

Non Disclosure Agreements

Naavi

@ Nalsar

27th November 2020

1

Naavi

1

Agenda

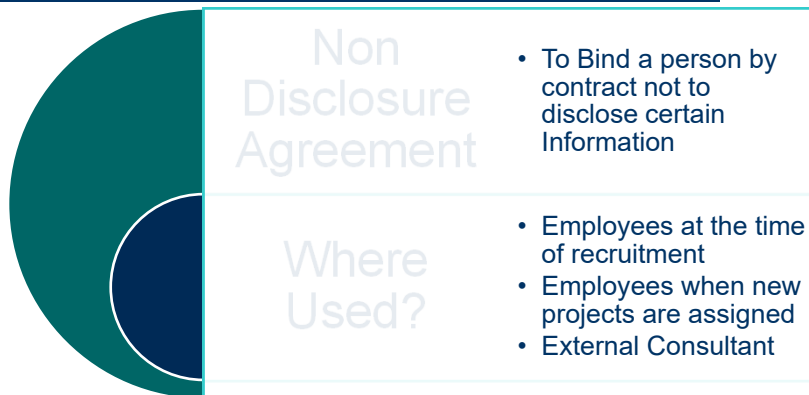
- What is NDA?
- Where are they used?
- What are the legal precedence?
- Examples

2

Naavi

2

What is NDA?



3

Naavi

3

Requirements of an NDA

NDA needs to meet the general requirements of a Contract under Indian Contract Act

Free will- No threat or coercion, undue influence, fraud or misrepresentation or mistake of fact

Not an Unconscionable Contract

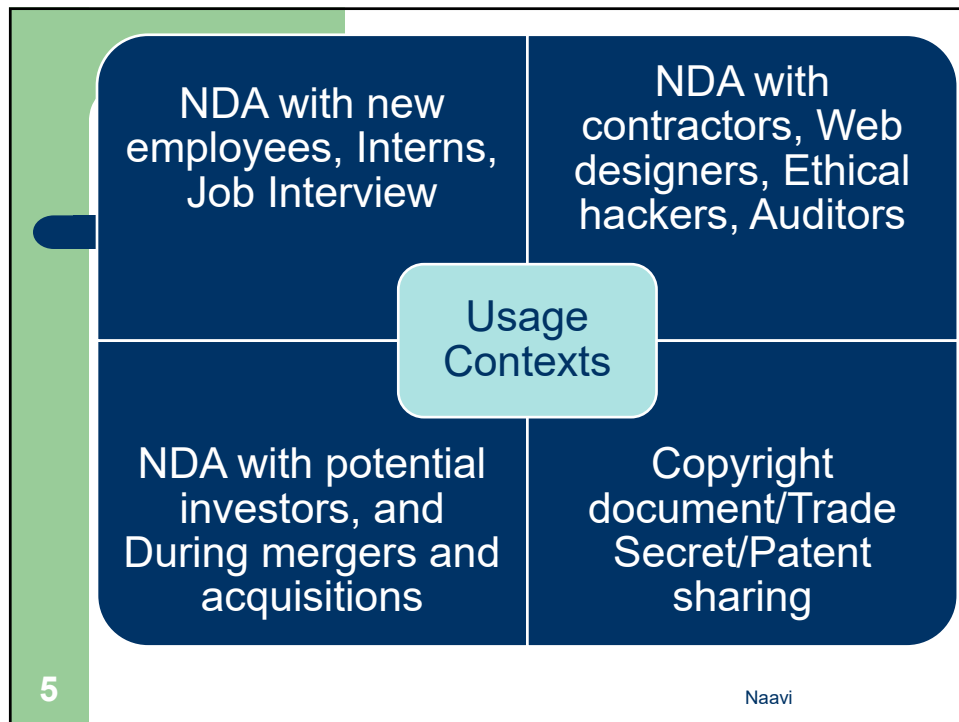
Need for authentication recognized in law

Should be stamped in physical form

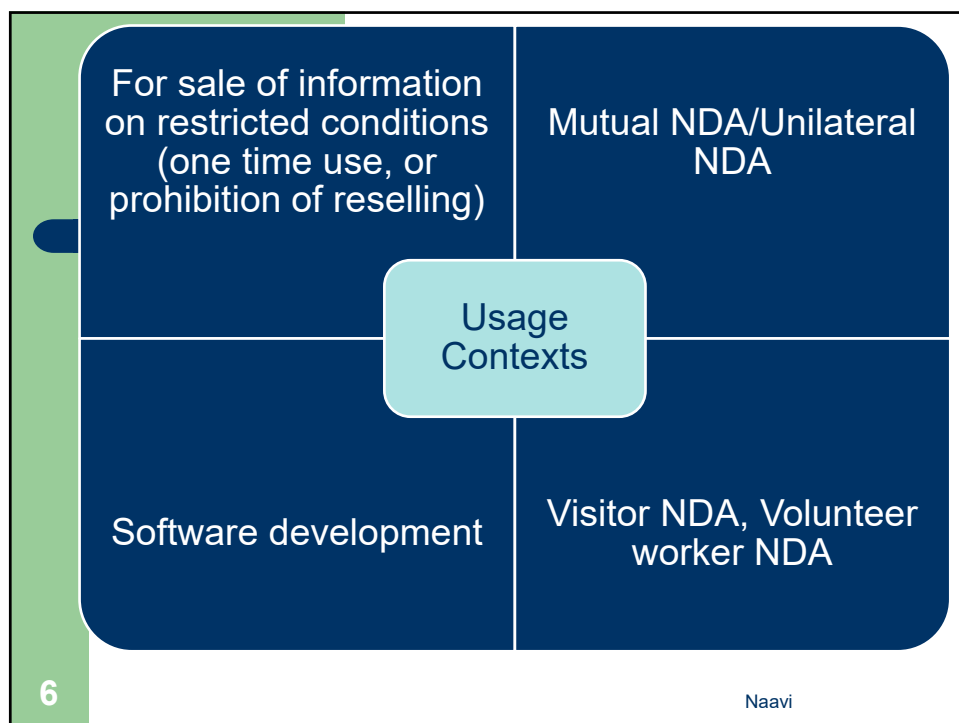
4

Naavi

4



5



6

Contents of an NDA



- Parties to Contract with Contact Details
- Background and Context
- Applicability. To what information it refers to
- What information is likely to be shared and how?

7

Naavi

7

Contents of an NDA



- Period of the obligation...beyond the basic contractual period
- Date of contract, commencement and Termination
- Indemnity, Waiver etc
- Jurisdiction, Dispute resolution, severability, public information, legal impediments, God's hand

8

Naavi

8

Definition of Confidential Information

1

- For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged

2

- If Confidential Information is in written form, the Disclosing Party shall label or stamp the materials with the word "Confidential" or some similar warning.

3

- If Confidential Information is transmitted orally, the Disclosing Party shall promptly provide a writing indicating that such oral communication constituted Confidential Information

9

Naavi

9

Exclusions: Receiving Party Obligations does not extend to..

1

- publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party;

2

- discovered or created by the Receiving Party before disclosure by Disclosing Party; .

3

- learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or

4

- is disclosed by Receiving Party with Disclosing Party's prior written approval.

10

Naavi

10

Obligations of Receiving party

Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party.



Receiving Party shall carefully restrict access to Confidential Information to employees, contractors and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions at least as protective as those in this Agreement.

11

Naavi

11

Obligations of Receiving party

Receiving Party shall not, without the prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information



Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.

12

Naavi

12

Period

Could Extend beyond the Termination of the Contract



Should be for a reasonable period



Perpetual Contract may be invalidated by Courts as unconscionable

13

Naavi

13

Special Care to be Exercised

- Confidentiality definition should not be too broad
- Correct description of the name of the party and the company
- Unreasonable and onerous clauses to be avoided (eg: Indefinite period of confidentiality)
- NDAs cannot lawfully prohibit employees from officially reporting illegal conduct.
- Information provided by third party not to be included
- Information already known or in public domain to be exempted

14

Naavi

14

Special Care to be exercised

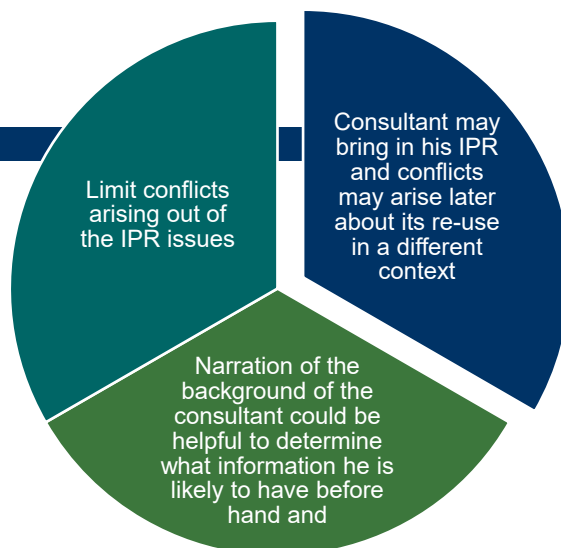
- Receiving party developing the information independently
- Disclosures made prior to NDA
- Signed by a person with proper authority
- Correct jurisdiction
- Adequate due diligence to be exercised by the Company
- Compelled disclosure

15

Naavi

15

Consultancy Related Contracts



16

Naavi

16

Remedial Action

- Cease and Desist letter
- Ombudsman
- Mediation
- Arbitration
- Jurisdiction of Courts
- Limitations to damage

17

Naavi

17

Negative covenant enforceable during the term of employment

- In the case of *Niranjan Shankar Golikari* [3]
 - the Apex Court held
 - Negative covenants operative during the period of the contract of employment when the employee is bound to serve his employer exclusively are generally not regarded as restraint of trade and therefore do not fall under Section 27 of the Contract Act.

Sec 27: Every agreement by which anyone is restrained from exercising a lawful profession or trade or business of any kind, is to that extent void"

18

Naavi

18

Negative covenant enforceable during the term of employment

- Meanwhile, in *Wipro Ltd. v. Beckman Coulter International S. A*^[4]
- the court held that
- negative covenants between employer and employee contracts pertaining to **the period post termination** and
- restricting an employee's right to seek employment and/or to do business in the same field as the employer would be a restraint of trade and
- therefore, a stipulation to this effect in the contract would be void.

19

Naavi

19

Is an NDA in restraint of trade?

- The Bombay High Court in *VFS Global Services Pvt Ltd* held that
 - a clause prohibiting an employee from disclosing commercial or trade secrets is not in restraint of trade.
 - The effect of such a clause is not to restrain the employee from exercising a lawful profession, trade or business within the meaning of Section 27 of the Contract Act.

20

Naavi

20

Is an NDA in restraint of trade?

- The Delhi High Court in
 - *Mr. Diljeet Titus, Advocate v. Alfred A Adebare and Ors*
 - **Dispute between an advocate and associates**
 - Were the parties working for Titus or were they partners?
 - When defendants left the firm, they took away privileged information
 - Court restrained the Defendant from misappropriating the information including the lists of clients and other information forming the database of the firm,

21

Naavi

21

Key principles in NDA

- **Inevitable Disclosure Doctrine** –
 - Under this court-made rule, adopted by only a few courts, a court can stop an ex-employee from working for a competitor if the former employer shows that the employee will “inevitably disclose” trade secrets of the former employer.
- **Non-Solicitation Provision** (also known as a “diversion provision”)
 - An agreement that restricts an ex-employee’s ability to solicit clients or employees of the ex-employer.
- **Option Agreement** –
 - An agreement in which one party pays the other for the opportunity to later exploit an innovation, idea or product.

22

Naavi

22

Advent of Data Protection Act

- Data Protection Act imposes a higher level of diligence on the “Data Controller/Data Fiduciary”
 - To ensure that “Personal data is held confidential”
 - To hold the required “Consent” before it is disclosed.
 - Consent should be specific and explicit in case of Sensitive Personal information
 - Eg: PWC case

23

Naavi

23

Hellenic DPA-PWC-Penalties

- Administrative fine of Euro 150,000 fine based on the published net annual turnover of EUR 41,936,426 (0.35%)
- Processed the personal data of its employees in an unfair and non transparent manner
 - contrary to the provisions of the GDPR giving them the false impression that it was processing their data under the legal basis of consent while in reality it was processing their data under a different legal basis about which the employees had never been informed.

24

Know How and Trade Secrets

- Trade secret law tries to balance
 - companies' need to keep certain things secret with employees' desire to transfer skills between employers.
- Technical Knowhow may not all be "Trade Secrets"
- The problem is that NDAs are often written broadly, and once an employee signs one, the case against them is stronger should they take their know-how to a competitor.
- Not all courts are diligent in policing the lines between general knowledge and confidential information.
 - Therefore, signing a broad NDA opens employees up to legal risk beyond what trade secret law otherwise would protect.

25

Naavi

25

Non-Disparagement Clause

- A new common extension of NDAs is the inclusion of a non-disparagement clause, which beyond the protection of concrete corporate information
- requires employees to never speak negatively about their employer or former employer.
 - A boilerplate non-disparagement clause reads
 - "you shall not at any time, directly or indirectly, disparage the Company, including making or publishing any statement, written, oral, electronic or digital, truthful or otherwise, which may adversely affect the business, public image, reputation or goodwill of the company, including its operations, employees, directors and its past, present or future products or services."

26

Naavi

26

BSNL Tender (BSNL Vs Chander Shekar, 23rd March 2012)

- BSNL invited a tender signing NDA with the bidders
- Bids were opened but subsequently Tender was cancelled
- One of the bidders filed for information on the bidding process settlement but CPIO refused.
- The first appeal was against the CPIO.
 - Another appeal was made to the Delhi High Court by the CPIO

27

Naavi

27

BSNL Tender (BSNL Vs Chander Shekar, 23rd March 2012)

- i) that the evaluation process stood completed and thus the commercial position of any of the bidders could not be adversely affected by such disclosure;
- ii) the exemption under Section 8(1)(d) of the Act is not available since the information was already in public domain owing to the finalization and completion of the bidding process and evaluation and cannot pose a threat to the competitive position of any of the bidders;
- iii) it was in the larger public interest to disclose such information;

28

Naavi

28

BSNL Tender (BSNL Vs Chander Shekar, 23rd March 2012)

- iv) that the Non Disclosure Agreements were valid only for the "Confidentiality Period" i.e. till the opening of the bids;
- v) even otherwise such Non Disclosure Agreements debarring access to information and thereby disrupting the transparency and accountability of the public authority were in violation of the very spirit of the Act and therefore illegal to the extent they prevented disclosure beyond what was exempted under the Act;
- vi) that thus the Non Disclosure Agreements if prevented disclosure beyond the confidentiality period also, were illegal;
- vii) that the public interest "far outweighs the weak contentions put up by the appellant to protect the so called private interests";
- viii) that even though the tender process had been challenged in some of the High Courts but the same also did not entitle the appellant to exemption. Accordingly, directions for disclosing the information were issued.

29

Naavi

29

BSNL Tender (BSNL Vs Chander Shekar, 23rd March 2012)

- Though the Non Disclosure Agreement extended the obligation of confidentiality beyond the date of opening of the tenders also but only for a period of two years from the date of disclosure or to the completion of business purpose whichever is later.
- The business purpose stands abandoned with the scrapping of the tenders.
- However, we are of the opinion that disclosure of such information which would be part of the evaluation process would still require a notice to be given to the third party.
- Appeal partly allowed and remanded back to CIC

30

Naavi

30



31



32

Digital Evidence

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

33

Naavi

www.naavi.org

33

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

34

Naavi

www.naavi.org

34

35



www.ceac.in

Cyber Evidence Archival Center

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

Naavi
www.naavi.org

35

Amendments to IEA

36

Cyber Law College

Naavi

36

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;

37

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.

38

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

39

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

40

Cyber Law College

Naavi

40

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

41

Cyber Law College

Naavi

41

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.

42

Cyber Law College

Naavi

42

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

43

Cyber Law College

Naavi

43

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.

44

Cyber Law College

Naavi

44

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?

45

Cyber Law College

Naavi

45

“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)

46

Cyber Law College

Naavi

46

“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.

47

Cyber Law College

Naavi

47

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.

48

Cyber Law College

Naavi

48

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.

49

Cyber Law College

Naavi

49

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”

50

Cyber Law College

Naavi

50

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

51

Cyber Law College

Naavi

51

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.

52

Cyber Law College

Naavi

52

65B. Admissibility of electronic 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

Cyber Law College

Naavi

53

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.

54

Cyber Law College

Naavi

54

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.

55

Cyber Law College

Naavi

55

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.

56

Cyber Law College

Naavi

56

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

57

Naavi

www.naavi.org

57

Cases for study

- Shaporji Pallonji

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

58

Naavi

www.naavi.org

58

Cases for study

- **Shafhi Mohammad**
 - Court has discretion to accept electronic evidence and waive Section 65B
 - Refer naavi.org for details
 - **Arjun Panditrao Khotkar V. Kailash Kushanrao Gorantyal**
 - Clarified that Shafi Mohammad ruling was incorrect

59

Naavi

www.naavi.org

59

Thank You

- Naavi
- naavi@naavi.org
- 9343554943

For more information

Refer

www.naavi.org

-E Books on Cyber Crimes, Electronic Signatures, Section 65B etc

-Print book on Personal Data Protection Act

60

Naavi

60