Wishing You a Happy Digital Society Day of India

Naavi

www.naavi.org

ITA 2008- A Birds Eye View

Naavi

www.naavi.org

ITA 2008 Chapterization

Chapter	Title	Sections	
I	Preliminary	1, 2	2
II	Digital Signature and Electronic Signature	3, 3A	2
III	Electronic Governance	4,5.6,6A,7,7A,8,9,10,10A	10
IV	Attribution, Acknowledgement and Despatch of Electronic Records	11,12,13	3
V	Secure Electronic Records and Secure Electronic Signatures	14, 15, 16	3
VI	Regulation of Certifying Authorities	17,18, 19 21,22,23, 24,25. 26,27,28,29,30,31,32,33,34	17
VII	Electronic Signature Certificates	35,36,37,38,39,	5
VIII	Duties of Subscribers	40,40A,41,42,	4
IX	Penalties and Compensation for damage to computer, computer system, etc	43,43A,44,45,46,47	6
X	The Cyber Appellate Tribunal	48,49,50,51,52,52A,52B,52C,52D, 53,54,55,56,57,58,59,60,61,62,63,64	21
XI	Offences	65,66,66A,66B,66C,66D,66E,66F ,67,67A,67B,67C,68,69.69A,69B, 70,70A,70B,71,72,72A,73,74,75, 76,77,77A,77B,78,	30
XII	Intermediaries not to be liable in certain cases	79	1
XIIA	Examiner of Electronic Evidence	79A	1
XIII	Miscellaneous	80,81,81A,82,83,84,84A,84B,84C 85.86,87,88,89,90,	15
		Total	120

Essence of ITA 2000/8

- Basics
  - Legal Recognition of Electronic documents, means of authentication and digital contracts
- Contraventions and Offences
  - Civil Contraventions and Adjudication
  - Criminal liabilities and Powers of Police
  - Data Security and Privacy protection obligations
  - Vicarious liabilities of intermediaries and corporate executives
  - Defining of jurisdiction
- Digital Evidence and admissibility

Applicability

- Type of Excluded Documents
  - Sec 1 (4):
  - Nothing in this Act shall apply to documents or transactions specified in the First Schedule by way of addition or deletion of entries thereto.

THE FIRST SCHEDULE
(See sub-section (4) of section 1)

- **Documents or Transactions To Which the Act Shall Not Apply**
  1. A Negotiable Instrument (Other than a cheque) as defined in Section 13 of the Negotiable Instruments Act 1881 (26 of 1881)
  2. A Power of Attorney as defined in section 1A of the Power of Attorney Act 1882 (7 of 1882)
  3. A trust as defined in section 3 of the Indian Trusts Act, 1882 (2 of 1882)
  4. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 (39 of 1925) including any terstamentary deposition whatever name called
  5. Any contract for the sale or conveyance of immovable property or any interest in such property

Legal Recognition

Section 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

Section 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,
  - notwithstanding anything contained 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" shall be construed accordingly.

Section 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.

Sec 3..contd

- **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.

Sec 3..contd

- (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.

How does a Digital Signature look like?

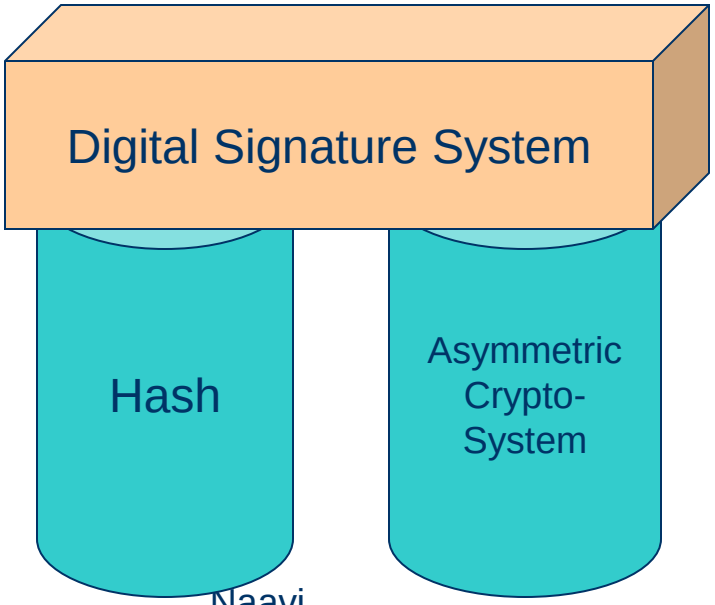
- 01001010 01011010 01000010 01000101 01001110 01011000 01110101 01110000 01010101 01110101
  01010110 00111000 00111000 01101100 01110100 00110010 01001101 01101100 01110110 01010011
  01010101 01000101 01100100 01001100 01001010 01001011 01100001 01110010 01001010 00101011
  00111000 01010000 01101000 01001100 01100011 01110011 01001000 01100100 01000011 01111010
  01010110 01110000 01000111 01101011 01101111 01010100 00110010 00111001 00110000 01011000
  00101111 01010000 01001011 00110100 00111001 01110011 01100011 01111001 01110101 01010010
  01001110 01111001 01100100 01010100 00001101 00001010 01101110 01110111 01100111 01010111
  01100011 01101010 01001001 00101111 01000100 00101111 01101001 00111001 01110110 01001111
  01100011 01000101 01101100 01101101 01110100 01000011 00110011 01000100 00101111 00110111
  01010010 00110001 01001001 01110000 00110010 01011010 00110111 01000100 01001010 00101011
  01011010 00110101 01011001 01101000 01101011 01110001 01110110 00101011 01100110 01101000
  01011000 01101101 01000001 01010010 01111000 01101010 00101011 01111000 01110111 01011001
  01000101 01010000 00110001 01001101 01100110 01000111 01111000 01001101 01110110 00110111
  00001101 00001010 01001000 01010110 01001000 01001010 01111010 01010010 01100100 01011010
  01000001 01110101 01010100 01010010 01110001 01100100 01011000 01001101 01110101 01000100
  01100010 01100110 01100111 01010100 01010111 01101110 01110000 00110001 00111000 01010001
  01011000 00110001 01010101 01110000 00110101 01001011 01010101 01011000 01100110 01011001
  01100111 01101001 00110001 01101011 01010001 00111101
  - A binary representation

Digital Signatures-What they are not

- It is not a Scanned form of a Signature
- It is a variable
  - It is document specific

Technology Behind Digital Signatures

- Digital Signature System is built on the foundation of two technologies, Hashing and Asymmetric Crypto System



Digital Signature Definition

- Digital Signature
  - Of a document of a person
    - Is
    - The hash value of the document encrypted with the private key of the person

Law of Cyber Contracts

naavi@vsnl.com

Section 10A 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.

naavi@vsnl.com

Applicability of Indian Contract Act 1872 (ICA) to Electronic Documents

- **Sec-4 of ITA-2000**
  - 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

naavi@vsnl.com

Electronic Documents..examples

- E-Mail
- Web page
- Word/ Power point etc document
- Data, Audio and Video CD s/ Floppies

naavi@vsnl.com

Attribution

- Sec 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

naavi@vsnl.com

Time and Place of Contract

Determined by the completion of Contractual obligations or as otherwise specified

naavi@vsnl.com

Time Of Despatch [sec 13(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.

naavi@vsnl.com

Time Of Receipt [Sec 13(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.

naavi@vsnl.com

Place of Despatch [Sec 13(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.

naavi@vsnl.com

Place of Despatch [Sec 13 (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).

naavi@vsnl.com

Place of Despatch [Sec 13 (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.

naavi@vsnl.com

Acknowledgement of Message

- If the sender has prescribed a form in which acknowledgment has to be provided, sent message is valid only on receipt of such acknowledgement…
  - Otherwise, any form
  - If acknowledgement has been mandated, message is deemed to have been sent only when such acknowledgement is given
- if no acknowledgement form has been specified or time has been specified for acknowledgement and Acknowledgement has not been received
- if the sender has to revoke it,
  - He needs to send notice of revocation

Civil Contravention

Chapter IX

S43: Penalty and Compensation 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 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 programmes residing in such computer, computer system or computer network;

Sec 43..contd

- (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,

Sec 43..contd

- (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.

Adjudication

Sec 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 thereunder 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.

Sec 46..contd

- (1A) 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 five crore
  - Defines Pecuniary Jurisdiction limitation
- Provided that the jurisdiction in respect of claim for injury or damage exceeding rupees five crore shall vest with the competent court.

Sec 46..contd

- (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.

Sec 46..contd

- (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
  - P.S: Execution of decrees etc (Reference)

Notification of 25th March 2003

- Secretary of Information Technology of each of the States or of Union Territories shall provide the infrastructure and maintain the records of the matters handled by AO functioning in the States/Union Territories

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.
- Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter.

Appeals

- Appeal from the Adjudication
  - Cyber Appellate Tribunal
    - Now merged with TDSAT (Telecom Disputes Settlement appellate tribunal)
  - Further appeal to the High Court of jurisdiction relevant to the place of adjudication

Offences under ITA 2008

Sec 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, 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.
      - **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.

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 five 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;
    - b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

66..contd

- Sec 24/25 of IPC
  - **24. "Dishonestly"**
  - Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".
  - **25. "Fraudulently"**
  - A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

66 A Punishment for sending offensive messages through communication service, etc (Now Scrapped)

- 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** 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 (Inserted vide ITAA 2008)**
  - shall be punishable with imprisonment for a term which may extend to **three** years and with fine.

Sec 66A (Scrapped)..contd

- 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.

Section 66B..Stolen Computer

- Whoever
  - dishonestly receives or retains
    - any stolen computer resource or communication device knowing or having reason to believe that the same to be a 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.

Section 66 C: 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 that extends upto three years and shall also be liable to fine which may extend to rupees one lakh

Sec 66D: Impersonation

- 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.

Section 66 E:..Video Voyeurism

- 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**.**

66 E..contd

- 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 video tape, 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 to 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.

Section 66F: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 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 infrastructure specified under Section 70, or

Sec 66F..contd

- **(B)** knowingly or intentionally penetrates or accesses a computer resource
  - without authorization or exceeding authorised access, and
  - by means of such conduct
    - obtains access to information, data or computer database
      - that is restricted for reasons of the security of the state or foreign relations or
      - any restricted information data or computer data base with reasons to believe that such information, data or computer data base 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, friendly relations with foreign states, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence or to the advantage of any foreign nation, group of individuals or otherwise,
- commits the offence of Cyber Terrorism
- (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 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.

Sec 67 A..contd

- Exception: This section and section 67 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 bona fide for religious purposes.

Section 67B:

- 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**:

Sec 67B..contd

- **Provided that the provisions of section 67, section 67A 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.**

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.

Cognizability, Bailability, Compundability

0-3 years	Non Cognizable, (Bailable), Compoundable
3 years	Cognizable, Bailable, Compoundable (with exceptions)
Above 3 years	Cognizable, Non Bailable, Non Compoundable

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

- **(1)** Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a **Inspector** or any other officer of the Central Government or a State Government authorized 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.

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.

Suggested Amendments..TKV committee (check Naavi.org: Oct 16 2017)

- Amendment to ITA 2000/8
  - Section 78..Power to investigate to be provided to Sub Inspector
- CrPc Amendments
  - State Cyber Crime Coordinator proposed (IG Level)
  - District Level Cyber Crime Cells with participation of experts from private sector proposed..Dsp to head+Sub inspectors+atleast 3 experts
- IPC Amendments
  - 153C: Prohibiting incitement to hatred.
  - 505A:Causing Fear, Alarm or Provocation of violence in certain cases.
    - 2 years imprisonment and fine Rs 5000
      - To replace Sec 66A which was scrapped by SC

ITA 2008..Road Ahead for IT Companies

Naavi

How ITA 2008 impacts an IT Company?

- Types of IT Companies
  - Companies for whom Data Protection is Relevant
  - Companies (IT and IT user companies such as Banks) for whom Information Security is relevant
  - Company executives for whom vicarious liabilities on Cyber Crimes are relevant
  - Companies for whom new products and services are relevant

Data Protection

- Section 43A and Section 72 A provide for civil and criminal liabilities under the Act
  - 43A prescribes that a body corporate handing “Sensitive personal Data” should not be negligent in implementing and maintaining “Reasonable Security Practices”
    - Non compliance may result in a liability without any upper limit

Liability under 43A

- Applies to Intermediaries also subject to the provisions of Section 79
  - Intermediaries include telecom service providers, network service providers, webhosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes
  - Sec 79 requires “Due Diligence” to be observed
  - Intermediary has to set up a mechanism for acting when a notice is received about unlawful use of any of his resources

Sec 43 A ..liability extended

- “Abetment””assistance” or “inducement” by an employee of an Intermediary may get extended to the Company through operation of Section 85

New Data Protection Act Expected

- Following the Supreme Court confirmation that Privacy is a fundamental right and the controversies sorrounding Aadhaar
  - Government has set up a Committee under Ret SC Justice Srikrishna, to draft a new Data Protection Act for India
    - Draft expected next week.
      - May have some provisions that overlap with ITA 2008

Liability under 43A

- What is Sensitive Personal Information?
  - As prescribed by the Central Government
    - May include personal identity information, financial information and health information
- What is Reasonable Security Practice?
  - As specified in an agreement between parties or
  - As specified in any law for the time being in force
  - As prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit

Section 43

- Contravention occurs when a specified act is done “without the permission of the owner or any other person who is in charge of a computer”
  - Companies need to put in place mechanisms which does not inadvertently grant permissions or place permission giving authority with all and sundry
    - Any liability that may arise out of the section may get transferred to the Company by operation of Section 85 which requires “Due Diligence” to be practiced

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.

Sec 72A

- Applies when there is disclosure of information in breach of lawful contract
  - Three year imprisonment and fine of upto Rs 5 lakhs
  - Applies to intermediaries also
  - Intent to cause or knowing that he is likely to cause wrongful harm required
  - Lack of consent of the person is required

Sec 72A..liability

- Company need to put in place mechanisms to obtain “Consent” where required in such a manner that it would be acceptable to the Courts
  - Should not be done with misrepresentation
  - Should conform to internationally accepted Privacy principles
  - Contractual terms should be clear
  - Note that liability may arise even when there is no intention but reasonable knowledge
    - Negligence can bring liability

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.

Section 67C

- Central Government is expected to specify
  - the manner and format in which certain data may have to be retained.
  - May also indicate period upto which data has to be retained

Implications of Section 69

- Central Government and State Government can designate officials who can
  - Intercept, monitor or decrypt, information
  - Transmitted, received or Stored in any computer resource
- In national security interests as well as
- For preventing incitement to the commission of any cognizable offence or for investigation of any offence
- Failure to assist may result in imprisonment of 7 years
  - Companies need to watch out for guidelines in this regard and take every step to comply

Implications of Section 69A

- Central Government can designate officials who can
  - Block access to any information generated, transmitted, received, stored or hosted in any computer resource
  - Transmitted, received or Stored in any computer resource
- In national security interests as well as
- For preventing incitement to the commission of any cognizable offence or for investigation of any offence
- Failure to assist may result in imprisonment of 7 years
  - Companies need to watch out for guidelines in this regard and take every step to comply

Implications of Section 69B

- Central Government can designate officials who can
  - Monitor and collect traffic data or information generated, transmitted, received, stored or hosted in any computer resource
  - Transmitted, received or Stored in any computer resource

Failure to assist may result in imprisonment of 3 years

  - Companies need to watch out for guidelines in this regard and take every step to comply

Sec 70-Protected System

- Government reserves the right to notify certain systems as “Protected Systems”
  - Access is regulated, attempt to access unauthorized is an offence
  - Punishment could be upto 10 years
  - May be used for “Critical Infrastructure System”

Vicarious Liabilities

Sec 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:
  - **Provided** that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

Sec 85..contd

- (2)Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place
- with the consent or connivance of, or
- is attributable to any neglect
- on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to 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

Sec 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 (Inserted Vide ITAA 2008)

Sec 79..contd

- (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

Implications of Sec 85

- Where a person committing a contravention is a company, the vicarious liability may extend to its officials and Directors unless they prove
  - lack of knowledge and
  - due diligence
- When a computer resource or an employee of a company has committed the contravention, it may be possible to interpret that the contravention was committed by the Company.
  - Hence vicarious liability may arise on account of any of the penal sections of the Act including Sections 65, 66, 67 etc

Implications of Sec 85

- As a measure of abundant caution therefore every company should undertake such steps as are considered necessary for preventing contraventions with the use of any computer resource belonging to the Company
  - This requires Cyber Law compliance audit
  - Implementation of risk mitigation efforts suggested in the audit
  - Certification of CyLawCom audit

Seven basic compliance requirements

1) Designate a Cyber Law Compliance officer
2) Initiate training of employees on Cyber Law Compliance
3) Introduce sanction procedures in HR policy for non compliance
4) use authentication procedures suggested in law
5) Maintain data retention as suggested under Section 67C
6) Identify and initiate safeguard requirements indicated under Sections 69 and 69A, 69B
7) Initiate global standards of data privacy on collection, retention, access, deletion etc

Some Cases

The Case of Suhas Katti

- State of TN Vs Suhas Katti, The Court of the Additional Chief Metropolitan Magistrate, Egmore, No: 1680/04
- Mr Suhas Katti (SK) and Ms Roselind (R) have studied in a College in Mumbai several years back, SK has proposed marriage, R has politely declined, continue to be friends
- R gets married and later divorced
- SK re-proposes, R again declines

The Case of Suhas Katti..2

- R starts receiving telephone calls at her residence from strangers inviting for company.
  - Callers refer to her message on Yahoo e-groups stating that she is available
    - F says she has not posted such a message and files a Police complaint.

The Case of Suhas Katti..3

- The investigation is initiated
  - First a certified record is made about the commission of the offence through Cyber Evidence Archival Center
  - The identity of the Computer used for posting of the message is traced to addresses in Mumbai.
  - After further enquiry, the complainant discloses the presence of Mr SK, as the only acquaintance in Mumbai they know of.
    - Police visit Mumbai, secure Mr SK, get positive identification from two Cyber Café owners and file charge sheet.

The Case of Suhas Katti..4

- Judgement by Thiru D Arul Raj
  - SK convicted for a total of 5 years of imprisonment and Rs 5000 fine
    - 2 years RI + Rs 4000 under Sec 67 of ITA-2000
    - 2 years RI+ Rs 500 under Section 469 (Forgery for harming reputation)
    - 1 year under + 500 under Section 509 (Insulting the modesty of woman)
      - To run concurrently
  - Commission of offence February 7, 2004
  - Complaint dated February 14 2004
  - Arrest of the Accused on February 18, 2004
  - Date of Judgement November 5, 2004

Cases for study

- State of Tamil Nadu Vs Suhas Katti
  - Application of Section 67/ITA 2000 along with ther sections of IPC, Foregery and Outraging the modesty of woman
  - Acceptability of Section 65B certified electronic document on Yahoo server

Cases for study

- S.Umashankar Vs ICICI Bank (2008)
  - Adjudication against bank for a Phishing fraud
  - Customer had responded to the Phishing Mail in the name of the Bank
  - 6,45,000/- had been transferred out of the account and credited to a current account in ICICI Bank at Mumbai.
  - Rs 4,60,000/- withdrawn by the current account holder
  - Rs 35,000/- adjusted to overdraft
- Adjudication process launched at Chennai
  - Rs 150,000 returned.

Cases for study

- Customer contended that there was negligence on the part of the Bank
  - Invoked Section 43 along with Section 85
  - Negligence for not using digital signature for operations and not identifying an unusual transaction at the Mumbai branch
  - Appropriating part of the proceeds
  - Erasing evidence of CCTV footage etc
- Bank defended
  - Customer was negligent in answering the Phishing mail
  - Contract on the website provides indemnity

Cases for study

- Bank's defence countered
  - RBI Guidelines on Internet Banking
  - Digital signature mandatory under ITA 2000
  - Standard form contract unconscionable
  - Involved forgery
- AO gave his award in favour of the customer in 2010…Bank went on appeal
  - TDSAT confirmed the award
    - Held Bank's negligence tantamounts to "Assistance" under Section 43(g)

Cases for study

- Baazee.com
  - Intermediary liability under Section 79 for a Section 67 offence
    - A customer of Bazee.com posted an obscene video for sale in the C2C E Commerce platform
    - The customer was charged under Section 67 Bazee.com CEO and GM was also charged
      - Acquitted by Supreme Court only beause the Police had filed the case against the CEO without arraigning the Company.
        - Check Naai.org for more details

Digital Evidence

Digital Evidence

- Evidence that can be seen but not seized
- Evidence which is in a hard disk/media which can be siezed
- Evidence that is transitory
- Evidence that has been erased
- Evidence that is hidden

Section 65B of IEA

- Meant for evidence that can be seen but not seized
  - A true copy can be captured in print or on a digital media.
  - Duly certified by the observer

www.ceac.in

Cyber Evidence Archival Center

Articles | Archival | CEAC-EDB | Cyber-Notice | Arbitration | Miscellaneous | FAQ | Contact | Collaboration | Home | Activity | Members

Home

What this Cyber Evidence Archival Center is All About

CEAC is a Multifaceted Service Center providing a **"Trusted Third Party Cyber Law Assurance Service"** .The service is a first of the kind global service backed by the provisions of Information Technology Act 2000 (ITA 2000) as amended by Information Technology Act 2008 (ITA 2008).

CEAC was started in 2002 to provide assistance to Cyber Law Practitioners and Law Enforcement Agencies with a service that can convert electronic evidence into admissible paper evidence for the purpose of submission in a Court of Law as per Section 65B of Indian Evidence Act. CEAC is proud to have been associated with the Chennai Police in

Search

Social

Recent Posts

- Contemporaneous Certification required under Section 65B
- Evidence Drop Box and Shapoorji Pallonji E Tender Case
- Why there cannot be a standard format for Section 65B Certificate
- Affidavit is not the correct format of Section 65B Certificate
- Wisdom from Puri..on Section 65B and Section 79A

Amendments to IEA

Section 3

- Evidence Means and Includes..
  - (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry;such statements are called oral evidence;
  - (2) all document including electronic records produced for the inspection of the Court, such statements are called documentary evidence;

Section 17

- **17. Admission defined**
- An admission is a statement,
  - oral or
  - documentary or
  - contained in electronic form,
    - which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances, hereinafter mentioned.

Classes of Evidentiary Statements

- According to the amended section 3 it appears that evidence is classified into only two categories namely Oral and Documentary
- According to amended Section 17, it appears that evidence can be classified into three categories, namely Oral, Documentary and Electronic documents

Section 65A of Indian Evidence Act

- 65A. **Special provisions** as to evidence relating to electronic record –
  - The contents of electronic records may be proved in accordance with the provisions of section 65B.
    - Inserted vide Information Technology Act 2000 with effect from 17th October 2000

65A is independent of other sections

- According to Section 61
  - Contents of documents may be proved either by Primary or by Secondary evidence
- According to Section 62
  - Primary Evidence means the document itself produced for the inspection of the Court

65A is independent of other sections

- According to Section 63
  - Secondary Evidence means and includes
    - Certified copies given under the provisions hereinafter contained;
    - Copies made from the original by **mechanical processes** which in themselves insure the accuracy of the copy and copies compared with such copies;
    - Copies made from or compared with the original;
    - Counterparts of documents as against the parties who did not execute them;
    - Oral accounts of the contents of a document given by some person who has himself seen it.

65A is independent of other sections

- According to Section 64
  - Documents must be proved by primary evidence except in the cases hereinafter mentioned.
- Acceptance of Secondary Evidence is therefore only an exceptional provision
- It is subject to conditions mentioned in Section 65

Exceptions for invoking Section 65

- Secondary evidence may be given of the existence, condition or contents of a document in the following cases:
  - (a) When the original is shown or appears to be in the possession or power of the person against whom the document is sought to be proved, or of any person **out of reach of,** or not subject to, the process of the Court, or of any person legally bound to produce it, and when, after the notice mentioned in Section 66, such person does not produce it;
  - (b) When the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest;
  - (c) When the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;
  - (d) When the original is of such a nature as not to be **easily movable**;
  - (e) When the original is a public document within the meaning of Section 74;
  - (f) When the original is a document of which a certified copy is permitted by this Act, or by any other law in force in India to be given in evidence;
  - (g) When the originals consist of numerous accounts or other documents which cannot conveniently be examined in Court, and the fact to be proved is the general result of the whole collections.

Sec 65A

- Sec 65A is titled: "**Special provisions** as to evidence relating to electronic record"
  - Why does Section 65A call it a "Special Provision"
    - if it was not to distinguish electronic evidence from the "Secondary Evidence" as referred to in Section 65?

“Primary” and “Secondary” in Electronic Documents

- Any electronic document whether it is primary or secondary is not
  - Humanly readable.
  - Court cannot take a view of its own.
    - Because the document is written in binary language
    - Readable only in a binary reading device (computer)

“Primary” and “Secondary” in Electronic Documents

- Hence Electronic Documents are to be always produced only with another human being providing a written testimony to what the document contains.
  - Hence it is not necessary to discuss “Primary” and “Secondary” nature of documents in electronic form.

Is hard disk a “Primary Evidence”?

- The hard disk that is taken out of a computer and said to contain an electronic document
  - Is only a “Container” of an “Electronic Document” and not the electronic document itself
    - Applies even to a CD which contains only one document which is under reference of the Court.

Is hard disk a “Primary Evidence”?

- The subject document can only be read by a human being when the “container” is connected to a compatible electro mechanical device namely the “Computer System” and read through an operating system such as Windows with an application such as “Microsoft word”
  - Even if the Judge fixes a computer in the Court room and himself reads the document, his reading is dependent on the device called the “Computer”, the operating system and the application which should be functioning normally.

Every Electronic Document has to be "Certified"

- Hence an electronic document has to be always certified to the effect
  - "This is what the document means when read in a computer with appropriate application running in an appropriate operating system"
    - The person who provides the certification assists the Court like an "Expert"
  - This has been recognized and implemented in the Section 65A calling itself as "Special Provision" and indicating the certification process under "Section 65B"

Section 65B Requirement

- Section 65B of Indian Evidence Act
  - Indicates the manner in which a certificate has to be produced in order to make an electronic document admissible in a Court.
    - It is immaterial to discuss whether it is admissible as a “Primary” document or a “Secondary” document

65B. Admissibility of electronic records.-

Two Output Modes-
Print out,
Soft copy

- (1) Notwithstanding anything contained in this Act,
  - any information contained in an electronic record
  - which is printed on a paper,
  - stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output)
    - shall be deemed to be **also a document**,
      - if the conditions mentioned in this section are satisfied in relation to the information and computer in question and
      - shall be admissible in any proceedings, **without further proof or production of the original,**
      - as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

65B. Admissibility of electroni records.-conditions

Said Period? Person with lawful control?

- (2) The conditions referred to in sub-section (1) in respect of a **computer output** shall be the following, namely:—
  - (a) the computer output containing the information **was produced** by the computer **during the period** over which the computer was used regularly to store or process information for the purposes of **any activities** regularly carried on over that **period** by the **person having lawful control over the use of the computer;**
  - (b) during the said period, information **of the kind** contained in the electronic record or of the kind **from which the information so contained is derived** was regularly fed into the computer **in the ordinary course of the said activities**;
  - (c) throughout the material part of the **said period**, the computer was **operating properly** or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
  - (d) the information contained in the electronic record **reproduces** or is derived from such information fed into the computer in the ordinary course of the said

Computer Output?..printout or copy

65B. Admissibility of electronic records.-Multiple Computers

- (3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—
  - (a) by a combination of computers operating over that period; or
  - (b) by different computers operating in succession over that period; or
  - (c) by different combinations of computers operating in succession over that period; or
  - (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,
- all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

65B. Admissibility of electronic records.-certification

- (4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—
  - (a) identifying the electronic record containing the statement and describing the manner in which it was produced;
  - (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
  - (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,
- and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate)
  - shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

65B. Admissibility of electronic records.-certification

- (5) For the purposes of this section,—
  - (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
  - (b) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
  - (c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
- Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

Cases for study

- Basheer Case
  - Section 65B… Mandatory for electronic documents…Oral evidence not acceptable..etc
  - Admissibility and Genuineness are different stages
  - Sec 65B at the time of Admission, Section 45A at the time of genuineness
    - Refer ceac.in for details

Cases for study

- Shaporji Pallonji
  - E Tender process not followed for alleged technical failure
    - Refer naavi.org for details

Cases for study

- Shafhi Mohammad
  - Court has discretion to accept electronic evidence and waive Section 65B
    - Refer naavi.org for details

New Laws on the horizon

- Personal Data Protection Act 2018
  - Refer www.pdpa2018.in
  - Participate in www.fdppi.in
- Replaces Section 43A
  - Introduces new concepts of Personal Data, Sensitive Personal Data, Compliance, etc
  - New Civil and Criminal liabilities etc

Thank You…Questions?

- Contact me at: www.naavi.org
- Or through the Android App