Chapter VII

Changing Face of Cybercrime

The recent robber can take more with a computer than with a pistol. Tomorrow’s terrorists’ use keyboard than a bomb to do more damage.

“The Duty to Disclose Knowledge of Crime rests upon all citizens.”

INTRODUCTION

Privacy is the interest that persons have in satisfying a ‘private space’, free from intrusion by other people.

This chapter deals with, right to independence of speech and expression and the right to secrecy shall be discussed. The constitutional provisions under Article 19 and Article 21 and certain landmark judgments are discussed in this chapter. A research has been conducted as to how The I.T. Act, 2000 and Amended Act, 2008 has taken necessary steps in preventing violation of these Articles.

Constitutional Provisions

Article 19 - Speech and Expression and its Freedom and Restrictions Article 19(2) which include Decency and Morality. Indecency results in obscenity and it is a subject of constitutional interest as it can deprave and corrupt the community. Therefore it is the duty of the state to prohibit such obscenity so as to promote decency and morality.

In the landmark judgment, namely Ranjit.D.Udeshi v State of Maharashtra which the court upheld that the novel in question was obscene. It was further held that obscene matter must be considered separately and whether it will deprave and corrupt the minds of the readers. Further Article 21 – Protection of Personal Liberty, Life includes in its ambit the Right to privacy.

Article 21, of the Indian Constitution, Protection of Personal Liberty, and Life: Which states that every individual shall have his right to life and cannot be deprived of it only through legal
procedures? The right safeguards from invasion upon personal freedom and deprivation of life except according law. iii

In another historic judgment in People’s Union for Civil Liberties v Union of India iv popularly known as “Phone Tapping Case,” the Apex Court has held that tapping of telephone is a serious invasion of an individual’s right to privacy which is a part of the right to “Life and personal Liberty”. The court further stated that such a right cannot be encroached unless there is a public emergency or essential for public safety. The court has laid the following procedural safeguards for exercise of power i.e. a permission of the Home Secretary of Central Government or the State Government is required. There can be an authority appointed to review such and he shall maintain the records of intercepted communications.v

In R. Rajagopal v State of Tamil Nadu vi popularly known as “Auto Shanker case” the Apex Court has stated that the right to privacy and the right to be let by yourself, are guaranteed under Article 21. It is stated that every citizen has the right to protection. No one can publish anything of the above without their consent unless such publication is based on court records.

In State of Maharashtra v Madhukar Narain vii it was held that right to privacy is available even to woman of easy virtue and no one can invade her privacy.
In Mr. ‘X’ v Hospital ‘Z’ viii the court laid that restrictions can be imposed on right to privacy if it is for deterrence of crime, disorder or defense of health or ethics.

In Malak Singh v State of Punjab ix it was held by the Apex Court that keeping surveillance on persons with bad character and habitual offenders is allowed in order to prevent crime in future. But if it is done for innocent persons then it may amount to violation of right to privacy.

In another case Rayala M. Bhuvaneswari v Nagaphamender Rayala x it was held by the honorable Apex Court that tapping conversation of his wife with others seeking to produce in court violates her right to privacy and also if every conversation with her parents is tapped by the husband then it shall amount to failure of the institution of marriage.
This right has been further envisaged in *Maneka Gandhi v Union of India*\(^{xi}\) and *Bandhua Mookti Morcha v Union of India and Other*\(^{xii}\) where it confers on every person the fundamental right to life and personal liberty which has become inexhaustible source of many other rights.\(^{xiii}\) The article further expands the right of every person to live with dignity free from exploitation. It is the duty of the state to see that there is no violation of fundamental right of a person.

The meaning of the word life has in it the right to live in reasonable conditions, right to rehabilitation after release, right to livelihood by legal means and decent environment.

- **Expansive Interpretation of Article 21**
  Article 21 has further expanded concept of ‘privacy’ - is to search and seizure, to dignity and protection of personal rights. Black’s law dictionary states that right to be let alone; the right of a person to be free from unwarranted publicity; and the right to live without unjustified intrusion by the public in matters with which does not concern the public.\(^{xiv}\)
  Cybercrime and Privacy – As we know Cybercrime are defined as "Crimes that are made against persons or groups so as to harm the reputation /physical or mental harm. There is the use of advanced telecommunication networks such as Internet (Rooms for chat, emails) and mobile phones (SMS/MMS)”. These are detrimental to the nation. These are in the forefront through copyright infringement, pornography and secret information being lost or interrupted, lawfully or unlawfully.

7.1 **Human Rights and Right to Privacy**

There is global respect to ‘Privacy’ as a right of human beings and is laid down as ‘Privacy’ which is a vital human right known globally by all treaties and envisaged under the UNDHR, the International Covenant on Civil and Political. Privacy reinforces dignity and other freedom of association and speech. In India and US these rights are recognized through various legal provisions.

There are a number of rights like life, education, speech and expression rights.\(^{xv}\)

Privacy has roots deep in history. Ancient Text like the Bible\(^{xvi}\), the Hebrew culture, Classical Greece and ancient China envisage privacy rights. These were the privacy right. Today’s’ age
interprets such rights as management of personal data. A line has to be drawn as to how far one can intrude into personal affairs of individuals. xvii
There are many reasons for adopting comprehensive laws for privacy and protection of data, so as to promote e-commerce. This is in order to facilitate and protect electronic commerce by having uniform rules.

The youth of protesters in Arabia used social media in 2011, to protests for democracy and to discuss political topics globally and mass communication in the country. Through this social media they were able to share their views and experiences globally, so as to get international public opinion for international harmony.

In a global attempt the E.U. decided to regulate the information by preventing business interference on individual’s privacy. The member nations agreed to block such thereby protecting “privacy”. xviii

- **Challenges faced**
  1. Profiling for public and private purposes – Where surveillance or “watching over” the personal behavior of individuals. These are undertaken by different equipment’s like Closed Circuit televisions (CCTV) or wire tapings, other sensing devices, body scans and other devices.
  2. Geo-location,
  3. Cloud computing,
  4. Data loss, mobile Internet,
  5. Privacy policies of social networks,
  6. Trans-border data flows. xix

The IT Act 2008 has included the offence of violation of privacy. Whosoever violates the piracy right, is punished with custody for three years or fine of 2, 00,000 rupees. xx A number of Apex Court cases and High court cases in India have shown the safe guard to Privacy as a crux of Fundamental Right.
In the case of *Jackuline Mary v The Superintendent of Police, Karurand Ors.* the Calcutta High Court and the Cybercrime Bureau took action on the ground that the action done was a violation of her privacy.

In *Kamlesh Vaswani Petitioner v Union Of India &Ors* the writ petition filed in Apex Court of India under Article 32 of the Constitution of India in public interest challenging the Sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the I.T. Act of 2000 as amended from time to time till amendment, as ultra-vires of the Constitution of India, and recognize the harmful effects of Pornography. It was held by the honorable judge that it is deemed proper to quash the charge under Section 292 of IPC against the present petitioners/applicant. (The matter is under consideration).

- **Provisions under the Information Technology Act 2000:**

  **Sec.66E. Punishment for violation of privacy.**-
  Where any person does acts to show in the form of picture any of their private areas and transmits such and violates the privacy of individual, is punishable with custody shall for three years or fine.

  Here the word transmit is the e-transfer of such photographs or images for public viewing. The word capture may be any video or film. Private area are any private parts of human body.

  **Section 67 - Sentence for printing or conveying indecent material in electronic form.** – Any person involved in such activity will be punished with custody for three years and fine of 5,00,000 rupees.

  **Section 67-A - Sentence for publication or conveying of material containing sexually in electronic form.** – Any person who transfers sexually material will be punished with custody for a term of five years and fine to ten lakh rupees.

  **Section 67 – C Protection and retaining of information of intermediaries** -

  1. The intermediary shall reserve and hold any such information as
  2. Any intermediary who deliberately or purposefully breaks the rules shall in custody for 3 years and fine.

  There is an ambiguity as to if the material is published from a server outside India, then the jurisdiction issue still exists. The researcher further states that there is no mechanism in the Act, which blocks sites immediately as soon as a complaint is made, only according to permission of
central government with respect to national security. Till then the offensive or prohibited material continues to be uploaded on the internet of private individuals.

- **The Evolution of Data Protection**

  One of the dimensions is the privacy of personal data which is also known as data privacy or information privacy. The main aim is that data about one should not be automatically be available to other persons and establishments and the other should be able to exercise control over its use. A person can significantly control the use of its own personal data.

  There are certain OECD Guidelines i.e. Guidelines - Protection of Privacy and Trans border Flow - Personal Information. The aim was to harmonies national privacy legislations. They are:

  1. The Principle as to Limitation - Limits to be imposed on the collection of information as they have to be got from legal means.
  2. The Data Quality Principle – They must be relevant for which they are used.
  3. The Principle on Specification - The DATA collected should have a purpose and such to be specified.
  4. The Limitation Principle - There must not be any misuse of such data unless for which they are collected.
  5. The Security Safeguard Principle - This data must be protected against risk.
  6. The Openness Principle – The principles and policies must be open and frank.
  7. Individual Participation Principle – From where such data has been collected.
  8. The Accountability Principle – The person collecting the data should be responsible and must take measures for its security.

  The right to privacy and the internet increased during the year 1960 - 1970 with the beginning of this information technology (IT). The beginning of the new tool like computer to store data it demanded the government to have specific rules. These could handle personal data and maintain secrecy. The origin of the first laws for data protection was in the Land of Hesse in Germany in 1970. Soon corresponding laws were laid down in Sweden (1973), the United States (1974), and France (1978).
Global development of two crucial international instruments-

The two main important international conventions passed to govern mechanical processing data were:

1. The Council of Europe's, (C.O.E), in the year 1981 – this was to protect the Automatic Processing of Private Data (xxiv)

2. The Organization for Economic Cooperation and Development's Guidelines, (O.C.E.D) – set up to maintain Privacy and cross border flow of data (xxv)

They communicate rules specific for electronic data. These two documents form the basis laws for Protection of the Data, India being one of them. These rules govern collection and storage of data. The term data protection varies in declarations and laws to the extent of only a degree. But it revolves around personal information like:

- Lawful obtainment of information;
- Such are used for a specified purpose;
- Relevant to purpose;
- Accurate; and
- Should be destroyed after it serves the purpose.

These two Conventions form the jurisprudence for the adoption of many laws around the world. Many as to 20 countries have adopted the convention of Europe and nearly 6 have yet to adopt it. The guidelines of OECD have been used in domestic legislation.


These two directives protect from abuses of their data. They set a model of privacy with a series of rights. The Directive on Data Protection, harmonizes law throughout the European Union. (xxvi) Each state of the Union should pass complementary legislation Sensitive personal data is given top priority. The European Directive for Telecommunications (xxvii) lays protections which cover all form of communication including televisions, mobile and computers.
A number of principles of protection of data are supported by the Directives, so as to enable the state to know:

i. where the documents came from
ii. erroneous data corrected
iii. the remedy in the event of illegal processing
iv. The right to deny consent to use data.

The Directive levies a duty on member States to safeguarding individual information of citizens of Europe, when exported to countries. xxviii

- **Global issues and problems encountered as to Right to privacy** -
  There are gaps in the laws which are not in pace with technology. Violations of laws exist with respect to electronic investigation of communications.
  In the annual review of rights of human, the U.S. State Department's, observed that maximum of 90 out of 100 countries engage in unlawfully watching the communications of political opponents xxix. In a U.S case *Katz v United States* xxx the U.S Apex Court upheld that wherever a man may be, he is entitled to know that he will not be searched and seized. In 1970 a range of Acts were passed to control breach of online privacy and some of them were Fair Credit Reporting Act, 1970, Family Education Rights and Privacy Act, 1974, The electronic Communication Privacy Act, 1986, Video Privacy Protection Act, 1988.

- **Global Instance**
  An opinion poll was held, wherein concern over privacy violations was the key issue. The population all over the world expressed concerns about violation on privacy. Thereby making nations incorporate laws to protect the privacy of their citizens. xxxi It is seen in America that television took thirty-five years to reach thirty percent of households whereas on comparison, the Internet’s took only eight years after its launch. It spread like wild fire among people globally. xxxii
Some of the Interruptions in instruments like computers, mobile

- Retrieving
- Copying/extraction of data or extracts any data
- Deploying computer virus
- Causing damage either to the computer resource or data residing on it
- Disruption
- Rejection of access
- Allowing unauthorized person to access
- Transferring services to the account of another person, by the person who has asked for it.
- Stealing source code with an intention to destroy xxxiii

In India the above acts attracts civil remedy through damages or compensation and anyone who fraudulently does so will be liable to custody of 3 years or fine.

There are many incidents which show that the Information Technology Act has protected the right to privacy of citizens. In a case namely Sekar v The Principal General Manager (Telecom) (B.S.N.L.) xxxiv an I.T professional was convicted for hacking government BSNL sites. The Chennai High Court sentenced him to R.I of 1 year and fine of Rupees 5000 under u/s 420 I.P.C and u/s 66 of I.T. Act 2008. On investigation it was found out that the logging into the sites as if as he was an unapproved genuine user and also made alterations in the database. There was unauthorized use of the broadband Internet. The subscribers suffered loss Rs. 38,248.xxxv This case shows that the I.T. Act protects the right to privacy.

In Rajeev Sawhney vs. Unknown xxxvi the facts of the case was the complainant's company executed share purchase agreement with respect to petitioner's company. Strained relationship arose between both sides. This culminated in a business dispute leading to a money dispute. A shareholder obtained a copy of R.B.I's report concerning certain alleged financial irregularity committed by the defacto complainant and the report was doctored, Interpolated, fabricated and uploaded in a website so as to bring down the name and fame of the defacto complainant and to show a bad picture about the defacto complainant in the financial world.
The important fact is that the Counsel appearing contended that once a cognizable offence is registered, it is not that invariably in all cases police should arrest the accused. Indiscriminate arresting of persons simply because they were involved in a criminal case has been decried by the Apex Court.

The trend of the judiciary from *Joginder Kumar vs. State of U.P. And Others* is to safeguard the human rights of the individual and prevent their humiliation by unnecessarily arresting them. The current trend of the law is that when an offence is punishable up to seven years, every effort should be taken and observed by the Investigation Officer to avoid arrest and give fullest opportunity. Later the case was investigated by Cybercrime Cell. Subsequently, the Cybercrime Cell also has been involved due to material being uploaded.

The above mention examples impose a liability on the police officer to not arrest arbitrarily and to give a chance or opportunity to be heard following the principles of natural justice. But it is very well observed that there exists easy access to the internet by the end users and tarring the reputation of individuals is easy. A check must be made to upload any kind of information on the website.

In another case *Dr. L. Prakash v State Rep*, a petition filed by the accused seeking to quash the criminal proceedings through the Fast Track Court, Chennai. The offences were punishable u/S 67 of the I.T. Act, 2000; Sec.4 and section 6, of the Act of 1986, Indecent Representation of Women (Prohibition) and various other Act namely Section 5 and 6 of Immoral Traffic (Prevention) Act. The said case tangled abuse of men / women wherein, Dr. L. Prakash for photographing pornographic photos and videos, showing acts of sexuality. Later he sold selling such videos to foreign websites. The Fast Track Court, Chennai, being a "Mahila Courts" was set up exclusively to solve offences against women and for speedy trial of cases, against women. The accused was convicted and it went into appeal to the Apex Court where the petition was dismissed.
In another case *SMC Pneumatics (India) Pvt Ltd v Jogesh Kwatra*\(^x\)\(^i\), the accused had defamed the reputation of the complainant through emails and the Delhi High court passed an ex-parte ad interim injunction. The attempt was made to defame the reputation of the company through the use of internet and such was done at a global level. These emails were vulgar, abusive, humiliating and defamatory in nature.

In another case namely, *Mrs. Seema Puranik vs. Bank of Maharashtra* on 9 November, 2011.\(^x\)\(^ii\) The Appellant's bank account has been defrauded of Rs.17000/- by a phishing fraud. In query 1 to 4 the Appellant had sought information about an account to which her money had been diverted. Here the information was directed to be disclosed and such was in the interest of the public at large.

The researcher observes here that if information is to be disclosed at large it is in the interest of the public and does not amount in the violation of right to privacy.

In India the 52\(^{nd}\) Report on Cybercrime, Security and Privacy right, highlights the need for improvement in India’s cyber security outline and the need for privacy law to be finalized and made into a law. The Report consists of questions on the state of cyber security, Cybercrime, and privacy posed by the Standing Committee and briefings and evidence provided by the Electronics and Information Technology Department, (DEITY). The Report concludes with recommendations from the Standing Committee on the way forward. The Personnel and Training Department, (DOPT) develops privacy legislation that will address the general concerns of privacy in India which will be sufficient to tackle cyber issues and security in India.

When the committee was asked with respect to foreign server in India DEIT stated that by hosting these foreign servers in India it will be a solution to protecting the security and privacy of Indian data. The Standing Committee supported this stand.

It further recommended entering into Memorandum of Understanding with other countries so as to obtain international cooperation. Presently there are a number of MOUs with the US, Japan, South Korea, Mauritius, Kazakhstan, Finland, and the Canada Electronics and ICT sector. DEIT is also seeking Memorandum of Understanding with Malaysia, Israel, Egypt, Canada, and Brazil. The Standing Committee supported India entering into Memorandum of Understanding for purposes of international cooperation, and encouraged DEIT to continue entering into
Memorandum of Understanding to mitigate jurisdictional complications when seeking to address issues related to cyber security.

The Centre for Internet and Society has ensured that the process is in line with human rights, and also to ensure that all mutual agreements MOU’s/or Legal Assistance Agreements:

- Uphold the principle of double criminality
- Apply the highest level of guard for individuals in the case where the laws of more than one state could apply to investigation of communications
- Are not used by any party involved to evade national legal limits on communications surveillance.
- Are clearly documented and publicly available
- Contain provisions guaranteeing procedural fairness.

The Centre for Internet and Society has welcomed *the Fifty Second Reports on Cybercrime, Cyber Security, and the Privacy* right and echoes the Standing Committees recommendation and emphasis on the need for a comprehensive privacy legislation to be passed in India.

**The cybercrime**

1. **Cyber Pornography**- In the case of *R v Curl* it was laid down that the publication of obscene matter is a Common Law misdemeanor under the English Law. It was further stated that the test for obscenity varies from place to place. The basic test is that whether the matter in consideration may corrupt the minds of the readers that are open to such immoral influences. The same test is incorporated in Section 292 of Indian Penal Code. In an American case *Miller v California* a different test called the ‘C.S’ i.e Company Standard was laid down. It takes into account an average person on whom contemporary community standards are applied. Compared to India where the test applied is “Target standard” where people are likely to read, or hear.

   In a leading case of the Apex Court, *Ranjit D. Udeshi v State of Maharashtra* it is observed that in America the onus lies on the prosecution to prove that the accused had knowledge of the obscene material found.
Protection of Online Privacy of Children’s Data

As computers and the Internet are a part of day to day activities then children are exposed to crimes such as porn sites, stalking, where such material are used for private gains. Section 67B of the IT Act (2008) protects children from violation of their privacy in the form of penalty for criminals.

It penalizes anyone engaged in child pornography and be punished with custody upto five years and fine of 10,00,000 rupees.

It punishes the virtual enticement of children into sexually acts thereby limiting children from sexual predators. If the act is good for public viewing then such may be exempted. So also for religious purpose" is also exempt.

The new Draft xlviii put a liability on the ‘intermediaries’ xlix to inform the users not to stock, inform, convey and store any information that may harms minors in any way. ‘Intermediary’ u/s 2(w) of the Act is any person who obtains supplies, conveys record, or provides service on any form of communication using the web. Every intermediary has to take action quickly so as to remove access to such information that may infringe any activity. The duty of the middle man is to inform the police and preserve the records for a period of 90 days.

This bestows duty upon the intermediary to safe guard the interests of children.

There is a need to have internet censorship which may be carried out by the government or private individuals to avoid unrest and communal violence in a secular state like India. The ISP’s may obtain formal and informal requests to remove any publishing or content on the web. There are certain technical censorship where the (IP) or the Internet Protocol may be blocked or (DNS) Domain Name System may be filtered or redirected, packet filtering, Portal Censorship.

Internet relay chat crime – pedophiles’- crime when pedophiles in chat rooms allure small children.1

Global Challenges faced by nations on privacy

Privacy is an important field in the internet. Most of the companies collect greater amount of data from online users. The government seeks access and surveillance capabilities, it is the need for India to put strict security on privacy. There are principles put forth by the government on Privacy and a draft privacy bill is made yet lacks sanction.li Some of them are:-
a. biometric data
b. sharing of data across databases
c. whether individuals can transmit images of their own “private areas” across the internet.

- **Whether Internet Access should be a Fundamental Right**

  This issue was raised in Egypt’s shutdown in January 2011. The debate was whether the access to the internet is a fundamental human right or not? The same discussion was raised by Frank LaRue, the UN Special Rapporteur. To identify the internet as a basic means, through which individuals can express the basic fundamental right to freedom of speech and expression. The question arises whether the internet should be a protected right. lii

  This Article along with the above mentioned provisions of the Information Technology Act gives utmost power to the law enforcement body to arrest any accused without any arrest warrant as it is in the interest of Security of the Nation and prevention of internal Strife. The internet blackout in Egypt is regarded as foreseer of Internet access as a fundamental right.

  As per the BBC pollliii four out of five adults across 26 countries, regard this issue that was raised in the US Helsinki Commissionliv.
In the above poll it was seen that the access to internet is a right for the people. Four / five people globally believe that it is a fundamental right to access the internet – opinion poll - BBC Service.

Does it place unreasonable restrictions on online free speech as opposed to free speech in the real world? The question arises whether free speech is applicable only on the ground and has more restriction in air? The intensity and the importance of such free speech should be judged by the law enforcement body before banning and arresting any person. In a democratic country like India a clear line of demarcation must be drawn between “providing opinions” and “Defamation / hurting sentimental” values of people. Whether any issue is “right or wrong” is an opinion of the public and should not be mixed with reasonable restrictions under Article 19 of the constitution.

Whether section 69A of the amended Information Technology Act, 2000 and rules made there under, viz. the Information Technology rules, 2009 (procedure and safeguards for blocking for access of information by public) are violative of Article 14, 19 and 21? It is not violative of Articles 14, 19, 21 of the constitution of India as it is observed here that the speed with which the crime is committed and transferred is in nano seconds making it necessary for the police to act swiftly.

Sec.80 of the amended I.T. Act of 2000 is violative of Art. 14, 19, 21of the Indian constitution. This section gives unchecked powers to a police officer, to arrest without warrant, anyone, found in any public place. This section makes it legally liable for the people who have “liked” the comment equally liable in crime. The point of dispute in this section is only to the extent of safeguard of innocent people who are broiled into the crime. Redressal machinery is required to be formed to cater to innocent people. Once the free speech enters the virtual boundaries of India, there is a need to curtail these as most of the people are internet savvy and sentimental values could be affected in a country like India being a Secular state and where different religion lives under one roof. It is the need of the police to be faster in the virtual world to foster law and order with the changing in definition of crime.

- Adoption of New privacy of Regulations by India
In the year 2011, 11 April, India undertook the new regulations for privacy. It was known as I.T. Rules of Reasonable Security practices and Procedures. They envisage obligations on the body corporate that “receives and deals with personal information. This is achieved by the company providing privacy policies. They introduce privacy guidelines.\textsuperscript{i}\textsuperscript{vi}

The Key Guidelines are in the nature of:-

1. **Privacy Policies** – The body corporate to set up privacy policies explaining how data is collected and used and provide for security procedures.

2. **Personal Data (Sensitivity)** – Data protection law is defined by The European Union those that include physical, mental, medical and sexual records. This also includes biometric data along with passwords. The financial information is also included as personal sensitive data.

3. **Restrictions on Data Collection and Processing**– Every individual must know from where data is collected. They must be aware as to the purpose of their data being collected. All the information collected also possesses restrictions. The use is only for why the information is collected.

4. **Additional Restrictions**– The prior consent in written of an individual is necessary to process their data. The consent may be by letter, fax or email. This data collected is only used for lawful purposes only and for the corporate activities only or for specific purpose. This information can be retained only for stipulated purpose.

5. **Access and Alteration Right** – Individuals should have the right to evaluation their personal information so as to see that data is authentic and correct.

6. **Disclosure to Third Parties** – Only on consent can the information be disclosed to third party. This does not hold good in case of government or legal bodies.

7. **International Transfers** – Can be done by a body corporate in India or abroad through data protection. This is applicable only if necessary.

8. **Security** – Everybody corporate has to comply with the security procedures. They have to have the necessary infrastructure and procedures and have documentation of these controls. Every organization has to implement the International Standard IS/ISO/IEC 27001 or an approved industry code of practice.\textsuperscript{i}\textsuperscript{vii}

**Secrecy under the Indian I.T Act of 2000 (Privacy)**
The I.T. Act establishes an offence of “Breach of Confidentiality and Privacy”. This section is for those who collect information by use of power under the Act. Punishment is in the form of fine of one lakh rupees or custody for a term to two years.

Global Scenario of Privacy – The Europeans have a much higher standard and barrier to retain privacy whereas in USA, they easily give out the details of their privacy like Credit Card numbers, License numbers etc.

UNESCO aims to initiate a global research

1. to map the existing regulatory framework in countries like U.S., the EU, Asia, Latin America, Arab States and Africa
2. To safeguard Internet privacy
3. To create a global snapshot of trends and developments.
4. There shall be privacy policy recommendations informing member states and international policymakers.

7.2 Cyber Terrorism

Cyber Terrorism and Cyber Warfare are the most destructive form of warfare rendering helpless, the entire world. There is combination of weapons and technology which the terrorists use producing irreversible and most catastrophic results.

The most cited paper on the issue of cyber terrorism is “Testament before the Special Oversight Panel on Terrorism (Denning, 2000)”, in which cyber terrorism is described as the junction of terrorism and cyber space so as to force the government in its political objective. This attack results in violence which may be against persons or property or may incite fear.

The Unites States Department defined terrorism as “Unlawful use, threatening, violence against individuals / property often to achieve political, religious objectives”. Cyber Terrorism has been defined by many organizations in the world namely United States Department of States (DOS), The United States Federal Bureau of Investigation (FBI).

Modalities for Cyber Terrorism:

a. Hacking
India needs tools to counter cyber warfare. In association with NATO the growing cyber threats can be encountered. The major threat to India is from China. New Delhi has been warned from the Organization of National Technical Research (NTRO) that there is a full blown attack by Beijing.\footnote{\textsuperscript{lxiv}}

\begin{itemize}

\item **Cases Depicting Use of Internet as a Tool for Committing Cyber Terrorism**

In the case wherein Indian Parliament was attacked and there was extensive use of internet as cell phones and laptops and IP addresses and SIM cards were confiscated from the accused. This shows that the Internet makes available data which is of high security of a country and everything is accessible on the internet from anywhere in the world.\footnote{\textsuperscript{lxv}}

In another case where online pharmacy website dealing with banned narcotic drugs under sec 79 of IT Act was not granted immunity. The accused was a network provider and used his network for ordering supply of Narcotic Drugs outside India and the Appellate was not entitled bail.\footnote{\textsuperscript{lxvi}}

In **MD.JAMILUDDIN NASIR v State of West Bengal** The accused used a cyber café and internet facility to conduct the crime. They were involved to conduct a shootout at the American Embassy in Calcutta. The death sentence was changed to life imprisonment. This is with respect to cyber terrorism in India.\footnote{\textsuperscript{lxvii}}

Refer case of **People Union for Civil Liberties v. Union of India**, \footnote{\textsuperscript{lxviii}}

In **Md. Ajmal Md. Amir Kasab @Abu ... vs. State Of Maharashtra** the whole of Mumbai city was under terrorist attack. Many people in the process were killed. The Pakistani terrorist Kasab along with his group entered India for creating terrorist attack on India. He had extensively used internet as a weapon for committing the attack. They used Indian Sim cards in the mobiles and
they were instructed to activate it only when they reach Mumbai. During their journey, they were communicating via satellite telephone. This shows the extensive use of internet and related gadgets for the committing cyber terrorism in India.

In the case of *State of Maharashtra v Praful Desai* lxx, the Apex Court held that Sec 273, of Code of Criminal Procedure, 1973 with respect to recording of evidence by video conferencing satisfied the requirement laid under section 273 of CrPc.

In the *Pappu Yadav case* lxxi it was pleaded by the jail authorities to transfer Pappu Yadav out of Bihar jail but at the same time he would lose his right to fair trial. He will not be able to attend the court proceedings. The court relied on the following:

i. Even if he is transferred out of Bihar and not physically present in the court room, the trial can be held with the aid of video conferencing and directed Pappu Yadav from Bihar to Tihar.

ii. The cause list is available on the internet and the proceedings can be got from any part of the country.

iii. The Apex Court has also initialized e-filing as it would save time and energy and money of litigant.

iv. Lead to speedy disposal of cases.

In Telhaka .com case the court admitted video evidence as valid evidence as it is possible to detect the authenticity, breathing and air conditioner noise easily and it is difficult to remove them. Therefore there are effective ways to check the authenticity of evidence with the aid of modern technology lxxii.

Putting records online or on the internet would prevent facing long undertrials or would have been innocent or they have suffered more punishment than expected. This is prevented by keeping records on internet. Due justice can be given to them. There is a need to have a legal Assistance Cell on the internet to solve the problems and to keep a track of these underprivileged victims.

- **Global Scenario of Terrorism**
The U.N Office- Drugs and Crime (UNODC) contributes, globally, in curbing and provides aid to its members. They follow the rule of law and all the standards of rights of Humans.\textsuperscript{lxxiii}. In the United Kingdom, U/S 59 of The Act on Terrorisms, 2000, makes an offence to incite another person to commit terrorism.

In the well-known case of \textit{R v. Tsouli and others}\textsuperscript{lxxiv} where the accused, Younes Tsouli, Waseem Mughal and Tariq al-Daour were guilty to charges under the Act. They instigated murder for terrorist through websites and chat sites. These were used to instigate terrorism.

In the United States, there have been cases which in terrorists have been prosecuted for the words or actions used by terrorists to communicate via the Internet. These include \textit{United States of America v. Emerson Winfield Begolly}. In this case a 22 year old student, Emerson Winfield Begolly, a U.S national, was accused as he uploaded information with respect to to bomb-making and to commit Begolly. He was an activists and took part in jihadist forum called the Ansar al-Mujahideen. His views on terrorism, made others of his religion to take part. He uploaded videos along with instructions for making explosive devices. The targets being holy places like synagogues, train lines, police stations, bridges, towers of cell phone and water plants.

In a period of time he posted several messages for inciting violence. Begolly further posted links “The explosives course”, available for download which contained detailed instructions on setting up a chemistry laboratory for the manufacture of explosives.\textsuperscript{lxxv} These were downloaded by FBI and in the process led to his arrest. The accused was charged with unlawful distribution of such data, weapons which aided in bombing. He was held guilty and awaits sentence.\textsuperscript{lxxvi}

\textbf{Violation of privacy and Punishment}\textsuperscript{lxxvii} Inserted Vide ITA 2008: Any person, who uploads images of a private area of another without consent, will be punished with custody for 3 years / fine - two lakh rupees.

- \textbf{Section 66F- Cyber terrorism - Punishment}\textsuperscript{lxxviii}
Any act against the unity, honesty, safety or sovereignty of India or to strike terror in the people. Such a person who commits or conspires an act of terrorism is punishable with custody for life.

### 7.3 E-Contracts

E-commerce has a wide definition including retailing and wholesale business, online newspapers and other information sources and services, online gambling services, video conferencing offshore and inland banking everything with respect to commerce and trade.

All the machines communicate with each other through this IP address this is given a domain name. There are a number of elements involved i.e. the Network Provider, the Internet Service Provider(ISP) the Users and the Websites followed by the payment providers. These all play very important role e-commerce. It operates based on advertising of both tangible and intangible products. They provide services.

E-contracts are

1. Converging of technologies and
2. Knowledge economy.

E-contracts facilitate the re-engineering of business made by a software system via the internet and signed electronically.

**The type of e-contracts**

a. **Web-wrap agreements** assent is got by “I agree or I accept” button.

b. **Shrink-wrap agreements** are those which a user accepts as soon as a software is loaded. E.g. Nokia pc-suite software.

**Merits of e-contracts:**

- e-contracts reduce costs
- Saves time as it is faster in entering and executing contracts.
- faster customer response
- Improve quality of services and reducing paper work through automation.
• Increases business output by adding speed and efficiency.

Under e-contracts a number of options are made available to the public. The consumers get extraordinary access to a global market via the internet and product ranges.

In electronic contract, the proposal focuses on how risk is in an automated environment. Electronic contracts are in power with hard copy contracts. All electronic contracts are valid contracts and governed by the I.T Act. \(\text{xxxiii}\)

The I.T Act of 2000 is based on the UNCITRAL Model i.e. Commission on International Trade Law by United Nations. The following sections of the IT ACT 2000 to a certain extent govern e-contracts. Yet the skepticism of the contracting parties regarding the legal principles to be applied is not well founded despite the fact that the various Acts do tackle the complicated issues and problems, legally\(\text{xxxv}\). The Information Technology Act is supplemental to the existing provisions of The Indian Contract Act of 1872.

The authenticity of e-contracts is governed by Section 5 of the IT Act 2000\(\text{xxxvi}\). The word 'signature' is construed accordingly for its authentication.

Yet this section is not full proof as it lacks the desired method/tool to prove its authenticity. People are unaware of electronic signature and so may land in trouble. There are no proper standards laid down for encryption as data which flows on the internet may be intercepted at various places. The service providers can collect all the data and then decrypt it then safety can be maintained. This process has to be standardized by certain authority created by the government especially for this purpose also by bringing about uniformity in encryption.

The DoT (Department of Tele-communication) along with Internet Service Providers (ISP Guidelines) has laid down that the individuals and corporate while using the ISP are permitted to 40 – bit key length, the SEBI provide for 64 bit /128 bit encryption, RBI has specified public key infrastructure for the security of internet banking services. They use 128 –bit encryption. Thereby there exist a number of different standards for encryption standards.

There is a liability imposed upon the banks and corporate which hold large public data to maintain secrecy of such information under Sec 43A of I.T. Act, 2000.\(\text{xxxvii}\)
Section 10-A – Validity of e-contracts – They are enforceable they were in electronic form and used for the purpose of communication, acceptance, and revocation.

Section 11- Original originator. He/ She is the original person having authority to any device operating automatically.

Section 12 - Acknowledgement of receipt may be done on any communicating device so as to show that the originator has received it.

Where the creator has not specified that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the creator within the time specified, then, the creator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time and if no acknowledgement is received he may issue a notice to the addressee, treat the electronic record as never been sent.

The above sections govern offer and acceptance and consent. But it does not govern revocation of offer and acceptance.

Sec.13 of the Act states that a creator has no control when the e-record is received by a computer outside his control. The time and place is the time when it enters the designated computer resource.

Section 15 – Secure digital signature - It states that the digital signature to be unique to the subscriber and capable of identification.

The other provisions of The Indian Contract Act are applicable.

**Electronic Evidence**

The Electronic Evidence is permitted in the court of law due to corresponding amendments made to the various Acts namely Indian Evidence Act, u/S 65A and Section 65B of the I.T Act, 2000. Section 65A and section 65B state that the electronic records are permissible in court of law.
Section 67 of the Evidence Act – Proof as to signature and hand written if in the form of Digital Signature.

Section 73 of IT Act 2000 states that publication of others Electronic Signature, Certificate – not permissible and punishable u/s 74.

Section 85A, 85B, 85C of Indian Evidence Act has been amended corresponding to I.T. Act.

Under the Indian Contract Act of 1872, a contract to be valid must have an offer, acceptance and such to be given by the person who makes the offer and the acceptance to be made to the person to whom the offer is made. The contract must have a lawful object, consideration and mutual consent. One of the legal rules as to acceptance is that the acceptance must be given to the person who gives the offer and no one else.

- **Legal Issues in Web Contracts**
  
  There are a number of web contracts created yet there are a number of legal issues surrounding web contracts.

1. The major challenge is if the acceptance is given without the principal’s knowledge, as the computer is used as tool in the formation of contract?

2. Section 13 of the IT Act 2000 is vague as does it mean the computer or the server of the receiver or originator. Time of receipt also vague as does it takes the time of the server or the time of the computer?

3. The next issue is the cancelation of offer as the speed of sending of the offer is fast so the revocation has to be equivalently fast prior to acceptance.

4. The time limit for acceptance if it has exceeded the given time period then does it amount to acceptance on the part of the party? If the agent gives acceptance, does it amount to acceptance on the part of the principal?

5. Can a software tool be a legal person and how the user is bound by its action?

6. What parameters to be followed that the contract in not made under coercion, undue influence?

7. Once the acceptance is given either knowingly or unknowingly, it is difficult to revoke the acceptance or stop the acceptance in the virtual world.

8. Jurisdiction issue – As the Indian Code of Civil Procedure 1908, bases territorial jurisdiction i.e. on the address of the defendant and secondly the cause of action(place) arises.
Yet such aspects cannot be determined in the context of the internet, as does it include the address of residence or office or does it include the server location. The cause of action may be said to arise at a variety of places – where the site is accessed or where its server is located.

9. What is the effect of the loss of the letter of acceptance in internet?

10. How do you know the capacity of the parties to e-contracts as its territory is global?

**Cases in India**

1. **Issue of place in case of e-Contract u/s 13 of the IT Act.**
   The issue of Place in case of Electronic Contract was given the first judicial clarity in the case of P R Transport Agency v. Union of India\(^{xciii}\). In this case, one of the issues before the Allahabad High Court was: “Does the Court have jurisdiction?”
   P R Transport Agency (PRTA) was awarded a tender by BCCL in Jharkhand. The acceptance of the PRTA’s bid was conveyed through an e-mail. The e-mail was received at Chamauli, Uttar Pradesh (U.P.). The respondent contended that since the tender had taken place in Jharkhand, no cause of action arose in Uttar Pradesh. The Court relied on Sec 13(3) as mentioned in earlier pages. Where the e-record is dispatched to the place where the maker has address(business) and received where the addressee (business) and held that when the mail was sent, it was intended for the address from where the Company was working. Since, the office of the Company was in Chamauli and Varanasi, both of which fell within U.P so the High Court had jurisdiction. So, a partial cause of action arose which allows the High Court to exercise its jurisdiction.
   Point of Contention - This leads to confusion as to making known the acceptance to the offeree. It piles up to the time take for forwarding the message to the offeror. Again if acceptance is not forwarded then what will be the remedy available to the other party or the promise?

   The Apex Court in Trimex International FZE Ltd. Dubai v. Vedanta Aluminum Ltd\(^{xciv}\) recognizing the legitimacy of e-transaction- held that mutual contracts through exchange of e-mails exchanges are valid.

**Issues governing E-contracts in India**
The Uber Technologies - U.S Taxi company, violated rules in India, by “bypassing”. The company did not follow a “two-step verification” laid down by the RBI thereby violating the regulations in India.

The Two step verification is a process which had to be followed in case of domestic credit card. The online transactions require a two-step verifications process. The company violated such by routing online payments through an offshore server.

Two step verification – Prevents misuse of credit card. The bank sends a 'One Time Password (OTP)' on his mobile. This completes the transaction. OTP is valid for that one transaction and expires soon after. Every new transaction generates a new OTP on credit card use. The card holder inserts his password known to him. Therefore no one can misuse the credit card online. It is the need of RBI to set up an easy way of verification that would allow small value electronic transactions without a second level of verifications. In India in cases of online payment of money it is important to undergo the two way verification.

Global Cases on e-contracts

*Chwee Kin Keong v Digilandmall.com Pte Ltd* the case is about an issue of one-sided mistake. The case is one of its kind as it talks about web based contract. The defendant selling products (I.T.) over internet in Singapore. The HP laser printer was advertised on the Defendant’s website for $3,854. Due to the mistake on part of one of the employee, the price got altered to $66 on the website, which went noticed. The Appellants seeing this price placed an ordered for 100 printers. The mistaken was seen and rectified by the company. An e-mail was sent immediately as to not complete the order.

The Court held that:-

They were aware about the mistake in the pricing of the product. Due to which the contract was held void under the law.

Three important inferences from the judgment of the Court are drawn:
i. The goods displayed on the e-commerce websites are an invitation, just like any common advertisement displayed on boards/shop. Such is different from offer.

ii. The difference between invitation and offer depends on the language used on the website.

iii. The element of *consensus ad idem* does not hold good.\textsuperscript{xci}

In every contract under The Indian Contract Act of 1872 there is a need of an offer. The question arises in e-contracts, if another finds an offer then its validity is a question with respect to Acceptance? In such a situation it will be governed by subsection 12(2) that only if acknowledgement of the record is made then the e-record is believed to have been sent by the creator else it is deemed not to have been sent. There is a problem in this situation that if both the parties constantly ask for acknowledgement of not only their offer but also of their acceptance and acknowledgement. Then it will lead to a vicious circle of loop.\textsuperscript{c}

Revocation of acceptance – the Contract Act as u/s 5 - an acceptance may be cancelled at any time before the communication is complete and not afterwards. But under the I.T. Act of 2000 - an acceptance is binding on the offeree the moment the receipt enters the system not in his control. So this provision of the I.T Act differs from the Contract Act.

In Germany, email messages, are deemed to be received on reaching the addressee’s computer.\textsuperscript{ci}

- **Guideline by Banks with respect to e-contracts**

  E-banking – It provides banking services through e-delivery. E-banking exists in the form of automatic teller machines (ATMs) and telephone transactions.\textsuperscript{cii} There are a number of ways of transfer of funds using banking services.

  1. **RTGS** – Real Time Gross Settlement – A mechanism of settlement of funds from one bank to another. The minimum transfer is two lakhs rupees and the maximum is any amount. There is inter banking transfers. This system is used extensively among customers and banks.

  2. **ECS** - Electronic Clearing Services – Is used for bulk transfer from one bank to another through clearing houses of Reserve Bank of India.

  3. **NEFT** Credit card and Debit Card – An electronic payment system which uses a secure mode of payment system. No limit as to maximum or minimum amount of transfer. Credit card enables users to avail credit from the banks. Debit card is used to withdraw cash.
4. ATM – Automated Teller Machines – HSBC was the first to introduce this system. Internet banking has changed and is now from click to mortar. ICICI was the first to introduce this system. A study revealed that:-

a. ATM is preferred by 53%. / 6356 Internet user,
b. 35% use online banking channels in India
c. They prefer internet instead of standing in front of cashiers in banks.
d. Allowed all time withdrawal.

There are many reasons as to why people do not use internet.

i. Security concerns - people are not doing financial transactions on the bank Internet sites in India because of reasons as to security.

ii. Face-to-face transactions are preferred

iii. Lack of knowledge about computers

iv. Lack of user friendliness

v. Lack of facility in the current bank

The R.B.I they laid down guidelines as to

1. Technological and security – Wherein the banks to designate a network database administrator. The security policy to be approved by board of directors. To have a proxy type server of firewall. If any security violation such to be reported.

2. Legal Issues - To make enquiry as to reputation and identity of customers. To recognize authentication of digital signatures.

3. Regulatory and Supervisory issues - Only banks having a license and supervised in India will be permitted. There exist many traditional risks as conventional banking facilities are not stopped totally so accounting of transactions and keeping of records both offline and on-line is a difficult task. The personal touch with the banks is lost.

Today a number of bank employees are seen involved in issue of fake credit card by the company. It is seen that a person has a number of duplicate number held on his/her name.
In a historic judgment passed by the Mumbai High court a number of banks have been ordered to pay compensation. They include bank of India - Central Bank, bank of Scotland, National Bank of Punjab, IndusInd Bank, Yes Bank, S.B.I. Other institutions who have been directed to pay are Vodafone and SBI Cards. HDFC have also been charged with fake credit cards transactions.

It is seen by the researcher that new regulations to be drafted for the employees of banks as they will be prevented from entering fraudulent practices. The researcher suggests the following:

1. To take a thumb impression of the employees of banks.
2. To have CCTV surveillance on bank employees.
3. To make the customer and the employee aware of a secret code before verification of customer details.
4. To have a 7 layer verification
   a. One supervisory report by peons of the banks.
   b. Second supervisory report by managers
   c. Third checks by the computer with respect to eye ball verification and thumb impression.
   d. A lock system to be put on telephones and a call register to be maintained with respect to outgoing calls.
   e. Separate cell phones to be provided to bank employees for banking purposes
   f. To fill out a form for exchange of duty in banks with other employees.
   g. To have customer details under the custody of the manager of the banks.

5. The banks to be made liable to pay certain amount of fees for verification of customer details.

There is a need to have effective governance of the banks on the e-transactions and e-banking as it allows for credit card payments. The researcher has given a brief note of what exactly are credit card payments.

**Credit Card Payments**

This mode of payment is made with the plastic card. They are a safe means of carrying money. This mode of payment is often used across boundaries. There are a number of credit cards available by various banks. There is a contract with the issuer of the card to discharge the
balance in his account. The mode of payment allows the owner to obtain credit. Periodic statements are issued every month. Most of the business houses are using the credit card for their transactions as it eases the business gains. Whenever a transaction is conducted, the business house verifies the credit card number with the phone number. This is a method whereby security is maintained. This system is not well proofed as it has the risk of being ‘hacked’.

7.4 Cyber Warfare –

Today this method is adopted almost by nations and big business houses. The act is to sabotage the critical information of the other. There is use of Malware to spy and steal. There are two ways of cyber warfare

- **By Nations who hack into computers of other nations.**
- **By business houses who steal data of other business houses.**

Acts undertaken by nations today are to damage another’s internet or information system. This can be undertaken by any enemy country. Cyber vandalism is ‘cyber hacktivism,’ a term used for hackers who use digital tools, illegally chasing political ends. This practice is adopted by big corporate/business organization. The many ways are:-

First, defenses are weak and second, attacks in cyberspace are much faster, where defenses are under great pressure. Third no geographical barriers as such attacks can come from anywhere lastly, modern society is depended on the internet making it a target-rich environment, giving the defender great strain.

• **Information Warfare**

The IW is a mixture of tools of network and e-weapons against the information systems of opponents’. Anyone with access to such systems irrespective of geographical location can be a great threat to the network.

Acts of Cyber Warfare

2. Malwares
3. Denial of Service Attacks
4. Legal Frameworks to check Cyber Attacks.

The aim is to:
1. To steal and spy on the activities of another country or other business organizations.
2. To cause physical damage.
3. To use components used in chemical plants.
4. Use of hateful code to manipulate the control of pipelines and to cause disorder.
5. To cause blackouts and disruption to water supply of a country.

Under the I.T Act there exist provisions u/s 66, punishes for hacking for a 3 yr. or fine till two lakh rupees.

The websites of Maharashtra Government were hacked. The only solution was to remove the data. In another case Hacker Dr. Neruker case. Where the Cyber Cell Mumbai received unknown telephone at 7:00p.m that their website www.ccicmumbai.com is going to be hacked and it was hacked. The hackers were untraceable but later on, on repeated incidences they were traced. Today they work as official hackers for Mumbai Police Cybercrime Investigation Cell.\textsuperscript{cxi}

Section 66A - Penalize those sending offensive messages causing inconvenience, annoyance to others. The Punishment is for 3 years and fine.

In an incident Miss Malini Murmu\textsuperscript{cxi}\textsuperscript{ii}22 a 1\textsuperscript{st} year student of MB, IIM- B, committed suicide. Her boyfriend disclosed on Facebook “Feeling super cool, deserted my ex-girlfriend. Happy independence Day”. She left a suicide note stating the aforesaid reason for her suicide.

The Act does not define offensive message or messages which are misleading. As in the above case a suicide note was left so one could be convicted else the vagueness still exists. The message could also be sent by a proxy server.

It is seen that most of the spam comes from US.\textsuperscript{cxi}\textsuperscript{ii} The IT Act is silent on Cyber war as it extends to activities abroad but is still ineffective.
In another case cxiv where employees of Indicom were detained for illegal handling of e-records which were programmed into phones that were licensed to Reliance Infocomm. This was invading the secrets of another business organization. The court passed its judgment that such resulted in manipulation and meddling with the source code of computer u/s 65 of the I.T. Act of 2000 and that a computer includes cellphone under the I.T. Act of 2000. The ESN and SID came is defined as “source code of computer” under section 65 of I.T. Act 2000. Every provider of service has to have his own SID code to give customer a specific number to his instrument. cxv

It is seen from last couple of years that government sites and government offices are constantly under threat of cyber war. They have come under repeated attacks. It is seen that India is tapping into a pool of young talent to fortify its anti-cyber war strength. The Indian Response Team of Computer Emergency (CERT-IN), headed by Mr. Gulshan Rai is the national security coordinator of Cyber (NCSC), it coordinates all cyber agencies. There is a need to employ young cyber professionals to overcome such threat. cxvi

In India agencies that are focused on cyber defense are

1. The Organization of National Technical Research under the control of defense - RAW agency of intelligence.
2. National Critical Information Infrastructure Protection Centre – to protect the critical infrastructure such as transport, banking telecom and defense.
3. The Computer emergency team of India, set up in 2004, protects non-critical assets. It is a Nodal Agency to respond to computer security incidents. cxvii

It is seen that in 2003 the government asked the mobile operators to change the SIM as foreign SIM could have worms which could disrupt the Indian cellular networks, mobile system. cxviii

7.5 Cyber Espionage - Threat to India

India’s biggest threat is from China. They have the ability to fight high technological wars. cxix The Chinese are focusing on a “ZERO DAY”. They are buying tool required to create a ZERO DAY. There are websites which list the prominent hackers of China. cxx
The United Kingdom British Airways was hacked leading to freezing of many accounts. This was done by an unknown source. It was an attempt made to steal personal data of frequent fliers. This attempt is similar to that of where the Malaysia Airlines suffered its Hack by “Lizard Squad – Official Cyber Caliphate”.

- **Cyber-Espionage Methodology**
  The Chinese have programmers called ‘black hat’ or ‘hacker forum’. They provide hateful software.
  With the aid of Forensic science it helped to reveal that these penetrators were masking their activities.

- **Chronology of crimes committed by the Chinese targeting Foreign Networks**
  In the year 2009, March, A Canadian team, conducting research, published Ghost Net cyber espionage network. This network attacked 1,300 hosts globally i.e the embassies of German, Pakistan, Portugal and India. The Canada-based Information Warfare Monitor (IWM). This functioned from China’s Hainan Island.
  It is seen that this amount of warfare cannot be proved nor can the country be made liable for their act. In the same case the government denied all the charges of involvement of the state.
  On 9th December, reported on 19th January 2010, the national security advisor of India reported of Hacking. Google had similar attacks. It was in the form of PDF emails. The Chinese were suspected to be the originator. There have been other cases of cyber-attacks in the past, on the sites/computers of external affairs Ministry - (MEA), home affairs ministry - (MHA), and defense ministry - (MOD) by unidentified hackers.

7.6 **SUMMARY AND CONCLUSION**

The researcher suggests that there must be a filtering plant/ Censorship on the use of internet whereby the following will be protected

1. Unknown users will be denied access to target government machines or business organizations.
2. Links to immoral websites should be restricted.
3. Under aged children or adolescent should be protected from inappropriate content.
It is not a question of Freedom of Speech and Expression that is violated but protection of a vulnerable section of the society. Now-a-day’s people are undergoing stress and mental issues due to many reasons, such mentally weak people may be drawn towards downloading sites which may harm them in the long run.

It is learned that China is the most advanced country which blocks sites. They have the most advanced techniques for controlling information which relates to “Democracy” and “Rights of Human”. Iran is also another leading country which uses internet censorship to great extent.

As India being a secular state there is a need for a multi layered communication system. There is a need to protect the freedom of Speech Right, yet, there must exist censorship so as to prevent civilians as being victims of internet.

It is further observed by the researcher, that when the websites are hacked by people from abroad it becomes a difficult task to bring the accused to India and convict him. But if the accused is from India then convicting him becomes an easier task.

The need of the future is to have a bilateral treaty with other nations and in consonance with the United Nations so as to minimize Cyber Espionage and Cyber Warfare.

Further there is a need to have a clear encryption policy in India following uniformity with all the service providers. This policy is based on international minimum subscription level.
Jackson, Robert H., Stein v New York, 346 U.S. 156,184 (1953)


AIR 1991 SC 207.

AIR 1995 SC 495
AIR 1981 SC 760
AIR 2008 AP 98.


Section 66-E, I.T. Act of 2000
W.P. No. 587 of 2014,MANU/TN/0427/2014
MANU/SCOR/37484/2014Writ Petitions Civil Nos. 177/2013 © Manupatra Information Solutions Pvt. Ltd.

The Information Technology (Due Diligence observed by Intermediaries Guidelines) Rules, 2011;

Intermediary Due-Diligence Guidelines, 2011.


“Internet Privacy in India”, The Centre for Internet & Society, (C.I.S)


UNESCO” A Global legal Survey of Internet Privacy”, https://www.google.co.in/?gfe_rd=cr&ei=gqKTVMHnEITV8geOw4GYAw&gws_rd=ss l#q=papers+on+privacy+on+internet. Visited on 15th June, 2014


Sanjay Kumar Kedia v Narcotics Control Bureau and Anr, (2008)2 SCC 294


"Electronic Contracting with Suppliers under German Law" by Dr. Alexander Loos, pg. 5


Ibid 529

The Times of India, Delhi edition, March 08, 2011.

Ibid 400, p 290


Ibid 400, Pg.290.

