Offences under ITA 2008

..contd

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
      - <u>that is restricted for reasons of the security of the state or foreign relations</u> 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 <u>one-half of the longest term of imprisonment provided for that offence</u>, 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

..continued

Jurisdiction Issues in Cyber Space

Naavi

@ Nalsar

18th October 2019

Basic Principles

- International law limits a country's authority to exercise jurisdiction in cases that involve interests or activities of Non Residents

Three Types

- Jurisdiction to Prescribe
  - Legal Jurisdiction
- Jurisdiction to Adjudicate
  - Judicial Jurisdiction
- Jurisdiction to Enforce
  - Enforcement Jurisdiction

Jurisdiction to Prescribe

- Jurisdiction to prescribe exists with respect to
  - Conduct that wholly or in substantial part **takes place within the territory**
  - Conduct outside its territory that has or is **intended to have substantial effect** within its territory
  - The activities, interests, status or relations of **its nationals** outside as well as within its territory
  - Certain conduct outside its territory by persons who are not its nationals that is directed **against the security** of the country or against a limited class of other national interests

Jurisdiction to adjudicate

- Tribunals/Courts of a given country may resolve a dispute in respect to a person or thing where the country has a jurisdiction to prescribe the law that is sought to be enforced
  - There must be reasonable links between the defendant and the forum state in terms of substantial, direct and foreseeable effect within the country from his conduct

Jurisdiction to Enforce

- A Country may employ judicial and non judicial measures to induce or compel compliance or punish non compliance with its laws or regulations provided it has jurisdiction to prescribe.
- A country may employ enforcement measures against a person located outside its territory if
  - The person is given notice of the claims or charges against him that are reasonable in circumstances
  - Person is given an opportunity to be heard in advance of enforcement and
  - Where enforcement is through courts if the country has jurisdiction to adjudicate.

Minimum Contact Principle

- Cybersell, Inc v Cyber Sell Inc, 130 F 3d 414 (9^{th} Cir 1997)
  - Plaintiff was an **Arizona** corporation that advertised its commercial services over the Internet
  - Defendant Cybersell FL was a corporation in **Florida** offering similar services
  - Defendant did not have offices, did not advertise, had no clients in Arizona
  - Plaintiff informed the defendant about the existence of their registered service mark and filed a suit in Arizona.
  - District court dismissed the case for lack of personal jurisdiction and Court of Appeals affirmed the decision.

Minimum Contact Principle..2

- Cybersell, Inc v Cyber Sell Inc, 130 F 3d 414 (9^{th} Cir 1997)
  - Court applied a three part test of minimum contact test
    - Defendant had not purposefully availed itself of the privilege of conducting business in the forum state
    - No Arizon except for the plaintiff accessed the defendant’s website
    - Court classified the website as “Essentially passive” and it did not “deliberately” direct its efforts towards Arizona residents.
      - Declined to exercise jurisdiction

Yahoo-French Government (2001-2006)

- Is Yahoo subject to the jurisdiction of
  - French Law/French Courts ?
  - If so, Are there any limitations?
    - Does French Jurisdiction extend to Yahoo if its action hurts the sentiments of the French?

Yahoo and Nazi Memorabilia

- On Yahoo.com's auction site, more than 1,200 Nazi-related items -- everything from Nazi flags and uniforms to belt buckles and medals -- are offered to cyberspace consumers under the shield of U.S. notions of free expression.
- Yahoo's France-based subsidiary, Yahoo France, did not host auctions for Nazi memorabilia.
  - organizations sought to stop the English-language auction sales from appearing in France.

Yahoo-French Government (2001-2006)..2

- French Government Rules that Yahoo cannot auction Nazi Memorabilia through its site
  - Ruled that Yahoo must put a three-part system in place that includes
    - filtering by IP address,
    - the blocking of ten keywords, and
    - self-identification of geographic location.
    - Three months to put the system in place, after which time the company would be subject to a fine of 100,000 francs ($13,000) a day if the system has not been implemented.
  - Yahoo accepts for Yahoo-France site
  - Rejects for Yahoo-US site
  - Also Refuses to block access to French people

Yahoo-French Government (2001-2006)..3

- U.S. District Court for the Northern District of California in San Jose
  - Upholds Yahoo’s Rights not to block the site as it would amount to curbing Freedom of Speech
- Appeal Filed at Ninth U.S. Circuit Court of Appeals
  - judgment delivered on 26th August 2004, Yahoo lost. A Six bench Court, rejected Yahoo's arguments, for two different reasons.
  - Three judges ruled that California courts have no jurisdiction over the French organizations.
  - Another three judges stated that the case isn't "ripe," meaning Yahoo hasn't suffered sufficient hardship stemming from the French court's decision.

Yahoo-French Government (2001-2006)..4

- Yahoo then asked the appeals court to again hear the case with 11 judges.
- That appeal was argued in March 2005, and the court's decision was handed down on 12th January 2006.
- The Court dismissed Yahoo's contention.
  - These developments, therefore upheld the right of French Government to ensure blockage of the objectionable content from the website.

GDPR Case Against Google (CNIL Vs Google)

- Google Search Engine received a “Right to Forget” request from a data subject.
  - Google removed the information from search data presented in France
  - The French Supervisory authorities demanded that it be removed from search results across the Globe.
    - EU Court held
      - ***…There is no obligation under EU law for a search engine operator to extend the rule beyond the EU States***

GDPR Case Against Google (CNIL Vs Google)

- By decision of 21 May 2015, the President of the CNIL served formal notice on Google that,
  - when granting a request from a natural person for links to web pages to be removed from the list of results displayed following a search conducted on the basis of that person's name, it must apply that removal to all its search engine's domain name extensions.
- Google refused to comply with that formal notice,
  - confining itself to removing the links in question from only the results displayed following searches conducted from the domain names corresponding to the versions of its search engine in the Member States.

CNIL Vs Google (GDPR)

- The CNIL also regarded as insufficient Google's further 'geo-blocking' proposal,
  - whereby internet users would be prevented from accessing the results at issue from an IP (Internet Protocol) address deemed to be located in the State of residence of a data subject after conducting a search on the basis of that data subject's name,
    - no matter which version of the search engine they used.
      - CNIL fined Euro 100000 after adjudication

CNIL Vs Google

- where a search engine operator grants a request for de-referencing pursuant to those provisions,
  - that operator is not required to carry out that de-referencing on all versions of its search engine,
  - but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements,
  - effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.

The Indian Scenario

…

The Indian Scenario

- Civil Procedure Code
  - Suit for relief or compensation for wrong to an immovable property held by the defendant where the relief sought can be obtained entirely though his personal obedience can be filed
    - Where the property is situated or works
    - Where the defendant resides or carries on business
      - If the immovable property is situated in multiple jurisdiction, suit may be filed in either place

The Indian Scenario..2

- In case of compensation for wrong to a person or to movables
  - At the option of the plaintiff any of the following is applicable.
    - Where the person resides, carries on business or works at the time the suit is instituted
    - Where the cause of action wholly or partly arises
    - Place of principle office in case of a Company if it is not carrying on business in the place where the cause of action arose.

The Indian Scenario..3

- According to Supreme Court decisions
  - The making of a contract is part of the cause of action and hence suit can be filed in the place where the contract was made.
  - For determining where the contract was made, where the acceptance was given is the determining factor.
  - Performance of the contract is also part of the cause of action and hence a case can be filed where the contract ought to have been performed
  - Place where the repudiation was received or money payment ought to have been received and not received are also within the jurisdiction.

Indian Scenario..4

- In Copyright Act
  - Notwithstanding anything contained in Civil Procedure Code
    - Proceedings can be instituted in a place where the plaintiff is situated
- In Trademark disputes
  - The place where the infringement was made through sales
- In Contract Act
  - Specification of jurisdiction permissible
    - Supreme Court has however ruled that this cannot be used as a means of oppression.

Indian Scenario..5

- Jurisdiction of Courts may be determined by
  - Pecuniary Jurisdiction
    - Based on the value of the dispute
  - Territorial Jurisdiction
    - Based on the location
  - Subject matter Jurisdiction
    - Based on the nature of dispute

The Difficulties in Cyber Transactions

- Property may be neither immovable nor movable
  - Eg: Domain Name, Web space
- The damage may be to a Virtual entity and not a physical entity
  - eg: Defamation of a pseudo name or an e-mail identity
- Cause of action is not defined
  - Eg: Copyright violation claim when the infringed material is not visible to human beings (Euregio.net Vs Women.com)
    - (http://www.naavi.org/cl_editorial/edit_01jul_01_1.html)

The Indian Scenario-Cyber transactions

- Section 75 of ITA-2000
  - **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

Indian Scenario..2

- ITA-2000 as well as other UNCITRAL based laws define attribution and the place of despatch and receipt of communication

The Silver Lining..2

- The acceptance of Alternate Forms of Dispute Resolution’
  - Through Arbitration
    - May also be an expression of Forum Choice with representation from different countries

Jurisdiction in Arbitration

- Arbitration contracts define
  - Seat of Arbitration
  - Applicable Law
- Enforcement in India is subject to CPC
  - The Supreme Court has held that
  - enforcement of an Arbitral Award may be filed in any jurisdiction in the country,
  - for execution, where such decree is capable of being executed and there is no requirement of obtaining a transfer of the decree from the court which has jurisdiction over the arbitration proceedings.

Non Disclosure Agreements

Naavi

@ Nalsar

18th October 2019

Agenda

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

What is an NDA?

- NDA means a “Non Disclosure Agreement”
  - As the name suggests it tries to bind a person by contract not to disclose certain information.
  - Often used in employment scenario
  - Also used when an external consultant is entrusted with some work that requires sharing of confidential information
  - Can also be used in internal projects where an employee is entrusted to a new highly confidential project

NDA is an agreement

- Needs to meet the general requirements of the Indian Contract Act
  - Competency to contract
  - Could be unilateral, bilateral mutual) or Multilateral
  - Free Consent (No misrepresentation, fraud, Coercion, threat, undue influence, mistake of fact)
  - Valid consideration (legal)
  - Need for authentication recognized in law to be considered as a written, documentary contract not to be limited by the principle of "Unconcsionable contracts"
  - NDA should be stamped like an agreement

Usage contexts

- NDA with new employees, Interns, Job Interview
- NDA with contractors, Web designers, Ethical hackers, Auditors
- NDA with potential investors, and During mergers and acquisitions
- Copyright document sharing (eg; Film script)
- For sale of information on restricted conditions (one time use, or prohibition of reselling)
- Mutual NDA/Unilateral NDA
- Trade Secret or Patent NDA
- Software development
- Visitor NDA, Volunteer worker NDA

Contents

- The parties to the contract, their contact details
- Background and the context
- Applicability..the information to which it refers to
- What information is likely to be shared and how?
- 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

Applicability

- 1. Definition of Confidential Information.
  - 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.
  - If Confidential Information is in written form, the Disclosing Party shall label or stamp the materials with the word "Confidential" or some similar warning.
  - If Confidential Information is transmitted orally, the Disclosing Party shall promptly provide a writing indicating that such oral communication constituted Confidential Information.

Applicability

- 2. Exclusions from Confidential Information.
  - Receiving Party's obligations under this Agreement do not extend to information that is:
    - (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party;
    - (b) discovered or created by the Receiving Party before disclosure by Disclosing Party;
    - (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or
    - (d) is disclosed by Receiving Party with Disclosing Party's prior written approval.

Obligations

- 3. **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.

Obligations

- 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.

Period

- Could extend beyond the termination of the Contract
  - Should be for a reasonable period
  - Perpetual Contract may be invalidated by Courts as unconscionable
- NDAs cannot lawfully prohibit employees from officially reporting illegal conduct.

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)
- Information provided by third party not to be included
- Information already known or in public domain to be exempted
- 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

Context

- In case of consultancy related NDAs
  - Consultant may bring in his IPR and conflicts may arise later about its re-use in a different context
  - Narration of the background of the consultant could be helpful to determine what information he is likely to have before hand and
  - Limit conflicts arising out of the IPR issues

Remedial Action

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

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.

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.

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.

Is an NDA in restraint of trade?

- The Delhi High Court in
  - *Mr.* ***Diljeet Titus, Advocate v. Alfred A Adebare and Ors***
    - restrained the Defendant from misappropriating the information including the lists of clients and other information forming the database of the firm,

Key principles

- **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.

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

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.

Hellenic DPA-PWC..Complaint

- Complaint against PWC BS (PWC Business Solutions)
  - From an employee … that “Employees were required to provide consent to the processing of their personal data”
  - Conducted an ex-officio investigation of the lawfulness of the processing of personal data

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.

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.”

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

- BSNL invited a tender signing NDA with the bidders
- Bids were opened but subsequently Tender wscancelled
- 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

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;

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.

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

Thank You

- Contact
  - naavi@naavi.org
  - www.naavi.org
  - www.cyberlawcollege.com