qualification and experience of adjudicating officers and manner of holding enquiry) Rules ,2003

Strengthening the role of Adjudicating Authority

- Reliance on documentary evidence, investigation reports , other evidence
- Compounding of contraventions
- Powers of Civil court and Section 46(5)© confers power of execution of orders passed by it- attachment of property, arrest & detention of accused, appointment of receiver- greater enforceability

Lacunae under amended IT Act,2000

- **Power of Controller under Section 28** – to investigate 'any contravention of the provisions of this Act,rules, or regulations made'.
- Should be replaced with words 'any contravention of the provisions of this Chapter' since amended Section 29 –controller power to access computers, data has also been amended and limited the power 'to contravention of the provisions of this chapter'
- Controller's power cannot overlap with Adjudicating officers, CAT or Police

Lacunae under amended IT Act,2000

- Section 55 of IT Act,2000 –order of CAT not open to challenge on ground of defect in constitution of tribunal- contrary to principles of natural justice
- Analogy to Arbitration law –defect in constitution of tribunal renders award subject to challenge

Liability of ISP revisited

- Under earlier Section 79, network service providers were liable for third party content only if they failed to prove offence was committed without knowledge or due diligence was exercised. Burden of proof was on Network service provider.
- The amended section excludes certain service providers and holds intermediary liable **only if he has conspired , abetted or induced whether by threats or promise or otherwise in the commission of unlawful act (S.79(3)(a).Onus to prove conspiracy, abetment, is shifted on Complainant.**
- **Intermediary is liable also if on receipt of actual knowledge or on receipt of intimation from govt agency, it fails to remove or disable such website's access.**
- **Could give rise to Red-tapism & difficulty in access of speedy remedy**

Strategies for effective enforcement of cyberlaws

- Imparting legal & technical training to law enforcement personnel
- One cyber cell in every state and trained police
- Set up EEE/ cyber forensic labs in each state
- Immediate rulemaking in S.67C- intermediary to preserve information
- Build International cooperation regime for solving cybercrime cases

Thank you!

SETH ASSOCIATES

ADVOCATES AND LEGAL CONSULTANTS

***New Delhi Law Office*:**

C-1/16, Daryaganj, New Delhi-110002, India

Tel:+91 (11) 65352272, +91 9868119137

***Corporate Law Office*:**

B-10, Sector 40, NOIDA-201301, N.C.R ,India

Tel: +91 (120) 4352846, +91 9810155766

Fax: +91 (120) 4331304

E-mail: mail@sethassociates.com