CHAPTER II

CYBER CRIME AND ITS CLASSIFICATION

1. Introduction

Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act. Cyber crime is the most prevalent crime playing a devastating role in Modern India. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation it can be said that, Cyber crime includes any illegal activity where computer or internet is either a tool or target or both.

The term cyber crime may be judicially interpreted in some judgments passed by courts in India, however it is not defined in any act or statute passed by the Indian Legislature. Cyber crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark sides too.[1] Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber-defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet.

2. History and Evolution of Cybercrime

During the period of 1950's, it would be an astonished feeling for everyone who uses palmtops and microchips today, to know that the first

[1] Prof. R.K.Chaubey, *"An Introduction to Cyber Crime and Cyber law",* Kamal Law House, 2012

successful computer was built and the size of the computer was so big that it takes the space of entire room and they were too expensive to operate. The functioning of these computer were not understandable to large number of people and only select people with expertise had direct access to such computers, and has the knowledge to operate them. For obvious reasons, the computer technology was extremely expensive and beyond the purchasing capacity of almost the entire population until IBM's came into being wherein it introduced its stand-alone "personal computer" in 1981 and exposing many to the rewards of quick data access and manipulation that, up to that time, had been realized by few. The Personal computers become cheaper and become household item at the start of 21st century in India. The Internet was first started by the US department of defence, after World War II with the idea to have a network which could work in the event of disaster or war and securely transmit information. The First Network was known as ARPANET, with the development of Transmission Control Protocol/Internet Protocol, World Wide Web and Hypertext the internet become rage all over the world. With the growth of Internet the quality and variety of information grew. However at that point nobody anticipated the opportunities' the internet is going to provide the technology savvy criminals.

In India the internet services started by the state-owned Videsh Sanchar Nigam Limited in year 1995 and in 1998 the government has ended the monopoly of VSNL and market is opened to private operators. At that point, the internet users in India are 0.1% of total population, and now India has become the 2nd largest country in terms of internet users after china with 33.22% people using internet.[2]

The process of criminalization of human behaviour judged to be harmful the public is typically one that builds slowly in common law jurisdictions. Momentum gained through problem identification and pressures

[2] https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users (Accessed on 3rd February, 2016)

exerted mg special interest groups can easily span decades before undesirable actions are classified as "crime". In some instances, this process is accelerated through the occurrence of certain "catalyst events" that capture attention of the public and the attention of lawmakers.[3]

The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modem computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime.[4]

In the case of computer crime, legislators grew increasingly attentive is the 1980s as businesses became more dependent upon computerization and as catalyst event cases exposed significant vulnerabilities to computer crime violations. Criminals can now easily encrypt information representing evidence of their criminal acts, store the information and even transmit it with little fear of detection by law enforcement. Due to the extraordinary impact of the Internet, a computer crime scene can now span from the geographical point of the victimization (e.g., the victim's personal computer) to any other point on the planet, further complicating criminal investigative efforts. In effect, computer technology has dramatically altered the criminal justice terrain such that enterprising and opportunistic criminals have consciously turned to the computer to commit their illegal acts in situations in which the computer serves as the instrument of the crime, the means by which the crime

[3] Abraham D. Sofaer, Seymour E, .The Transnational Dimension of Cyber Crime Terrorism, Hoover Institution Press, 2001.
[4] http://cybercrime.planetindia.net/intro.htm (Accessed on 4th February, 2016)

is committed, as well as in cases in which the victim's computer, or computer system, is the target, or objective, of the act. And, as stated above, the presence of new computer technology aids cyber criminals in situations in which the computer's role is incidental to the crime; situations in which the computer is used to house and protect information that is evidence tying the offender to criminal acts. A commonality among these types of crimes is that the offender, to a great degree, depends upon the lack of technological skills of law enforcement to successfully commit the offenses and escape undetected. Based upon what empirical evidence has been available on self-assessed skills of investigators in this area, computer criminals would have good reason to feel some confidence in their chances to evade detection of their crimes.[5]

As we advance towards the 21st century, it van be observed that the technological innovations have laid the way for the entire population using computer technology today, to experience new and wonderful conveniences in their daily life ranging from how to educated, shop, entertain, to availing the understanding of the business strategies and work flow. Our day to-day lives have been forever changed thanks to rapid advances made in the field of computer technology. These changes allow us to communicate over great distances in an instant and permit us, almost effortlessly, to gather and organize large amounts of information, tasks that could, otherwise, prove unwieldy and expensive. The technological treasures that have improved the quality of our lives, however, can reasonably be viewed as a doubled-edged sword. While computer technology has opened doors to enhanced conveniences for many, this same technology has also opened new doors for criminals.

3. Definition of Cyber Crime

[5] Stambaugh, H., et. al, Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Report, Washington, Dc: U.S. Department of Justice, March 2001.Available at : https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf (Accessed at 04th February, 2016)

The Indian Legislature doesn't provide the exact definition of Cyber crime in any statute, even the Information Technology Act, 2000; which deals with cyber crime doesn't defined the term of cyber crime. However in general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers.

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "*Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"*[6]

We do not have any precise definition of cyber crime; however following is the general definitions of term cyber crime:

The oxford Dictionary defined the term cyber crime as *"Criminal activities carried out by means of computers or the Internet."*[7]

"Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"[8]

"Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them"[9]

Professor S.T. Viswanathan has given three definitions in his book *The Indian Cyber Laws with Cyber Glossary* is as follows -

1 Any illegal action in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,

---

[6] http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf (Accessed on 4th January, 2016)
[7] http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 4th January, 2016)
[8] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 4th January, 2016)
[9] http://cybercrime.org.za/definition (Accessed on 4th January, 2016)

2 Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

3 Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.[10]

4. Nature and Scope of Cyber Crime

Crime is a socially correlated phenomenon. No matter how much we try, we cannot experience a society without cybercrime. In actual sense, when we are not yet able to control the crime rate to the desirable minimum in the real world, how would it be possible to curb the same in the virtual world, as the same is comparatively more unreal, everlasting and legally less controllable. However with the time, nature and scope and definition of crime changes in a given society. Crimeless society is a myth and crime cannot be segregated from a society. Thus the nature of the crime depends upon the nature of a society.

Complexity of the society determines the complexity of the crime that evolves' around it. To understand the crime in a society, it is essential and crucial to verify all the factors which influence and contribute to the crime. The socio- economic and political structure of the society needs to understand the crime and the recourse that may curb the same. The preventive and corrective measures adopted by the machinery to control the crime and delinquent behaviour in the society are also taken into consideration while studying the nature and scope of a crime.

The advancement of the technology has produced new socio-economic and political problem in the society and instead of helping the state in controlling the problem it has created new complex situation which is difficult to understand and even more difficult to apply current law to face the

[10] S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*, 2001, p. 81.

situation. The state machinery is not equipped with enough sources and knowledge to handle the modern crime.

Computers have transformed the modern society beyond expectations in last three to four decades. It has made life not only convenient but has also immensely helped different sections of the world come closer socially, economically and culturally. The Computer technology has made it possible to have access to all corners of the world while sitting in a room. Modern technology has put an end to the barriers of time and space. However, unlikely with the remarkable merits of having computers today, due to this the jurisdictional issue has been created in legal system.

Jurisdiction is one aspect which is very difficult to determine in transnational transaction over the internet. There was unmanageable ambiguity when courts were subjected to questions pertaining to jurisdiction law and were unable to decide the proper forum to entertain cases involving cyber crime as the cyberspace or virtual world is borderless if we compare it with physical world and that is why it is very difficult to control cybercrime. Through the local machinery we are not able to tackle the problem related with cyber crime because our machinery is not compatible to deal with transnational crimes. The law applicable to the territory is not advanced enough to regulate the cyber crime as their nature is far different from the existing crime.

Thus, the global dimension of cyber crime is made it difficult to handle and dealt with. The evolution of internet technology has given us so many advantages to deal with future problems and grow with rapid rate but also it has provided the scope for criminals to commit their crime with least chance of detection. The cyberspace has proved a boon to the deviant behaviour in the society. The concept of cyber crime has gained speed and we are facing great threat of its impact on world society. The human society is become vulnerable to cyber crime due to more and more dependence on technology.

Cyber crime becomes a global phenomenon and hence the nationwide generalization of crime cannot workable in present scenario. Our understanding and regulation of cyber crime cannot be national but has to be international. We have to enact new laws and prepare preventive and defensive mechanism globally, only then we can able to protect our society from this evil called 'Cyber Crime'.

Therefore, the threat of cyber terrorism throws serious challenge to world and its agencies. The terrorist organizations using technology to spread hatred among people and using it to recruit militants and train them using teaching tools. They are also launching websites which show them how to use weapons make bombs etc.

4.1 Doctrine of Mens Rea & Actus Reus in Cyber Crime

As far as Traditional Crime is concerned *Mens Rea* and *Actus Reus* are the two most important elements to crime. Actus Reus means "*Such result of human conduct as the law seeks to prevent"*[11]. There must be commission or omission to constitute a crime. As far as mens rea is concerned, it means "*A guilty state of mind"*[12]. The mental element forms the other important ingredient of crime. The act remains the same while the state of mind makes the act *'reus'* and hence an offence. Almost all the crime requires proof of mental element of some sort.[13] As far cyber crime goes it is very difficult to determine the mens rea in cybercrimes.

In Cyber crimes, one should see what the state of mind of hacker was and that the hacker knew that the access was unauthorised. Thus, a "Particular Computer" needs not to be intended by the hacker, it is enough if the unauthorised access was to "any computer". Awareness on the part of the hacker becomes easier to prove where he is an outsider and has no authority to

---

[11] J.W.C. Turner, *Kenney's Outlines of criminal law* (19th Edition University Press, Cambridge 1966) 17. also at Talat Fatima, *Cyber Crime* (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

[12] R.C. Nigam, "Law of Crimes in India", *Principals of criminal Law*, Vol 1, (Asia Publishing House, 1965) 6.

[13] Talat Fatima, *Cyber Crime* (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

access. But where hacker is already has limited authority as ion the case of the employee of a company, it becomes difficult establish that he exceeded his limits and was even aware of the fact that he is exceeding it.

Actus Reus in cybercrimes has become a challenge as the entire act is committed in intangible surroundings. The perpetrator may leave some footmarks in the machine itself though it becomes a herculean task for the law enforcement machinery to prove it in the courts, as it is required to be in physical form or atleast in such a form where it becomes admissible in evidence.[14]

5. Characteristics of Cyber Crime

The Concept of cyber crime is very different from the traditional crime. Also due to the growth of Internet Technology, this crime has gained serious and unfettered attention as compared to the traditional crime. So it is necessary to examine the peculiar characteristics of cyber crime.

1***. People with specialized knowledge*** – Cyber crimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in internet and computers and internet to commit such a crime. The people who have committed cyber crime are well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to tackle the perpetrators of cyber crime.

2. Geographical challenges **–** In cyberspace the geographical boundaries reduced to zero. A cyber criminal in no time sitting in any part of the world commit crime in other corner of world. For example a hacker sitting in India hack in the system placed in United States.

3. Virtual World **–**The act of cyber crime takes place in the cyber space and the criminal who is committing this act is physically outside the cyber space. Every activity of the criminal while committing that crime is done over the virtual world.

---

[14] *Ibid*

4. Collection of Evidence - It is very difficult to collect evidence of cyber crime and prove them in court of law due to the nature of cyber crime. The criminal in cyber crime invoke jurisdiction of several countries while committing the cyber crime and at the same time he is sitting some place safe where he is not traceable.

5. ***Magnitude of crime unimaginable-*** The cyber crime has the potential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc has wide reach and it can destroy the websites, steal data of the companies in no time.

6. ***Classification of Cyber Crime***

The researcher in this chapter examines the acts wherein computer or technology is tool for an unlawful act. The kind of activities usually involves a modification of conventional crime by using informational technology. Here is the list of prevalent cyber crimes, some of them widely spread and some are not prevalent on larger scale. The cyber crimes are discussed below-

6.1 Cyber Pornography

The word 'Pornography' derived from Greek words '*Porne*' and '*Graphein*' means writing about prostitutes, or referred to any work of art or literature dealing with sex and sexual themes. Defining the term pornography is very difficult and it does not have any specific definition in the eyes of law as every country has their own customs and tradition. The act of pornography in some countries is legal but in some it is illegal and punishable.

Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.[15] Pornography has no legal or consistent definition. The definition of

[15] http://blog.ipleaders.in/cyber-pornography-law-in-india-the-grey-law-decoded/ (Accessed on 5th February, 2016)

pornography depends how the society, norms and their values are reacting to the pornographic content.

The reason why we do not have a clear definition as far as pornography is concerned is that we do not have uniform standard culture and ethics in the world nor do we have uniform laws which defines the pornography. The concept of obscenity and pornography varies from country to country and time to time. The terms obscenity and pornography are different but related to each other. The same material which was banned in some countries may be allowed in some. The Indian law doesn't define the term pornography and not deal with this term.

In the modern world sex sells and sells extremely well, and the fact is that present pornography industry is larger than any other company or combination of companies in the world. The advent of internet in the world has started the new chapter in the porn industry. The porn industry find perfect place in internet to spread pornographic material all over the world. According to the internet filter review report of 2010, there are 4.2 million websites offering porn content to the world. 68 million daily search engine requests are made and 72 million worldwide user visit adult sites per month. 42.7 percent of total users who use internet watch pornographic material over the internet.[16]

In the initial years or we can say before internet available to the public, DVD's and Videotapes are the popular medium of distributing pornography. But after that internet is available to general public and it becomes the most popular medium to make pornography available to user in the comfort of their homes. An individual who due to the peer pressure or shame doesn't have access to the pornographic material, nowadays easily watch picture or video on the internet. The rise of pornography websites offering photos, video clips and streaming media including live web cam access allowed greater access of

[16] http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html (Accessed on 6th February, 2016)

pornography. Information technology has made it easier to create and distribute pornographic materials through the internet; such as material can be transmitted all over the world in a matter of seconds, the geographical restrictions which prevented to a certain extent, foreign publication to enter local territories have disappeared.[17]

6.1.1 Test of Obscenity and Pornography

To understand the gravity and effect of pornography and obscenity on society, we need to understand these terms in their widest possible amplitude. The Word Pornography has not been defined legally in any part of the world. The basic reason behind this is very simple; neither we do have any uniform standard of moral cultural, values and ethics and nor we have any uniform standard of law.

The term obscene means relating to materials that can be regulated or criminalized because their depiction of nudity, sex, or excretion is patently offensive and without artistic or scientific value.[18]

The test of obscenity was first laid down in the case of *Regina V. Hicklin*[19] as the tendency "to deprave and corrupt those whose minds are open to such influences and into whose hands a publication of this sort may fall", and it was understood that this test would apply only to the isolated passage of the work.

In *Miller v. California*[20], the Supreme Court of United States in landmark judgment gave the basic guidelines and three point tests to determine obscenity in the work i.e.

---

[17] Gorman, L. and Maclean, D. Media and Society in Twentieth Century, Blackwell publishing, 2003.
[18] http://www.thefreedictionary.com/obscene (Accessed on 7th February, 2016)
[19] (1868) 3 QB 360.
[20] 413 US 15(1973)

1. That the average person, applying contemporary "community standards", would find that the work, taken as a whole, appeals to the prurient interest.

2. That the work depicts or describes, in an offensive way, sexual conduct or excretory functions, as specifically defined by applicable state law or applicable law.

3. Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Before the *miller's* (supra) case, in *Roth v. United States*[21] The Supreme Court of United States in landmark case held that "*obscene material was not protected by the First Amendment and could be regulated by the States rather than by a singular, Federal standard and also a new judicial standard for defining obscenity that invoked the average person's application of contemporary community standards to judge whether or not the dominant theme of the material taken as a whole appeals to prurient interest*." The Supreme further held that "*to decide obscenity derived we need to consider the following five-part structure:*

(1) The perspective of evaluation was that of an ordinary, reasonable person.

(2) Community standards of acceptability were to be used to measure obscenity.

(3) Obscenity law will only apply to the works whose theme is in question.

(4) A work, in order to be evaluated for obscenity, had to be taken in its entirety.

(5) An obscene work was one that aimed to excited individuals' prurient interest."

[21] 354 US 476 (1957)

However, in India miller test was not adopted by the Supreme Court, instead it has adopted the *Hicklin's Test* in leading case of *Ranjeet D. Udeshi v. State of Maharashtra*[22]; the Supreme Court has decided many issues pertaining to the obscenity. The apex court doesn't consider obscenity a vague concept but a word which is well-understood even if persons differ in their attitude to what is obscene and what is not. The apex court has stated that "In judging a work, stress should not be laid upon a word here and a word there, or a passage here and a passage there. Though the work as a whole must be considered, the obscene matter must be considered by itself and separately to find out whether it is so gross and its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort. In this connection the interests of contemporary society and particularly the influence of the impugned book on it must not be overlooked. Where, obscenity and art are mixed, art must so preponderate as to throw the obscenity into a shadow or the obscenity so trivial and insignificant that it can have no effect and may be overlooked. It is necessary that a balance should be maintained between "freedom of speech and expression" and "public decency or morality"; but when the latter is substantially transgressed the former must give way."

The court however, sounded a note of caution that treating with sex and nudity in art and literature cannot be regarded as evidence of obscenity without something more. In the words of court "It is not necessary that the angels and saints of Michelangelo should be made to wear breeches before they can be viewed. If the rigid test of treating with sex as the minimum ingredient were accepted hardly any writer of fiction today would escape the fate Lawrence had in his days. Half the book-shops would close and the other half would deal in nothing but moral and religious books."

[22] AIR 1965 SC 881

In this case the Supreme Court has decided that Hicklin's test cannot be discarded, and said "It makes the court the judge of obscenity in relation to an impugned book etc. and lays emphasis on the potentiality of the impugned object to deprave and corrupt by immoral influences. It will always remain a question to decide in each case and it does not compel an adverse decision in all cases."

In *Samresh Bose v. Amal Mitra,*[23] the Supreme Court has held that "A vulgar writing is not necessarily obscene. Vulgarity arouses a feeling of disgust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the novels, whereas obscenity has the tendency to deprave and corrupt those whose minds are open to such immoral influences". In this case the court differentiated between vulgarity and obscenity and further held that while judging the question of obscenity "the Judge should ... place himself in the position of a reader of every age group in whose hands the book is likely to fall and should try to appreciate what kind of possible influence the book is likely to have in the minds of the readers".

In India, the Indian Penal Code, 1860[24] deal with the issue of obscenity. However with the evolution of internet technology, obscenity and pornography takes electronic form and it becomes impossible to convict the perpetrator under Indian penal Code, 1860(supra). To deal with this new technology, the government of India has enacted Information Technology Act 2000[25]. Section 67 of Information Technology Act, 2000; deal with obscenity and pornographic content on internet. Section 67 of the IT Act provides:

"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

[23] AIR 1986 SC 967
[24] Act 45 of 1860
[25] Act No 21 of 2000.

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 two 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."[26]

The Section 67 of IT Act 2000 is comparable to Section 292 of Indian Penal Code, 1860. In *Ranjit D. Udeshi v. State of Maharashtra*[27] held that unlike other provision which have words like "knowingly" or "negligently" and thus make *mens rea* a condition precedent to establish the guilt. Section 292 does not make knowledge of obscenity an ingredient of the offence. The prosecution does not prove something which the law does not burden it with. The difficulty of obtaining legal evidence of the offender's knowledge of the obscenity of the book, etc. has made the liability strict. The absence of such knowledge may be taken in mitigation but does not take the case out of the provision. If we apply the *Ranjit D. Udeshi case judgment* (*supra*) to Section 67 of IT Act, 2000, it can be concluded that mere publication and transmission of obscene material is an offence notwithstanding the mental state of offender. However, this cannot be a blanket rule applicable to all and sundry.[28]

6.1.2 Child Pornography a menance in modern world

The children especially adolescents are in modern world want to explore everything on information highway. The children in today's generation have access to internet and computer's at home, the internet and computer are part of their studies. The access to computer and internet makes them vulnerable to the potential danger of internet. The children are sometime

[26] Information Technology Act, 2000, S. 67
[27] AIR 1965 SC 881
[28] Prof. R.K.Chaubey, *"An Introduction to Cyber Crime and Cyber law",* Kamal Law House, 2012, p. 440

curious about sexuality and sexual explicit material. The parents don't have too much control over the children and the children are busy exploring the internet and other medium to fulfill their wishes through the on-line access. Sex–offenders exploit these conditions and fulfil the need of children. The child at this tender age doesn't understand and recognise the potential danger of these contacts. The internet is highly used by the abusers to abuse children sexually worldwide. The children in India become viable victim to the cyber crime, as internet becomes the household item in India. The children are becoming victims to the aggression of pedophiles.

In the physical world parents know the dangers, so they warn their children about the danger and tell me how to avoid or face the problems by facing simple guidelines. But as far as cyber crime or crime related to internet is concerned the parents themselves doesn't know about the problems or danger posed by various service offered over the internet. The pedophiles take advantage of these things and lure children and win their confidence and then exploit them because parents or teachers doesn't tell them about what is wrong or right over the internet.

The Information Technology Act, 2000 doesn't contain any specific provision related to child pornography but later a new section 67B[29] has been inserted in Information Technology Amendment Act 2008[30]. This section provides that: "*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*

[29] Information Technology Act, 2000, S. 67B
[30] Information Technology Amendment Act 2008, Act 10of 2009

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:

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."[31]

Recently Lt. Col. Jagmohan Balbir Singh was arrested by the Cyber Cell of the Crime Branch police on the charge of uploading sexually explicit images and clips of children on child pornography websites. Lt. Col. Singh was charged under Section 67 B (punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form) of the Information Technology Act. It was the German police who first spotted the activity from Mumbai on a server located in the United States. They sent a report to the Interpol, which in turn forwarded it to the CBI Delhi, and subsequently to the Mumbai Crime Branch. The Cyber Cell tracked the server activity to the Internet Protocol (IP) address of Lt. Col Singh and subsequently

[31] Information Technology Act, 2000, S. 67B

he was arrested from his residence and charged with section 292 of IPC and 67B of IT Act 2000.[32]

6.1.3 Obscenity and Freedom of Speech and Expression

Freedom of speech and expression is recognized as fundamental right subject to reasonable restriction to maintain law and order, public health morality, decency etc. in Indian Constitution. However freedom of speech and expression is restricted by section 292 and 499 of Indian Penal Code 1860. It means that one can't while exercising their basic right of freedom of speech and expression defame anyone and prohibits expression through obscene material or publication and distribution of obscene material.

The Fundamental right of freedom and speech is not absolute and reasonable restriction are imposed by article 19(2) of Indian constitution which says that reasonable restrictions on the exercise of the right conferred under article 19(1) in 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.[33]

In *Maqbool Fida Husain v Raj Kumar Pandey*[34] the fact of the case is that famous painter MF Husain painted an art work of a nude lady in grief without giving it any title. The untitled painting was sold to a private collector in 2004. In 2006 it was included as part of an online charity auction for victims of the Kashmir earthquake under the name 'Bharat Mata.' Husain had no role or involvement in this auction. There were large-scale protests against the painting, which appeared in an advertisement for the auction. There were multiple complaints filed under section 292, 294, 298 of the Indian Penal

---

[32] http://www.thehindu.com/todays-paper/army-officer-held-for-child-pornography/article763433.ece (Accessed on 6th February, 2016)
[33] The Constitution of India, Art 19(1) and (2)
[34] *Maqbool Fida Husain v Raj Kumar Pandey,* Delhi High Court Crl. Revision Petition No. 114/2007

Code, 1860. The question was that whether portrayal of the nude lady in the painting as "Bharat Mata" should be considered as obscene under section 292 of IPC. The Court held that "…the aesthetic touch to the painting dwarfs the so-called obscenity in the form of nudity and renders it so picayune and insignificant that the nudity in the painting can easily be overlooked." The nude woman was not shown in any peculiar kind of posture, nor was her surroundings painted so as to arouse sexual feelings or lust. The placement of the Ashoka Chakra was also not on any particular part of the body of the woman that could be deemed to show disrespect to the national emblem.

The Court pointed out that "...the literature of India, both religious and secular, is full of sexual allusions, sexual symbolisms and passages of such frank eroticism the likes of which are not to be found elsewhere in world literature." It went on to state that "While an artist should have creative freedom, he is not free to do anything he wants. The line which needs to be drawn is between art as an expression of beauty and art as an expression of an ill mind intoxicated with a vulgar manifestation of counter-culture where the latter needs to be kept away from a civilian society." The Court also said, "There should be freedom for the thought we hate. Freedom of speech has no meaning if there is no freedom after speech. The reality of democracy is to be measured by the extent of freedom and accommodation it extends."[35]

In *K.A. Abbas* v. *Union of India*,[36] the Chief Justice of Supreme Court M. Hidayatullah held regarding film censorship that "*our freedom of speech and expression is not absolute rather limited by reasonable restrictions under Art. 19 (2) in the interest of general public to maintain public decency and morality. Therefore, film censorship has full jurisdiction in the field of cinematograph film to prevent and control obscenity and pornography."*

[35] http://indiatogether.org/uploads/document/document_upload/2141/blawobscenity.pdf (Accessed on 7th February, 2016)
[36] (1970) 2 SCC 780

In *Raj Kapoor and Others v State and Others*[37], The Supreme court while deciding whether the movie, "Satyam Shivam Sundaram," was obscene and indecent or not has said that "While a certificate issued by the Censor Board is of relevance, it does not preclude the court from deciding if a film is obscene or not."

Justice Krishna Iyer further stated that "An act of recognition of moral worthiness by a statutory agency is not opinion evidence but an instance or transaction where the fact in issue has been asserted, recognized or affirmed. The Court will examine the film and judge whether its public policy, in the given time and clime, so breaches public morals or depraves basic decency as to offend the penal provisions. Yet, especially when a special statute (the Cinematograph Act) has set special standards for films for public consumption and created a special Board to screen and censor from the angle of public morals and the like, with its verdicts being subject to higher review, inexpert criminal courts must be cautious to "rush in" and must indeed "fear to tread" lest the judicial process become a public footpath for any highwayman wearing a moral mask holding up a film-maker who has traveled the expensive and perilous journey to the exhibition of his "certificated" picture. Iyer went on to state, "Art, morals and laws, aesthetics are sensitive subjects where jurisprudence meets other social sciences and never goes alone to bark and bite because state-made strait-jacket is inhibitive prescription for a free country unless enlightened society actively participates in the administration of justice to aesthetics." He observed, "The world's greatest paintings, sculptures, songs, and dances, India's lustrous heritage, the Konarks and Khajurahos, lofty epics, luscious in patches, may be asphyxiated by law, if prudes and prigs and state moralists prescribe paradigms and prescribe heterodoxies."[38]

---

[37] AIR 1980 SC 258

[38] http://indiatogether.org/uploads/document/document_upload/2141/blawobscenity.pdf (Accessed on 7th February, 2016)

The Indecent Representation of Woman Act, 1986[39] also related to pornography and obscenity as section 3 and 4 of the act has specifically prohibited the indecent representation of woman through advertisement or in publication, writing, paintings, and figure or in any other manner and or matters connected therewith or incident thereto. Every website on internet constitutes the indecent representation of woman would fall in the ambit of these sections.

In *Jayesh S. Thakkar* v. *State of Maharashtra,*[40] the petitioners wrote a letter to the Chief Justice of the Bombay High Court, about pornographic websites on the internet. The letter was treated as *suo motu* writ petition. The Bombay High Court passed an order to appoint a committee to suggest and recommend ways of preventive and controlling measure and means to protect children from access to pornographic and obscene material on the internet. The Committee upon identifying key issues made recommendations on cyber cafes that asking Cyber Cafés to maintain proper logs and registers of persons entering and using their facilities was feasible and desirable. The Cyber Café operators to keep physical records with addresses, checked against Photo Identity cards, of persons who use their machines. Regular users can be given free 'membership' to obviate the need for re-entering details on each occasion. That minor ought to be restricted to using machines that are not behind partitions or in cubicles and, preferably, are loaded with suitable checking software. This, the Committee felt, would serve both as a check and as a deterrent. The committee placed a special emphasis on lack of technical knowledge in police and recommends special training of cyber cops. The reports of the committee were well accepted by the courts and being put into practice by the police and cyber cafes jointly.[41]

[39] The Indecent Representation of Woman Act, 1986, (Act 60 of 1986)
[40] Bombay H.C. Writ petition No. 1611 of 2001, ; See also www.cyquator.com /html.vol1.pdf.
[41] http://cyquator.com/Html/vol1.pdf (Accessed on 7th February, 2016)

In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000. A student of the Air Force BalBharti School, New Delhi, was teased by all his classmates for having a pockmarked face. He decided to get back at his tormentors. He created a website at the URL www.amazing-gents.8m.net. The website was hosted by him on free web space. It was dedicated to Air Force BalBharti School and contained text material. On this site, lucid, explicit, sexual details were given about various "sexy" girls and teachers of the school. Girls and teachers were also classified on the basis of their physical attributes and perceived sexual preferences. The website also became an adult boys' joke amongst students. This continued for sometime till one day, one of the boys told a girl, "featured" on the site, about it. The father of the girl, being an Air Force officer, registered a case under section 67 of the IT Act, 2000 with the Delhi Police Cyber Crime Cell.[42]

In *Tamil Nadu* v. *Suhas Katti*,[43] The defendant was charged for annoying, obscene and defamatory message in the yahoo message group relating to a divorcee woman. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on a complaint made by the victim, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.The Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC. On the basis of the expert witness the court

[42] http://indiaforensic.com/compcrime.htm (Accessed on 8th February, 2016)
[43] File No. CC No. 4680/2004/February;
www.naavi.org/cl_editorial_04/suhas_katti_case.htm-9k

held that the crime is conclusively proved and the accused was convicted and sentenced to undergo rigorous imprisonment for 2 years and to pay Rs. 500 fine u/s 469 of the IPC i.e. forgery for the purpose of harming reputation; for the offence u/s 509 of the IPC. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.[44]

In *Bazzee.com case,*[45] the story started when a sexually explicit video clip of two school students was shot with a cell phone camera and then distributed among friends through the Multimedia Messaging Service (MMS). The clip, showing a young girl engaged in oral sex with a boy, was shot with her consent but was circulated to the others without her permission. The clip then landed in the hands of a smart entrepreneur who tried to make easy money out of it. Mr. Ravi Raj, a final year M.Sc. Geophysics student of Indian Institute of Technology, Kharagpur had opened an account under the name 'Alice Electronics' on the auction site *Bazee.com* on 21'st of July, 2004. He posted the clip in that account on the 27th of November, 2004 under the header 'DPS Girl having fun' and it remained there till 29th November, 2004. Mr. Raj was arrested on 14th December and produced before a Delhi court two days later. The Court remanded him to three days police custody. Meanwhile, the CEO of Bazee.com, Mr. Avnish Bajaj, was sentenced to jail for six days by a Delhi court. Mr. Bajaj sought his release on bail on the ground that he had been co-operating with the police in the investigation of the case and had flown in from Mumbai to assist the probe. He was granted bail later. The DPS boy who was at the centre of the MMS controversy was also arrested and bought before a Juvenile Court in Delhi. Describing the alleged act as a 'misadventure' and not 'moral depravation', The Principal Magistrate of Juvenile Justice Board granted him bail. On December 24, 2004 the other accused Mr. Ravi Raj was also granted bail by a Delhi court considering the

[44]http://www.indiancybersecurity.com/case_studies/state_of_tamil_nadu_%20suhas_katti.html (Accessed on 8th February, 2016)

[45]http://www.manupatrafast.com/articles/PopOpenArticle.aspx?ID=76985177-567e-48d3-aa2f-cb67be8da4a0&txtsearch=Subject:%20Miscellaneous

fact that the prime accused has already been released on bail. The impact of the incident was that the Delhi government by its notification dated February 1, 2005 banned the use of mobile phones not only by students but also by teachers in all government-run or aided schools. The most ironical part of the story is that it concluded without even knowing what the female student visible in the clip had to say or confess. Thus, Delhi Public School scandal was not only the issue of child pornography but also MMS clip in cyberspace.

In Feb, 2008, A Fast track court in Chennai Sentence orthopaedic surgeon Dr. Prakash to Life imprisonment in case relating to taking obscene picture of the women and uploading them on to internet. Dr. Prakash became the first person to be arrested under the Information Technology Act. He was accused of sexually exploiting women and uploading their obscene pictures on the internet with the help of his brother based in the US. He was charged with offences punishable under Section 67 of the Information Technology Act, besides the provisions of the Indecent Representation of Women (Prohibition) Act, 1986 read with Section 27 of the Arms Act, 1959, and 120-B of the Indian Penal Code.[46]

Addressing a national seminar on the enforcement of cyber law former chief justice Mr. K.G. Balakrishnan has said that "the government could place restrictions on websites that exclusively circulated pornography and hate speech, though it would not be right to clamp blanket bans on all categories of websites."

He stated that "it was also important to distinguish between intermediaries such as network service providers, website operators and individual users for placing liability for wrongful acts. Further said that Liability cannot be mechanically placed on Internet intermediaries, when it is specific individuals who engage in reprehensible conduct. That would be

[46] http://timesofindia.indiatimes.com/city/chennai/Porn-doctor-acquitted-in-drugs-case/articleshow/6088338.cms? (Accessed on 8th February, 2016)

comparable to punishing the persons who build roads for the rash and negligent driving of other persons who operate vehicles on the roads."

He further states that "Democratic values such as freedom of speech and expression, freedom of association and the freedom to pursue an occupation, business, profession or trade must be promoted in the online domain as well."[47]

The Supreme Court of India in *Kamlesh Vaswani v. Union of India & Ors*.[48] told the Centre on 27th February, 2016 to take steps and frame rules to stop access to websites featuring child pornography, classifying them as "obscene" and a threat to social morality. A Bench of Justices Dipak Misra and S.K. Singh was reacting to a submission made by the Supreme Court Women Lawyers Association that there were instances where school bus drivers and conductors forced children under their care to watch porn and sexually assaulted them owing to easy and free access to porn, including child pornography, in the country.

Hearing this, Justice Misra said, "freedom of speech is not absolute, liberty is not absolute" when such rights were misused to subject innocent children to such sexual perversions.

The Supreme Court said, drawing the line on where rights ended and criminality began has said that "Innocent children cannot be made prey to this kind of painful situations and a nation cannot afford to carry on any kind of experiment with its children in the name of liberty,"

Further stated that "The Centre is required to make certain rules and regulations to initially stop child pornography,"

The Supreme Court, however, said a clear distinction had to be made between art and obscenity and stated that "There are those who feel that even

[47] http://www.thehindu.com/news/national/curb-websites-circulating-pornography-says-cji/article425172.ece (Accessed on 8th February, 2016)
[48] Writ Petition No. 177 of 2013, Titled as Kamlesh Vaswani v. Union of India and others

Mona Lisa (painting) is pornography. A distinction has to be drawn between art and obscenity."[49]

6.2. Cyber Stalking

Stalking in general means behaviour of harassing or threatening the other person. Cyber Stalking is an extension of physical form of stalking, which is committed over the online medium with the use of information Technology. In cyber stalking the internet, e-mail, chat rooms etc. are used to stalk another person.

The Wikipedia defines cyber stalking, where the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It include the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass.[50]

Stalking is a continuous process, consisting of a series of actions, each of which may be entirely legal in itself. The definition of Cyber stalking is not universally acceptable as it varies place to place. According to Professor Lamber Royakkers -

"Cyber stalking is the repeatedly harassing or threatening of an individual via the internet or other electronic means of communication. A cyber stalker is someone with amorous and/or sexual motives who constantly harasses someone else electronically: via the bulletin board, chats box, e-mail, spam, fax, buzzer or voice-mail. Stalking generally involves the constant harassment or threatening of someone else: following a person, appearing at someone's house or workplace, making harassing phone calls, leaving written messages or objects, or vandalizing someone's property. Because the stalking

[49] http://www.thehindu.com/todays-paper/tp-national/prevent-access-to-child-pornography-centre-told/article8287151.ece (Accessed on 28th February, 2016)
[50] https://en.wikipedia.org/wiki/Cyberstalking (Accessed on 10 the February, 2016)

activities are so diverse and have to be seen in their connection it is difficult to give a precise description of stalking." [51]

Cyber stalking doesn't not involve any physical contact yet stalking through the internet has found favour among the offenders for certain advantages available like, ease of communication access to personal information and anonymity.[52]

As far as cyber stalking is concerned, the offender has the advantage that he can sit anywhere in the world and harass the victim by posting certain derogatory comment or post comments on common discussion boards or put the mobile number of the victim and his email address on certain social sites which prompt the other users to send massages or phone calls to the victim in misconceived notion. The internet has wide reach, the way we communicate online, the personal data of individual and other information is easily accessed by the offenders through the internet medium, and this makes the individual vulnerable to the offence such as cyber stalking.

Today internet become the integral part of each other life be it personal or professional life. The ease of communication in today's world made it easier for the offenders or person who seeks to take revenge may use this medium to malign the victim by threatening and harassing by sending offensive mails. The fact that cyber stalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. Whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. As with

[51] http://www.sociosite.org/cyberstalking_en.php (Accessed on 10Th February, 2016)
[52] S. K. Verma, Raman Mittal, *Legal Dimension of Cyberspace*, Indian Law Institute, New Delhi.

physical stalking, online harassment and threats may be a prelude to a more serious behaviour, including physical violence.[53]

Stalking has become a problem to women and children on a larger part in comparison to men. Women are threatened, vandalized, assaulted when it comes to real world but the same things happen when cyber stalking takes place. Obscenity also adds up with the, threatens and harassment. No doubt men also become the prey of the same but its lower when it comes to females. Children also undergo the same trauma by adult predators and pedophiles. The victim is normally a person who is less thorough regarding internet services and its applications. The stalker is generally a person who is a paranoid with no self-esteem. But the traits differ from one stalker to another. Some harass to seek revenge or some do so for their own pleasure. While some just to do it for playing a mischief.[54]

There are three ways in which cyber stalking is conducted i.e.

1. **stalking by E-mail** - where the offender directly sends e-mail to the victim to threaten her or to harass her. It is the most common form of stalking in the modern world. The most common is sending hate, obscene, pornographic material and threatening mail to the victim.

2. **Stalking through Internet** – this is global form of cyber stalking. In this the offender doesn't invade the private space of the victim but harasses her through the global medium publically. The offender through the internet medium post the phone numbers and email address of the victim on porn sites and put morphed photos of the victim on cyber space and threaten them. This is the serious nature of cyber stalking where the stalker chases all the activity of victim on the net and posted false information about her on the websites.

---

[53] https://www.astrealegal.com/internet-harassment-cyber-stalking-cyber-harassment-and-cyber/ (Accessed on 11th February, 2016)

[54] Verma Amita, '*Cyber Crimes & Law*', Central Law Publication, p-157-158 also available at http://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india/ (Accessed on 11th February, 2016)

3**. Stalking through Computer -** In this form the offender is technocrat and he can take control of the computer of the victim as soon as the computer starts operating. In this the stalker gets control of the victims computer address and gets control over it. This form of cyber stalking requires high degree of computer knowledge to get access to the targets computer and the option available to the victim is to disconnect the computer and abandon the current internet address.

The term stalking is not new to the world, in the physical space it existed for many centuries. The stalking in the physical world is done by the former friends, employees, or the person who wants to force his will over the target are the examples of stalkers. But after the advent of cyberspace, the reach of the stalker is widened, he can reach to any part of the world and threaten and harass the target. It is not necessary now to disclose his identity, most of the stalkers are the dejected lover's, ex-boyfriends, colleagues, who failed to satisfy their desire and wants to harass the victim. Most stalkers are man and most victims are women. The common reason behind the cyber stalking is rejection in love or one sided love, harassment, revenge and show-off by the offender.

Following are the methods use by the cyber stalker to target the victim:-

1. The stalker if he is a associates of the victim then he can gather all the information about the victim easily and if he is stranger then he collect all the information through internet from various social network sites and collect all and every information about the victim from Date of birth, place of residence, place of work, phone numbers, email ID's to places of visits everything.

2. The stalker may post all the information on any website related to sex-services or dating service, and uses filthy and obscene language to invite

person as if the victim himself posted these information so the interested person may call the victim on his numbers to have sexual services.

3. All the people from the world would call the victims on his phone numbers at home or on mobile asking for sexual services.

4. Some will send e-mail to the victim attaching pornographic material with it and sometimes posted these emails on the pornographic sites.

5. Some will post morphed pictures of the victim on these pornographic and sex-service websites or keep asking for favour and threaten them if they do not fulfill their demands then they will put these pictures all over the internet.

6. Sometimes the stalkers send them repetitive e-mails and call them day and night at his phone numbers and keep track on them. The stalkers sometimes get the help of third party to harass the victim.

The Social Networking sites such as Facebook, Twitter, Orkut, Google plus, Instagram and many more are becoming a medium to cyber stalking in the modern world.

6.2.1 Legal Recognition and Position in India

Though the behaviour widely identified as stalking has existed for centuries, the legal system has only codified its presence in the statues in the recent decades. Cyber stalking only gather importance after the evolution of the internet in the nineties. The rise in crimes related to cyber stalking through the online medium is an extension of traditional stalking that utilizes a high tech *modus operandi*.

In each jurisdiction the statute is different as far as cyber stalking is concerned. In The United States, California is the first state to pass the anti stalking law in 1990. But as far as the stalking through computers is concerned there are few states or countries that passed laws related to cyber stalking.

Indian law do recognise cyber stalking but we do not have law to deal with this issue specifically. The Information Technology act 2000 doesn't contain any provision regarding cyber stalking or cyber bullying or cyber harassment. It is glaring lapse on the part of the government agencies.

The gravity of cyber stalking came into focus in India with *Ritu Kohli's Case,* is the first case in India dealing with cyber stalking. The Delhi Police arrested Manish Kathuria the culprit of the case. In the said case, Manish was stalking a person called Ritu Kohli on the Net by illegally chatting on the website www.mirc.com with the name of Ritu Kohli. Manish was regularly chatting under the identity of Ritu Kohli on the said Website, using obscene and obnoxious language, was distributing her residence telephone number and inviting chatter to chat with her on telephone. Consequently Ritu Kohli was getting obscene calls from different chatters from various parts of India and abroad. Ritu Kohli reported the matter to the police and the Delhi Police swung into action. The police had registered the case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli. But Section 509 of the Indian Penal Code only refers to word, gesture or act intended to insult modest of a woman. But when same things are done on internet, then there is no mention about it in the said section. None of the conditions mentioned in the section cover cyber stalking. Ritu Kohli's case was an alarm to the Government, to make laws regarding the aforesaid crime and regarding protection of victims under the same. As a result Section 66A of the Information Technology Act, 2008.[55]

However, now the Indian Information technology Amended Act 2008[56] directly addresses cyber stalking. The provision for regulating cyber stalking in India is section 66A which runs as follows;

---

[55] http://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india/ (Accessed on 11th of February, 2016)

[56] Information Technology Amendment Act, 2008, Act no 10 of 2009

Punishment for sending offensive messages through communication service, etc.[57]: 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 makes 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,

Shall be punishable with imprisonment for a term which may extend to three years and with fine.

Incidents like sending persistent text massages and sexually explicit photographs/MMS have emerged in the recent past as major cyber offences. The intent behind this section is curbing the menance of sending offensive massages by means of computer resource or through internet device. The offences like obscenity, cyber stalking, defamation, bullying etc. come under the ambit of this section.

However critics felt that section 66A would be used as a tool to curb individual freedom of speech and expression and violative of article 19(1) of the constitution of India, and in year 2015 in the writ petition titled as *Shreya Singhal v. Union of India*[58] the Apex court struck down the section 66A of Information Technology Amendment Act 2008, as it is grossly misused by the authorities and violative of Article 19(1) of Constitution of India.

---

[57] *Ibid, s. 66A*
[58] WP (Crl.) No. 167 of 2012

Thus now, Information Technology Amendment Act 2008 does not directly address stalking. But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in the IT Act 2008. Hence the most used provision for regulating cyber stalking in India is section 72 and 72A of the Information Technology Amendment Act, 2008 which runs as follows[59];

Breach of confidentiality and privacy[60]:

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Punishment for Disclosure of information in breach of lawful contract:[61]

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

[59] http://www.haltabuse.org/resources/laws/india.shtml (Accessed on 12th February, 2016)
[60] Information Technology Amendment Act, 2008, s. 72
[61] *Ibid*, s. 72A

term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

However, after the December, 2012 Delhi gang rape incidence, the Indian government has enacted or amended several new laws. In this anti-stalking law was also passed. The Criminal Law Amendment Act, 2013 added S.354D to the Indian Penal Code to define and punish the act of stalking. This is as follows –

Section 354D[62]. (1) Any man who—

(i) Follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or

(ii) Monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking:

Provided that such conduct shall not amount to stalking if the man who pursued it proves that—

(i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or

(ii) It was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

(iii) In the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a

[62] Inserted by Section 7 of 'The Criminal Law (Amendment) Act, 2013

second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

In July 2015, the Metropolitan Magistrate court convicted a senior executive of a private company in a cyber stalking case for four months imprisonment. This case became first conviction case of cyber crime in the state of Maharashtra. Additional Metropolitan Magistrate N R Natu convicted and sentenced Yogesh Prabhu to four months imprisonment for cyber stalking his colleague working in a cargo handling firm in Panvel. The complainant stated in her complained that the stalker had sent her pornographic images and videos. She also said that she was getting scared as somebody was stalking her movements. "When she went to watch movie at Adlabs, she received an email asking her "How was the movie you enjoyed it?" Another email said why she did not come to temple Prabhadevi on that particular day? Where were she went she got email asking about her visit which scared her and she lodged a complaint. A few days later she started getting emails of pornographic images and movies which shattered her. During the course of investigations the CCIC first traced the IP address of the server from where the emails were sent. The trail led police to her office in Panvel and another IP address was of Gurgaon. Both the IP address was found to be of the same company having its office in Panvel and Gurgaon. Police than wrote to the Gmail server asking them to provide the details of the account holder. During the course of investigations police learnt that Prabhu and the victim used to see each other and wanted to tie knot but due to their age differences, victim's family were not keen on their relationship. Everything ended between them but Prabhu continue to like her and started stalking her. He used to follow her and then immediately send her emails of her locations and other details which scared her.[63]

In year 2011 Delhi University law student has been accused of stalking and threatening a woman online. He also created her fake profiles on social

[63] http://timesofindia.indiatimes.com/india/First-cyber-case-conviction-in-Maharashtra/articleshow/47927461.cms (Accessed on 11th February, 2015)

networking sites to defame her. The woman has lodged a complaint with Delhi Police alleging the accused has been harassing her for over a year now. She said the law student has been making obscene phone calls and sending threatening emails. The victim, while working in Delhi last year, became acquainted with the accused. He asked her to marry him. She alleged that when she refused, he assaulted her and also threatened to kill her. The victim also lodged a complaint with the police earlier and after that, the accused apologized and promised not to bother her in future and also given a written statement to police that he will not stalk her in future. The victim then moved to Goa to live with her parents. But soon after she left Delhi, the accused created her fake profiles on social networking websites. He then uploaded photographs on these sites and declared her to be his wife. The accused also impersonated the victim online and made contact with her friends through these profiles and due to this the girl's marriage was called off. A case under Section 66-A of Information Technology Act was lodged in New Delhi.[64]

In India there are few cases which are coming to limelight but cases related to cyber stalking are rapidly increasing. There are thousands of cyber stalking cases talking place in the nation, but only few reported the cases to the police due the fear or threat. The crime related to cyber stalking is increasing as its counterpart stalking in physical space as tracking the person is too difficult task and he can be anyone from billions sitting anywhere.

Few People now about the cyber stalking crime. Some even do not know that cyber stalking exists in the society or it is termed as crime. Very few people are aware about the legal aspect of cyber stalking. We need to aware people about these crimes and how can they avoid these kinds of crime. The legal provision has to be stringent and the police personnel too need to get regular education and training regarding the new emerging crime in the world.

[64] http://timesofindia.indiatimes.com/city/delhi/DU-law-student-charged-with-cyber-stalking/articleshow/8917937.cms (Accessed on 11th February, 2016)

6.3 Cyber Terrorism

The terrorism phenomenon is very complex issue in the current generation. The attacks of terrorist on the mankind have increased rapidly in last decade. Everyone from normal people to the statehood of the country has suffered due to the violent act of terrorism. The threat of terrorism has become a challenge for the world after post cold war. The state agencies are not adequate enough to tackle or control the terrorist attack on human kind; numbers of people were killed by the inhuman act of the terrorists worldwide. Several counter measures are adopted by the national and international front but they were failed to control the terrorist attack. However, most of these are designed in a conventional pattern, which might be successful in a usual terror attacks. But at present, we live in digital age and computers and internet are also playing their part and becomes a useful tool in the hands of terrorist.

A number of economies were thrown into disarray with the recent financial turmoil. Opinions remain divided on which way the road ahead leads to. But even when household names and industry heavyweights were being brought down to their knees, technology remained steadfast. In fact, technology today has so inconspicuously become a business enabler that it's almost easy to overlook. A new page in the information warfare book comes in a sinister form. Cyber-terrorism involves highly targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage. While we'd often associate terrorism with loss of life, we cannot overlook important results like intimidation or coercion that can be brought about by cyber-terrorism.[65]

A prolonged and targeted terrorism campaign against a country has the potential to render it weak in the long-run. Given the varied economic, financial, and even psychological effects such a campaign could have, cyber-terrorism poses a significant hurdle in times to come. Technology is the backbone of most countries in the world today. A hard hit on such a critical

[65] Dr. Sirohi M. N., *Cyber Terrorism and Information Warfare,* Alpha Editions Delhi

back- bone would be an ideal strategy for attackers. The United Nations telecommunications agency warns that the next world war could well be in cyberspace. This should come as no surprise. Wars have often included attacks on installations or facilities that are critical to the enemy, delivering a crippling blow to gain the higher ground. Considering the sheer magnitude of dependence that the modern world places on technology, it would logically make a fine target if a war were to ensue.[66]

Cyber Terrorism becomes an international threat to the global population as through the terrorism, the terrorist are spreading false propaganda in line with political and religious ideologies. The word "Cyber Terrorism" is of recent vintage and was coined by computer whiz Barry C. Collin[67]. The Term cyber terrorism is the combination of cyberspace and terrorism and we do not have any definition of cyber terrorism which can be accepted worldwide. Every researcher or scholar in the subject gives a different dimension while defining the term cyber terrorism. In this research the definition of cyber terrorism is divided into intent based and effect based. It refers to attacks on the computers, networks and network grids of the country which heavily depend on networks and create havoc or fear among the minds of its citizens.

6.3.1 Definition of Cyber Terrorism

The definition of cyber terrorism cannot be made extensive as the nature of crime is such that it must be left to be comprehensive in nature. The nature of "cyberspace" is such that new mode and tools are invented regularly; Hence it is not wise to put the definition in a straightjacket formula or pigeons hole. In fact, the first effort of the judiciary should be to understand the

[66] Dr. Sirohi M. N., *Cyber Terrorism and Information Warfare,* Alpha Editions Delhi
[67] Barry Collin, "*The Future of Cyber Terrorism*," Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, the University of Illinois at Chicago, 1996.

definition as liberally to punish the terrorist stringently, so the government can tackle the evil of cyber terrorism.[68]

Some efforts have been made to define cyber terrorism precisely. Most notably, Dorothy Denning, a professor of computer science, has put forward an admirably unambiguous definition before the House Armed Services Committee in May 2000: "*Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."*[69]

According to NATO (2008), cyber terrorism is "*a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal."*[70]

The US National Infrastructure Protection Centre, a part of the Department for Homeland Security: *"a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies."* [71]

In the Federal Government, the FBI describes cyber terrorism as: *"Cyber-terrorism is a criminal act perpetrated by the use of computers and*

---

[68] http://www.naavi.org/cl_editorial_04/praveen_dalal/pd_cyber_terrorism_oct25_04_02.htm (Accessed on 13the February, 2016)
[69] http://www.usip.org/sites/default/files/sr119.pdf (Accessed on 13the February, 2016)
[70] NATO, (2008). *Cyber defence concept MC0571*. Brussels, Belgium.
[71] http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/(accessed on 12th February, 2016)

telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda"[72].

A universal acknowledged definition of cyber terrorism is "*a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda."*[73]

The U.S. Federal Bureau of Investigation defines cyber terrorism as "*Cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub- national groups or clandestine agents."*[74]

The Former chief strategist at Netscape, Kevin Coleman, has given the definition of cyber terrorism as: "*The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives*."[75]

The term cyber crime and cyber terrorism is different all together we cannot say that every cyber crime is cyber terrorism. We have to see whether the cyber crime is politically and ideologically motivated or not, to tag it as

---

[72] H. M. Hendershot, '*Cybercrime 2003 – Terrorists*' Activity in Cyberspace and also at http://www.ijiee.org/papers/126-I149.pdf (accessed on 12th February, 2016)

[73] http://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf (accessed on 12th February, 2016)

[74] http://intelligencebriefs.com/what-is-cyber-terrorism-defination/ (accessed on 12th February, 2016)

[75] K. Coleman, 'Cyber Terrorism' (2003) Directions Magazine, http://www.directionsmag.com/articlephp?article also at http://www.ijiee.org/papers/126-I149.pdf (accessed on 12th February, 2016)

cyber terrorism. In Present scenario the aim of the terrorist organization is to destroy the communication, infrastructure, transportation and financial network of the country through the use of computers and networks to create fear in the minds of the people, as every country in the world is heavily depend on the technology. Recent attacks in India as well as in world have proved that the terrorist are also utilizing the computers and networking to carryout terrorist attacks.

6.3.2 Objectives of Cyber Terrorism

The Basic objective of the cyber terrorist organization while attacking a nation, a place and an organization, to destroy tangible property or assets and killing human beings to prove their agenda or political ideologies, Thus there is no doubt that technology advancement in computers and networking has played a vital part in providing them opportunity, which influenced terrorists methods and behaviour considerably. The researcher can identify three main objectives of cyber terrorism:

1. This organizational objective of cyber terrorism includes functions like recruiting, instigation training, fundraising, communication, planning, spying, etc. Following the intelligence reports, terrorist groups nowadays recourse to the Internet on a daily-basis. Their knowledge and skills in regard to computer technology is steadily growing and this build-up of knowledge and skills would eventually provide the necessary expertise for finding and exploiting vulnerabilities in the online security systems of governments or critical infrastructure institutions.[76]

Although those researching the terrorist use of the Internet often describe them as radical factions seeking some sort of virtual jihad, the actors committing cyber terrorism do not have to be religiously motivated. Furthermore, the organizational function of cyber terrorism enables the

[76] Wilson, C. (2005). "*Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress"*. CRS Report for Congress.
also at http://www.history.navy.mil/library/online/computerattack.htm and http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime (Accessed on 13th February, 2016)

wrongdoers to pursue their objective either through the means of traditional warfare or technology.[77]

2. Self-explanatory, the goal which terrorists seek to achieve here is to hinder the normal functioning of computer systems, services, or websites. The methods used are defacing, denying, and exposing. Since the Western countries are highly dependent on online structures supporting vital services, these methods are of proven merit. However, disruptive activities usually do not entail grave consequences, except perhaps in cases of an unpredictable knock-on effect.[78]

3. This purpose is directed towards achieving the same or similar results as classical terrorism, it is labeled pure cyber terrorism. Through the use of computer technology and the Internet, the terrorists seek to inflict destruction or damage on tangible property or assets, and even death or injury to individuals. There are no cases of pure cyber terrorism up to date, but perhaps its occurrence is only a matter of time, given the fact that the states' critical infrastructures have significant security flaws.[79]

6.3.3 Whether the Threat is real or not

The danger caused by cyber terrorism has grabbed the attention of the mass media, the security community, IT industries, Defence sector, politicians, and experts in variety of fields have popularized a scenario in which cyber terrorists electronically break into computers that control dams or air traffic control systems, wreaking havoc and endangering not only millions of lives but national security itself.[80]

---

[77] Brickey, J. (2012). *Defining Cyber terrorism: Capturing a Broad Range of Activities in Cyberspace*. Combating Terrorism Center at West Point also at http://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace and also at http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/ (Accessed on 13th February, 2016)

[78] *Ibid*

[79] *Ibid*

[80] Gabriel Weimann, Cyber terrorism: How Real Is the Threat? Special Report No.119, United States Institute of Peace, December, 2004.also at https://thepeacemission2013.files.wordpress.com/2013/03/study-guide-united-nations-counter-terrorism-committee.pdf (Accessed on 14th February, 2016)

Just how real is the threat that cyber terrorism poses? Because most critical infrastructure in today's world is networked through computers, the potential threat from cyber terrorism is very alarming. cyber terrorist through the help of Hackers can gain access to sensitive information and to the operation of crucial services and can cripple or at least disable the military, financial, and service sectors of advanced economies.[81]

The growing reliance of our societies on computers and internet has created a new form of vulnerability, giving terrorists the chance to approach targets that would otherwise be utterly watertight, such as national defense systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to cyber attacks against its infrastructure. Concern about the potential danger posed by cyber terrorism is thus well founded.[82]

The Crime related to cyberspace has been increasing rapidly; however there is no cyber terrorist attack in Indian public facilities, transport systems, nuclear power plants, power grids, or other key machinery of the national infrastructure. Cyber attacks are regular, but they have not been carried out by terrorists and they have not sought to inflict the kind of damage that would qualify them as cyber terrorism.

6.3.4 Recent Incident of Cyber Terrorism in World

The following are the number of incident which has created problems for nations or which can be termed as terrorist attack by the terrorist group with the help of information technology in the world –

Cyber Attacks in Middle East

With the Middle East Conflict at a very heated moment between bordering countries Pro-Palestinian and Pro-Israel Cyber Groups have been launching an offensive against websites and mail services used by the political sectors the opposing groups show support for. The attacks had been reported

[81] Terror on the Internet: The New Arena, the New Challenges USIP Press Books, 2006. also at http://www.usip.org/sites/default/files/sr119.pdf (Accessed on 14th February, 2016)
[82] *Ibid*

by the NIPC (National Infrastructure Protection Center) in October of 2000 to U.S. Officials. The attacks were a volley of e-mail floods, DoS attacks, and Ping flooding of such sites as the Israel Foreign Ministry, Israeli Defense Forces, and in reverse, sites that belonged to groups such as Hamas and Hezbollah.[83]

India and Pakistan Conflict

As tensions between the neighbouring regions of India and Pakistan over Kashmir grew over time, Pro-Pakistan cyber-terrorists and recruited hackers began to target India's Internet Community. Just prior to and after the September 11th attacks, it is believed that the sympathizers of Pakistan began their spread of propaganda and attacks against Indian Internet based communities. Groups such as G-Force and Doctor Nuker have defaced or disrupted service to several major entities in India such as the Zee TV Network, The India Institute of Science and the Bhabha Atomic Research Center which all have political ties. The Group, Pakistani Hackerz Club also went as far as to target the United States Air Force Computing Environment and the Department of Energy's Website.[84]

Retribution by China

In May 1999 the accidental bombing of a Chinese embassy in Yugoslavia by U.S. Bombers, led to a massive website defacement and email bombardment attack on American companies and agencies. Pro Chinese hackers and political groups executed the attacks to gain sympathy for Chinese cause. US Government sites such as the US department of energy and the interior and the National Park Service were all hit and had website defaced along with the White House website. The sites were downed for three days by

---

[83] "Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection C enter – October 26, 2000 and also at http://www.nipc.gov/warnings/assessments/2000/00-057.htm and https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931 (Accessed on 14th February, 2016)

[84] "Cyber Attacks during the War on Terrorism" India/Pakistan Conflict, Institute for Security Technology Studies - Dartmouth College Vatis, Michael A - September 22, 2001. also at http://www.ists.dartmouth.edu/docs/cyber_a1.pdf (Accessed on 14th February, 2016)

continual e-mail bombing. Although the attack was rather random and brief and affected a small number of U.S. sites, the effects could have been worse.[85]

Cyber attack by Tamil Tigers

In 1998, with surges of violence committed in Sri Lankan over Several years, attacks in cyber-space were the next area to target. The group known as the Tamil Tigers, a violent guerrilla organization bombarded Sri Lankan embassies with over 800 e-mails a day. This was carried out over a two week period. The attack by the e-mail message conveyed the message, "We are the Internet Black Tigers and we are doing this to disrupt your communications." After the messages created such major disruption the local Intelligence authorities were dispatched to investigate. The authorities declared the attack as the first known attack on the Sri Lankan by the terrorists on any computer system in the nation.[86]

Yugoslavia Conflict

When NATO[87] air strikes hit Former republic of Yugoslavia in Kosovo and Serbia, NATO web servers were subjected to sustained attacks by hackers employed by the Yugoslav military. All NATO's 100 servers were subjected to "ping saturation", Distributed Denial Of service assaults and bombarded with thousands of e-mails, many containing viruses. The attacks on NATO servers coincided with numerous website defacements of American military, government, and commercial sites by Serbian, Russian, and Chinese sympathizers of Yugoslavia. These attacks cause serious disruption of NATO communications infrastructures.

---

[85] Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001. Also available at https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931 (Accessed on 14th February, 2016)

[86] Cyber Terrorism – "Testimony before the Special Oversight Panel oil Terrorism"- Dorothy E. Denning - May 23, 2000. also at https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyber-assault-931 (Accessed on 14th February, 2016)

[87] The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance based on the North Atlantic Treaty which was signed on 4 April 1949. The organization constitutes a system of collective defence whereby its member states agree to mutual defense in response to an attack by any external party. (Source Wikipedia accessed on 16th February, 2016)

Cyber Attack on Estonia

The small Baltic country of Estonia was cyber-attacked from Russia. Ever since the government of the Baltic state decided to remove a war memorial to the Red Army from a square in the capital, Tallinn, Russian outrage has ensued. This took the form of demonstrations and even riots. But then something extraordinary happened: quickly, and wholly without warning, the whole country was subjected to a barrage of cyber-warfare, disabling the websites of government ministries, political parties, banks and newspapers. Techniques normally employed by cybercriminals, such as huge remotely-controlled networks of hijacked computers, were used to cripple vital public services. NATO has sent its top cyber-terrorism experts to Tallinn, with western democracies caught on the hop over the implications of such an attack. The Estonian defence ministry said: "*We've been lucky to survive this. If an airport, bank or state infrastructure is attacked by a missile, it's clear war but if the same result is done by computer's, then what do you call It. IS It a state of war? These questions must be addressed."* Estonia has blamed Russia, predictably enough; which, if true, would mean this is the first cyber attack by one sovereign state upon another. The Estonian attacks were more likely to be the work of angry young Russian hackers working alone than any sort of organised blitz by the Kremlin. But either way, the implications are serious.[88]

Sony PlayStation Network, Microsoft's Xbox Live network case

In this case the confidential data of the employees and their families has been leaked in 2014. The company has faced loss in revenue due to movies being leaked, sensitive employee information was disclosed including their salaries and social security numbers, and executive emails were publicized. The attack was hatched by the Lizard Squad, an organization that refers to itself as a cyber-terrorist. Then they launched a massive Distributed

[88] See "Attack of the cyber terrorists" by MICHAEL HANLON Available at: http://www.dailymail.co.uk/sciencetech/article-457504/Attack-cyber-terrorists.html (Accessed on 16th February, 2016)

denial of service attack against Sony's PlayStation Network and Microsoft's Xbox Live networks. They followed up these disruptions with an attack against the Tor Project, a network of virtual tunnels that allow people and groups to improve their privacy and security on the Internet and after that North Korea attacked the network infrastructure and network has gone down for almost Ten hours due to the attack affecting the lives of millions. Due to that many think that it is an act by the US government. However it is not but they manage to create doubts regarding purchasing the product among the consumer and people regarding the multinational companies. The Motive behind these cyber terrorist attacks is collateral damage involved and the obvious ties to geo-political situations that we see in so many attacks. The Current President Barack Obama of United States has said that "cyber-terrorism is perhaps one of the greatest threats against the U.S. today. Unfortunately, the attacks are not only here to stay, but given the utter reliance on the Internet today, they are likely to grow in a very serious manner".[89]

6.3.5 Indian Law & Cyber Terrorism

It is the easiest way in modern scenario is attack a country is through cyber network. India is in developing stage and the impact of cyber attack on Indian infrastructure and communication is going to be immense, because India now heavily depends on computers and information Technology.

There is need of series of innovative laws and global standards on dealing with cyber crimes. The Computer/Internet is changing the process of knowledge creation and dissemination of information as well as deeper transmission is taking place towards redefining the communication process. Thus a fine balance can be achieved between terrorism and Law enforcement with due care and consideration. Thus we have enacted Information Technology Act, 2000 to punish the cyber criminals.

---

[89] See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/ (Accessed on 16th February, 2016)

Earlier there was no specific provision in the IT Act, 2000 which deals specifically with Cyber terrorism due to this, a new section 66F has been inserted by Information Technology (Amendment) Act, 2008. It is a welcome change brought by the IT Amendment Act, 2008 in view of increasing terrorist activities in India and neighbouring nations.

Punishment for cyber terrorism[90] - (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 authorized 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 is 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 destruction of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database 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.

[90] Information Technology Act, 2000, s., 66F

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life.

For the prevention of cyber terrorism we can use the method of "Counter strike through aggressive Defence". The concept of counter strike through aggressive defence presupposes the adoption and use of information technology to produce legitimate and legalized disabling and reasonably destructive effects. Some adopted measures completely destroys the functioning of the offending computer while others simply disable the computer for the time being by either shutting it down or making it temporarily non-functional. The technology adopted must not only be safe and effective, but it must also be "legal and law-abiding". A counter-measure, which is not very accurate, and law abiding would be a remedy worst than the malady and hence it should be avoided. For instance, if a virus has been launched by using a public server, then by disabling that server the genuine and legitimate users will be unnecessarily harassed and they would be denied the services which they are otherwise entitled to. Thus, the countermeasure measure adopted must be job specific and not disproportionate to the injury sought to be remedied.[91]

In March 2013, suspected Chinese hackers breached the computers of India's top military organisation, the Defence Research and Development Organisation (DRDO), in what was touted to be amongst the biggest such security breaches in the Indian history. India has seen many such attacks on its critical installations and the misuse of social media and Internet has brought home the threat of cyber-terrorism, the country is vulnerable to such cyber-terrorism attacks with some countries and vested interest groups bent on espionage and destruction.[92]

---

[91] Article by Praveen Dalal, Cybercrime and cyber terrorism: Preventive defence for cyberspace violations, Computer Crime Research Center, March 10, 2006.

[92] http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274 (Accessed on 16th February, 2016)

According to Pavan Duggal the threat of cyber attacks remains "imminent", the country lacks an institutionalised mechanism of a cyber army to deal with the threat. Further stated that "the recent DRDO breach was a classical case of cyber war attack rather than mere hacking. It was an attack on India's critical information infrastructure. Cyber warfare as a phenomenon is not covered under the Indian cyber law. Clearly, India's cyber security is not in sync with the requirements of the times."[93]

Over the past few years, India has witnessed a growing number of cyber terrorist attacks, with government departments, particularly defence establishments, coming under attack. There are following cases of cyber terrorism in India.

1. In 2012, hacker group 'Anonymous' carried out a series of Distributed Denial of Service (DDoS) attacks against a number of government websites, in retaliation against the alleged Internet censorship.

2. Also in 2012, Hackers from Algeria carried out an attack on websites run by the DRDO, the Prime Minister's Office and various other government departments.

3. Hackers from Pakistan and terrorist organization are increasing their attacks on Indian Websites to provide a new dimension to the ongoing conflict over Jammu and Kashmir. 'GForce' a group of anonymous hackers whose members write slogans critical of India and its claim over Kashmir, have owned up to several instances of hacking of Indian sites run by the Indian government like breaking into the high security computer network of Bhabha Atomic Research Center.

4. Indian Parliament attack is one of the deadliest attacks on Indian Democracy. It is a case of cyber terrorism where accused committed cyber forgery and made passes, downloaded official logo and layout map of the parliament has been downloaded through the Pakistan service provider. They controlled the e-mail and identity system of Indian Army.

---

[93] *Ibid*

5. In March, 2016 the Indian Infrastructure was attacked by the Terror outfit with the name of Al Qaeda who, allegedly hacked a micro site of the Rail net page of the Indian Railways to show its sinister reach for the first time. The hacked page of Bhusawal division of Personnel Department of the Central Railway and part of a large intranet created for the department's administrative needs was replaced by a message of Maulana Aasim Umar, Al Qaeda chief in south Asia, for all Indian Muslims to participate in Jihad.[94]

Information Technology becomes an easy tool in hands of terrorist. They use computers and networks to communicate with their operatives all around the world in codes without detected by the enforcement agencies. Cases like Ayodhya incident, attack in Mumbai in 2006, defacement of Indian Military sites in India by hackers in July 2005, attack on American Center at Kolkata and Pathankot Terrorist Attack etc., are the major cyber terrorist attacks in India.

As per the cyber law and cyber security expert Prashant Mali "*The threat landscape remains very threatening, India is awakening to the global threat of cyber warfare now. Our cyber security is still ineffective as mass awakening towards it is missing or inadequate. Even though NTRO and DRDO are mandated with cyber offensive work, only time will show effectiveness of these organisations.*"

With cyber security impacting the country's security, Shiv Shankar Menon, the national security adviser, announced that the government is putting in place national cyber security architecture to prevent sabotage, espionage and other forms of cyber threats.

Shantanu Ghosh, vice president at India Product Operations-Symantec Corporation, which developed Norton Antivirus has said that "*The past few years have witnessed a dramatic shift in the threat landscape. The motivation of attackers has moved from fame to financial gain and malware has become a*

[94] http://www.ndtv.com/india-news/al-qaeda-hacks-into-indian-railways-website-leaves-message-to-join-jihad-1283023 (Accessed on 21 March, 2016)

successful criminal business model with billions of dollars in play. We have now entered a third significant shift in the threat landscape, one of cyber-espionage and cyber-sabotage."

Rikshit Tandon, advisor to the Cyber Crime Unit of the Uttar Pradesh Police, said: "*Cyber terrorism is a grave threat not only to India but to the world. It can come to any country and, yes, a proactive measure by government and consortium of countries needs to be taken as a collective effort and policy since internet has no geographical boundaries*".[95]

6.4 Hacking

Hacking is labelled as amongst the most serious of all cyber crimes. It is said that hacking erodes the faith of people in information technology and the Internet. Hacking a computer system has been projected as a menace requiring harsh laws to act as deterrents. Such a general projection is somewhat misconceived.

Hacking a computer simply implies getting into another's computer without permission. Gaining unlawful access to another's computer is hacking. Unauthorized entry into a computer belonging to another is hacking. It is equivalent to phone-tapping. Hackers see the weakness in the target computer programme and then find ways to enter and access therein. Anti-hacking tools such as the 'Firewall' technology and intrusion detection systems are preventive measures that can be taken to protect a computer from being hacked. Firewall, like a wall of fire, prevents hacking. Intrusion detection systems will in addition also try to detect the source of hacking.

Hacking *perse*, in simple terms, is criminal trespass into a computer that is a private property. Criminal trespass under the Indian Penal Code, 1860 is simply defined as entering into property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, by unlawfully remaining there with intent thereby to intimidate,

[95] *Ibid*

insult or annoy any such person or with intent to commit an offence.[96] Criminal trespass entails a punishment of imprisonment upto three months or fine upto rupees five hundred, or with both[97] Criminal trespass *perse* is thus a minor offence.

Here is a short list of great hackers of the world.

The most famous hacker in the history is Kevin Mitnick. At the tender age of 17 in 1981, he hacked into a phone exchange that allowed him to redirect subscriber calls in any way he wanted. In 1983, he accessed a Pentagon computer. In 1990s, he cracked/hacked/broke into the computer systems of the world's top technology and telecommunications companies like Nokia, Fujitsu, Motorola and Sun Microsystems. He was arrested by the FBI in 1995 and later released on parole in 2000.[98]

Gary McKinnon, an Englishman, was arrested in November 2002 on the accusation that he had hacked into more than 90 US military computer systems in the U.K.[99]

Vladmir Levin, a Russian computer 'expert' is said to be the first to hack a bank to steal money. In early 1995, he hacked into Citibank and robbed US$ 10 million. He was arrested by Interpol in the U.K. in 1995, after he had transferred money to his accounts in the US, Finland, Holland, Germany and Israel.[100]

A Los Angeles radio station announced a contest that would reward the 102nd caller with a 'Porsche 944S2'. Kevin Poulsen took control of the entire city's telephone network and ensured he was the winner being the 102nd caller. He also hacked into 'Arpanet' that was the precursor to the Internet. Arpanet was a global network of computers.[101]

---

[96] Indian Penal Code, 1860., s. 441
[97] Indian Penal Code, 1860., s. 447
[98] http://www.funonthenet.in/forums/index.php?topic=1260.0;wap2 (Accessed on 20th February, 2016)
[99] *Ibid*
[100] *Ibid*
[101] *Ibid*

US based hacker Timothy Lloyd planted a malicious software code in the computer network of Omega Engineering which was a prime supplier of components to NASA and the US Navy. Omega lost US$10 million due to the attack by which its manufacturing operations were impaired.[102]

Species of criminal trespass have been treated with more deterrent punishments. For instance, punishment for house-trespass is punishable with imprisonment upto one year.[103] House-trespass in order to commit an offence punishable with death (i.e. murder etc.) is punishable with imprisonment for life or rigorous imprisonment upto ten years.[104] House-trespass in order to commit an offence punishable with imprisonment for life is punishable with imprisonment upto ten years.[105] House-trespass, other than the above, entails punishment with imprisonment extending to two years and if the offence intended to be committed is theft, the term of the imprisonment may extend to seven years.[106] For house-trespass committed after preparation to cause hurt, assault or wrongful restraint or putting any person in such fear, the punishment prescribed is imprisonment extending to seven years.[107] Lurking house-trespass or housebreaking is punishable with imprisonment extending to two years.[108] Lurking house-trespass or housebreaking in order to commit an offence punishable with imprisonment, is liable for imprisonment upto three years and if such intended offence is theft, the term of imprisonment has been extended to ten years.[109] The punishment for lurking house-trespass or housebreaking by night is punishable with imprisonment extending to three years.[110] Grievous hurt caused whilst committing lurking house-trespass or housebreaking, is punishable with imprisonment for life, or imprisonment

---

[102] *Ibid*
[103] Indian Penal Code, 1860., s. 448
[104] Indian Penal Code, 1860., s. 449
[105] Indian Penal Code, 1860., s. 450
[106] Indian Penal Code, 1860., s. 451
[107] Indian Penal Code, 1860., s. 452
[108] Indian Penal Code, 1860., s. 453
[109] Indian Penal Code, 1860., s. 454
[110] Indian Penal Code, 1860., s. 456

extending to ten years.[111] All persons jointly concerned in lurking house-trespass or housebreaking by night, are liable to be punished with imprisonment for life or extending to ten years, where death or grievous hurt is caused or attempted to be caused by any one or more of them.[112]

Another instance of an offence that has numerous species is "mischief". Every species of mischief is separately laid down in the I.P.C. with differing punishments, depending upon the magnitude thereof.[113] Many of the offences in the I.P.C. such as robbery, criminal breaches of trust, cheating etc., have their respective species that are treated differently from one another.

The legal approach towards hacking should be the same as that of criminal trespass, mischief and the innumerable other offences in the I.P.C. All forms of hacking cannot be treated alike. It needs to be understood that hacking too has numerous dimensions and species like other offences.

A person who enjoys exploring computer systems is also a hacker. Many teenagers obsessed with the Internet and computers hack for fun and excitement. Excitement to make an impact, show of capability and knowledge of computers, fun and publicity, and the desire to explore are some of the motives of these teenagers to hack into computer systems.

Another form of hacking is by Internet security companies, to test the computer systems of their clients and potential clients, to impress them and get business assignments of setting up security systems for the clients.

Hacking is also committed to damage the business of competitors and enemies. Disruption of a computer and denial of access to a person authorized to access any computer, are some of the damages that may be caused by hacking. Hacking is also done to spy into others computer systems and for stealing information/data residing therein. Hacking is also used as a Weapon

[111] Indian Penal Code, 1860., s. 459
[112] Indian Penal Code, 1860., s. 460
[113] Indian Penal Code, 1860., s. 425-440

to commit other crimes such as cheating and misappropriation of funds electronically from the bank account of another.

Hacking is done at the country level too. Frequently, Pakistani hackers are accused of hacking Indian web-sites. For instance, the web-site of SEBI (Stock Exchange Board of India) was hacked whereby a link to a pornographic web-site was inserted.

Hacktivists are protestors against governments or institutions / organizations, who protest through hacking. For instance, anti-globalization protests have been made through hacking the web-site of WTO.

There are therefore numerous species of hacking, though in essence, it is the offence of criminal trespass. All forms of hacking cannot thus be treated alike. It is the intent, purpose and consequences of hacking that determine its gravity. A twelve year old, who, for excitement and playing a prank enters restricted web-sites, should not be treated as a national enemy. A terrorist organization hacking into a protected system such as the defence computer systems to steal nuclear secrets, or a criminal syndicate hacking to misappropriate huge amounts, cannot be treated on par with a teenager prying into the computer system of his best friend's girlfriend or even the CBI (Central Bureau of Investigation) for fun and excitement. The nature of the hacking determines the gravity and all forms of hacking should not be projected or legally treated in the same manner. Hacking has so many species. Hacking is a skill that can be used positively as well as negatively. A man opening locks to help people who have lost the key is a locksmith. However, a person who opens locks to steal is a thief.

The seriousness of hacking depends upon the nature, purpose, intent and the extent of loss and injury that are caused to the victim. For instance, in a reported incident in the U.S., the owner of a hobby web-site for children received an e-mail informing her that a group of hackers had gained control over her web-site. They demanded a ransom of one million dollars. The threat was overlooked as a mere scare tactic. A few days late, she discovered that the

hackers had ‘web-jacked’ her web-site. ‘Web-jacking’ has been equated with hijacking an aeroplane, as forcibly assuming control of a web-site, for diverse motives. The hackers had altered a part of the web-site which said “How to have fun with goldfish”. The word “goldfish” was replaced with “piranhas”. Piranhas are tiny but extremely dangerous flesh eating fish. Many children visiting the web-site, purchased ‘piranhas’ from pet shops and tried playing with them, thereby hurting themselves badly. [114]

Hacking in various forms is already part of several offences, either as the means to their commission or as a consequence. For instance, hacking could be a tool and means to commit cheating, misappropriation, criminal breach of trust, theft, copyright violations, spying into official secrets, or as part of the conspiracy to wage war against the State, that are all well defined offences. Some of the species of hacking have been defined as contraventions as well as criminal offences in the LT. Act, 2000 as amended by the I.T. (Amendment) Act, 2008. In the original version of the I.T. Act, 2000, section 66 defined and punished hacking in the following terms:

“Hacking with Computer System - (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects is injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both”.[115]

The title of the aforesaid section 66 was a misnomer, which created confusion. It was widely believed as if section 66 was the only legal provision that dealt with the offence of hacking a computer system. This confusion has

[114] “Hack Attack” by Shuchi Nagpal, Asian School of Cyber Laws in Indian Express Vigil, March 2002. also available at http://www.asianlaws.org/press/hack_attack.htm (Accessed on 20th February, 2016)
[115] Information Technology Act, 2000., s. 66

been done away with, by certain amendments made by the I.T. (Amendment) Act, 2008. The words "Hacking with Computer System" have been deleted from section 66, the scope of which has been substantially widened:

"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".[116]

The various species of the offence of hacking that are provided (even though not called 'hacking' specifically) for or may have elements of hacking, in the amended version of the I.T. Act, 2000 are:

- Access to a computer.
- Downloading, copying or extraction of data from a computer.
- Introducing computer virus and contaminants.
- Causing damage to a computer.
- Causing disruption of a computer.
- Causing denial of access to a computer.
- Affecting critical information infrastructure.
- Cyber terrorism.

6.5 Virus[117] and Contaminants

Computer contaminants and virus have a long history. Theories of self-replicating programs were first developed in 1949. In 1981, Apple Viruses 1, 2 and 3 were found on Apple II operating systems. These viruses had spread through pirated computer games. In 1987, the 'Lehigh' virus infected the

[116] Sec. 66 of the I.T. Act, 2000 as amended by the I.T. (Amendment) Act, 2008.

[117] A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

‘command.com’ computer files. In 1988, one of the most common viruses, ‘Jerusalem’ was unleashed. This virus was activated every Friday the 13th and affected both ‘.exe’ and ‘.com’ files and deleted any programs run on that day. In 1990, Symantec launched ‘Norton Anti-virus’ that was amongst the first anti-virus programs developed by a large company. In 1992, it was discovered that 1300 viruses were in existence, that was an increase of 420% from December, 1990. This was the year when the ‘Dark Avenger Mutation Engine’ (DAME) was created, which was a toolkit that turned viruses into polymorphic viruses. In 1994, the ‘Good Times’ e-mail hoax tore through the computer community. The hoax warns of a malicious virus that would erase an entire hard-drive just by opening an e-mail with the subject line "Good Times". In 1995, ‘Word Concept’ became one of the most prevalent viruses, which spread through Microsoft Word documents. In 1996, the ‘Baza’, ‘Leroux’ and ‘Staog’ viruses infected Windows 95 files, Excel and Linux respectively. In 1998, ‘Strange Brew’ was the first virus to infect Java files. This year, the ‘Chernobyl’ virus also spread quickly via ‘.exe’ files. The virus was quite destructive, attacking not only files but also the chip within infected computers.[118]

In 1999, the ‘Melissa’ virus infected about one million computers. Also, ‘Bubble Boy’ was the first worm that did not depend on the recipient opening an attachment for the infection to occur. As soon as the user opened the e-mail, the worm started its destruction. This year, ‘Tristate’ was the first multi-program macro virus to be deployed and it infected Word, Excel and Power point files. In the year 2000, the famous ‘Love Bug’, also known as the ‘I LOVE YOU’ virus multiplied itself via the Outlook program. The virus came as an attachment and deleted files including ‘MP3’, ‘MP2’ and ‘JPG’. It also sent usernames and passwords to the author of the virus. Also, the ‘W97M.Resume.A’, like the Melissa virus, infected ‘Outlook’ and spread itself. Unlike the previous viruses, ‘Stages’ was hidden in an attachment with a

[118] http://www.infoplease.com/ipa/A0872842.html (Accessed on 01 March, 2016)

false '.txt' extension, luring recipients to welcome it. The year 2000 was also the year when the 'distributed denial-of-service' attacks knocked out leading web-sites such as 'Yahoo', 'eBay', 'Amazon' etc, for several hours.

Shortly after the '9/11' attacks in 2001, the 'Nimda' virus infected hundreds of thousands of computers in the world. This virus has been amongst the most sophisticated ones, with five different methods of replicating and infecting computer systems. The 'Anna Kournikova' virus mailed itself to people enlisted in the victim's Microsoft Outlook address book. Several worms were also born this year such as 'Sircam', 'CodeRed' and 'BadTrans'. 'Sircam' spread personal documents over the Internet through e-mail, while 'Code Red' attacked vulnerable web-pages. It infected about 359,000 computers in the first twelve hours or so. 'BadTrans' captured passwords and credit card information.

In 2002, the creator of the 'Melissa' virus, David C. Smith was sentenced to twenty months in the federal prison. Several viruses named after celebrities like 'Shakira', 'Britney Spears' and 'Jennifer Lopez' also spread during this year. In 2003, the 'Slammer' worm, the fastest spreading worm till date, infected about 75000 computers in ten minutes. This year, the 'Sobig' worm became amongst the first few worms to make the infected computer systems spam relay points. In the year 2004, a computer worm called 'MyDoom' or 'Novarg' spread through e-mails and file-sharing software faster than its earlier cousins. 'MyDoom' enticed e-mail recipients to open an attachment that allowed hackers to access the hard-drive of the afflicted computer system. The objective of the worm was to make a 'denial of service' attack on the 'SCO Group' that was suing various groups for using an open-source version of its 'Unix' programming language. SCO offered a reward of US $2, 50,000 to anyone giving information leading to the arrest and conviction of the worm's authors. Also, the 'Sasser' Worm affected about one million computers using Windows. An 18-year-old German high school student confessed to developing this worm. The year 2005 'welcomed' the

world's first cell-phone virus called 'Common warrior-A'. It is said to have originated from Russia, spreading through a text message. In the year 2008, the 'Conficker' virus infected between nine and fifteen million computer server systems across the world, including servers of the French Navy, the U.K. Ministry of Defence, Norwegian Police and other large government organizations.[119]

Computer virus is as common as the common cold. Every computer even that of Mr. Bill Gates, the creator of Microsoft would suffer from a computer virus at some point of time or other. Just as some dust and insects are likely to creep into the home howsoever many precautions are taken, computer virus must get into the computer through a CD, floppy or pen-drive that is corrupted or through the Internet where they float like their cousins in the air that cause common cold, viral fever or more serious diseases.

Section 43-(c) of the I.T. Act, 2000 imposes a monetary liability of upto rupees one crore upon a person who, without the permission of the owner or incharge of a computer, introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network. "Computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource. "Computer contaminant" means any set of computer instructions that are designed-

- to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
- by any means to usurp the normal operation of the computer, computer system, or computer network;

[119] http://www.infoplease.com/ipa/A0872842.html (Accessed on 01 March, 2016)

Section 43 imposes a strict liability upon the person who plants any computer virus or contaminant. All the violations stipulated in section 43 including clause (c) that covers the violation of introduction or causing the introduction of any computer contaminant or computer virus into any computer, have also been made criminal offences.[120] Hence, dishonestly or fraudulently introducing or causing the introduction of a computer virus or computer contaminant into another's computer, would also constitute a criminal offence entailing an imprisonment of two years. Even with mens rea, to penalize the introduction of computer contaminant or virus into another's computer, in the present state of information technology in our country, is totally unjustified. Our law makers should have at least asked themselves certain fundamental questions before criminalizing the planting of computer virus and contaminants:-

- What is the level of general awareness in our country about computer contaminants and virus?
- How many people in our country, who use computers, are aware of anti-virus software and how many out of them use the same?
- What is the general level of consciousness amongst people, that before sending a computer file to another through a CD, floppy, pen-drive or the Internet, it should be checked whether there is virus in it or not?
- With computer contaminants and virus floating everywhere in floppies, CDs, pen-drives and the Internet, how will it be proven prima facie or otherwise, as to who introduced/transmitted the contaminants or virus in question?
- Are our law enforcement agencies and the judiciary equipped to determine the source of the computer contaminant and virus?

It is extremely difficult to find the source of a virus and contaminant in a computer system. The offence of planting virus and contaminant in a

[120] Sec. 66 of the I.T. Act, 2000 as amended by the I.T. (Amendment) Act, 2008.

computer system is susceptible to gross misuse and erroneous application. The author of a virus and contaminant, who infects multiple computer systems, like the viruses and worms discussed above, would stand on a different footing. A harsh liability including corporal punishment, on the author of a virus that is circulated by him, is justifiable. However, to prosecute persons who merely transmit virus and contaminants is ex-facie draconian. There is hardly any awareness in our country about computer virus and contaminants or anti-virus software. Our law enforcement agencies have no expertise to determine the precise source of the virus. It is practically very difficult to locate the source of a virus, especially with viruses and contaminants floating in the cyber world like dust, and virus that causes common cold. Our legislators ought to have conceived various other situations and problems. For instance, a person may not even know that there is virus in his computer. New types of virus come into existence from time to time and many of them are not detectable by anti-virus software. Hence, even if a person installs anti-virus software, virus can creep into the computer and unknowingly such virus can be transmitted to others. Since intention/mens rea is inferred from the incident and its consequences, apart from the allegations by the complainant, false and misconceived criminal cases alleging planting virus and contaminants are likely to be galore in our country. Adding insult to injury, it would be only at the end of the ordeal of facing prosecution-cum-persecution, that the accused would get an opportunity to prove his innocence during defence evidence.

To make transmission of virus and contaminants, a criminal offence, should have waited for our people to mature as users of computers and the Internet, which would take at least another fifteen to twenty years. A nominal fine like a traffic challan to start with, would have sufficed and the law should have evolved with the growth of awareness, consciousness and maturity amongst computer users at large. Transmission of virus or contaminant, as a civil violation under section 43 of the IT Act, 2000 with a nominal fine is still justifiable.

However, dealing with the law as it is, a heavy responsibility lies on our judiciary to protect citizens from harassment of being implicated for transmitting computer virus and contaminants. It would be a tragic comedy to see every computer user in the country as the complainant/victim of computer contaminants and virus, and also a criminal being accused of introducing computer virus and/or contaminants into another's computer.

6.6 Cyber Crimes related to Finance

The Price Waterhouse Coopers organization, which deals with the economic crime survey, has defined economic crime in cyber world as *"an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cyber crime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."*[121]

According to the findings of survey on Economic Crime in India in Global Economic Crime Survey 2011. The use of the internet in India is growing rapidly. According to a recent Telecom Regulatory Authority of India (TRAI) survey, we currently have 354 million internet subscribers.[122] While burgeoning growth in the use of internet provides multiple options to cyber citizens in all possible spheres from entertainment to education, it has also given rise to cyber crime. This new breed of tech-savvy fraudsters poses a new set of challenges. 24% of the respondents, who reported economic crime, have experienced cyber crime in the last 12 months. We believe that this data alone shows how serious the risk of cyber crime is to organizations. In the background of the recent incidents of cyber crime on multinational companies and financial institutions, a greater number of organizations are becoming victims of cyber crime. One potential reason that may explain this sudden rise

[121] As defined in the Global Economic Crime Survey 2011 by PwC in conjunction with our survey academic partner, Professor Peter Sommer
[122] http://www.trai.gov.in/

in cyber crime is the rise in the volume of e-business, greater penetration of internet and e-commerce.

Economic crime does not discriminate. It is truly global. No industry or organization is immune. We have seen that despite fraud being a serious business issue, 10% of the respondents in 2011 as compared to 6% in 2009 was not aware if their organization has been a victim to economic crime in the last 12 months. The reason for awareness levels being low can be attributed, to an extent, to the frequency of performing fraud risk assessment. One third of the respondents to the survey do not perform fraud risk assessment due to a perceived lack of value. This trend is exposing more organizations to the risk of fraud. The fallout isn't just the direct costs: economic crime can seriously damage employee morale, brands or tarnish reputation, leading organizations to lose market share. As society becomes less tolerant of unethical behaviour, businesses need to make sure they are building – and keeping – public trust. Today, most people and businesses rely on the internet and other technologies. As a result, they are potentially opening themselves up to attacks from criminals anywhere in the world. Against a backdrop of data losses and theft, computer viruses and hacking, this survey looks at the significance and impact of this new type of economic crime and how it affects businesses worldwide. Cyber crime ranks as one of the top four types of economic crime. More than half (58%) perceive Information Technology department as a high risk department with respect to committing cyber crime. 96% said that their organizations monitor internal and external electronic traffic and web-based activity. About 80% of Indian respondents reported that cyber crime threat originates within India or through a combination of in and outside the country. About 2/3rd of respondents did not have access to forensic technology tools that are useful in combating cyber crime. 35% of respondents did not have any cyber security training in the last 12 months. Asset misappropriation has not only been the most common type of economic crime but also shown a remarkable increase - 20% in 2007 to 68% in 2011. Nearly two-thirds of the

respondents found that the perpetrators were among their own staff. In most cases, perpetrators of fraud were male, between the ages of 31 and 40, and educated to degree level or higher. 80% of respondents said their organization terminated the individual who committed the fraud and more than half of the respondents ceased to conduct business with outsiders who engaged in fraudulent conduct. Despite the growing confidence that organizations surveyed have in their risk management systems most fraud (35 %) is still detected by chance.[123]

The cyber crime offers low risks and high rewards as compared to traditional crimes. For example, in an externally perpetrated cyber crime, a fraudster infiltrates a banking system, remotely, to steal money or personal information. The fraudster is at a lesser risk when compared to someone who physically steals assets from an organization. There are fewer risks when committing cyber crime. The fraudster is not present at the location; hence the chances of getting caught are less. It is difficult for law enforcement agencies to follow traditional investigative steps to prosecute the perpetrator owing to the different location and jurisdiction of the perpetrator. The perpetrators can return to the scene of the crime with relatively minimal fear of detection.[124]

The Financial Cybercrime includes cheating, credit card frauds, money laundering, forgery, online investment frauds etc. such crimes are punishable under both IPC and IT Act. A leading Bank in India was cheated to the extent of 1.39 crores due to misappropriation of funds by manipulation of computer records regarding debit and credit accounts. Most cases involving computer-related fraud have been prosecuted under existing criminal legislation and this has been adequate to cope with these offences. However applying traditional criminal concepts to acts involving intangible information has meant that some

---

[123] Economic Crime in India: an ever increasing phenomenon, Global Economic Crime Survey 2011, India, Price Waterhouse Coopers, 2011. also available at https://www.pwc.in/assets/pdfs/publications-2011/economic-crime-survey-2011-india-report.pdf (Retrieved on 17th February, 2016)

[124] *Ibid*

amendments have proved necessary to resolve issues of applying existing definitions to the new technology.

There are various legislations in India which deals with the Fraud and related activities, some of them are: Section 25 of Indian Penal Code[125] does attempt to define the word fraudulently by saying that there can be no fraud unless there is an intention to defraud. In general, fraud is used in different ways viz.

- To deprive a man of his right either by obtaining something by deception or by taking something wrongfully without the knowledge or consent of the owner.
- To withhold wrongfully from another, what is due to his or to wrongfully prevent one from obtaining what he may justify claim.
- To defeat or frustrate wrongfully another's right to property.
- Whenever the words fraud, intent to defraud or an intent to expose some person to actual or possible injury.
- The main intent and object of the fraudulent person is in every case, his own advantage.

A conclusive test as to the fraudulent character of a deception for criminal purposes is whether to it is the deceit derived any advantage from it which he would not have had if the truth has been known. If so, that advantage would generally have an equivalent in less or risk of less to someone else and if so, there is fraud. Fraud encompasses within its fold the scam of the Internet. Both the essential requisites of fraud i.e. deceit or intention to deceive and actual a possible injury to an individual or a group of individuals are present in such scams. All such scams whatever their *modus operandi*, are intended to gain advantage for some almost always at the risk of loss to others.

Sections 415 to 420, IPC detail the law relating to cheating, in the case of Internet Scams relevant sections relating to the crime of cheating such as cheating by impersonation (Section 416) cheating with knowledge that

[125] Indian Penal Code (Act No. 45 of Year 1860).

wrongful loss may ensure to person where interest if offender is bound to protect (Section 418), etc. may be applied according to the facts of the case.
The word Fraud is clearly defined under the Indian Contract Act, 1872.[126] Section 7 - "Fraud" Defined: "Fraud" means and includes any of the following acts committed by a party to a contract or with his connivance or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract.

The IT Act, 2000[127] deals with the crimes relating to Internet fraud and online investment fraud in sections 43(d), 65 and 66. Section 43(d) penalizes a person who damages or causes damage to data. 'Damage', under clause (iv) of the Explanation, means to destroy, alter, add, modify or rearrange any computer resource by any means. Therefore, unauthorized alteration of data would come within the ambit of section 43 (d) which is sufficient to cover computer crimes like issuance of false stocks or market manipulation schemes since they essentially involve alteration and/or addition of data. Section 65of the IT Act makes tampering with computer source code an offence. 'Computer source code' has been defined as the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Internet fraud would also come within the scope of section 66 of the IT Act dealing with wrongful loss or damage to the public or any person due to destruction or alteration of any data residing in a computer resource or due to diminishing its value or utility or affecting it injuriously by any means. Other related enactments are the Companies Act, 2013 and the Securities and Exchange Board of India Act, 1992 as also sections 415 to 424 of the IPC pertaining to cheating.

6.6.1 Recent cases relating to Financial Cybercrime

1. In 2005 a student of MBBS of Bangalore was arrested; he used to post juicy advertisements for high-performance laptops on different websites.

[126] The Indian Contract Act, 1872 (Act No. 9 of 1872)
[127] The Information Technology Act, 2000 (No. 21 of 2000)

Many took the bait and made online purchases but the laptops never reached them. He had made several lakhs in the bargain. After complain was made he was arrested by tracing his IP address, on the charge of Online Fraud.[128]

2. In May 2006: In a landmark judgment, the Delhi High Court passed an injunction order against four lawyers including a Nigerian national, restraining them and their representatives from using in any manner the proprietary data and confidential information stolen from their erstwhile employer Titus & Co. Advocates. In this Data theft case that involved law firm Titus & Co, its four employees had illegally copied and removed electronic records including protected and confidential information from computers belonging to Titus & Co. These lawyers later formed a new organization relying on the pilfered data. Thereby action was brought by Titus & Co against these former employees to restrain them from using the "copied material" from their erstwhile employer firm.[129]

3. Chennai Cyber Crime Police arrested four persons last week, who formed part of a UK-based gang. For withdrawing money from ATMs through the use of forged credit cards, whose data was stolen through the Cyber Crime of Skimming.[130] They had cheated people of over 20 lakhs rupees three days prior to their arrest. And police recovered 160 fake credit cards from their possession.[131]

4. In 2011, two persons who fraudulently made online transactions with credit cards of other customers were arrested by Central Crime Station sleuths. According to police, the duo used to call up people randomly and collect credit card data of cardholders, their phone numbers and other personal

---

[128] Bangalore MBBS student held for internet fraud Express News Service Delhi Newsline, New Delhi, March 21, 2005.

[129] India Cyber Law and Cases, one of the largest Database of Cyber Law and Cases from India. Available at: http://cybercases.blogspot.com/.

[130] Skimming: Fake card entry slots are used by criminals who perpetuate this crime. The information on the card is recorded on a device hidden in the card entry slot. In it the criminal use a small machine called a skimmer that reads the data on the magnetic strip of the card and clones it.

[131] http://www.ibnlive.com/news/credit-card-cloning-swipes-india/10923-3.html(Retrieved on 17th February, 2016)

details by posing as agents of banks. "Once they received the data, they created a fake email ID in name of the credit card holder and register the same on EBay". Before creating the ID, they change the card holder's phone number to their phone number by contacting the customer care of the bank by furnishing all details of the actual card holder. By misusing the above data, the fraudsters did online shopping. While making online purchases, they give false delivery address and their phone number. Once the courier agent calls them for delivering the goods, they insist they come to their office to deliver. To get the goods, they prepared fake ration cards, voter ID cards and PAN cards in name of the actual card holder with help of Photoshop software on their laptop and by producing the same, they get the goods.[132]

5. In 2013, A con man from Maharashtra who cheated ICICI Bank customers by obtaining their credit card data has fallen into the Delhi Police net after illegal online transactions of over Rs 1 crore in the past one year. He was misusing the data of around 4,500 credit card holders for the last one-and-half years, police said, adding that employees of the bank could be involved in leaking the data to him. He, claiming to be an ICICI Bank employee, assured the victim to refund their money. But just after getting the card details, he made an electricity bill payment of Rs 44,911 to Maharashtra district electricity board, there is a strong possibility of the involvement of employees of the ICICI Bank," said SBS Tyagi, deputy commissioner of police.[133]

6.7 Phishing and Vishing

In computing, phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an

[132] http://www.ibnlive.com/news/india/two-persons-held-for-online-credit-card-fraud-425297.html(Retrieved on 17th February, 2016)
[133] http://www.ibnlive.com/news/india/delhi-police-arrests-con-man-for-credit-card-frauds-623798.html (Retrieved on 17th February, 2016)

instant message.[134] The term phishing arises from the use of increasingly sophisticated lures to "fish" for 'users' financial information and passwords. The act of sending an e-mail to a user falsely claiming to be established legitimate enterprises in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Website where they are asked to update personal information, such as passwords, credit card, social security, and bank account numbers, that the legitimate organization already has. The Website, however, is bogus and set up only to steal the user's information.[135]

The motive behind phishing is that people will share their credit card information, passwords, bank account numbers and other information thinking that they are sharing their information to the legitimate organization but in real they are sharing their information with bogus website or organization which is going to steal their money.

Vishing is also alike phishing; it is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.[136]

Recently in a landmark judgment in India in the case of *Uma Shankar v. ICICI Bank*, the Adjudicator of Tamil Nadu has passed an award for

---

[134] Lance James, "Phishing Exposed", Elsevier 2005. also at https://en.wikipedia.org/wiki/Phishing (Retrieved on 17th February, 2016)
[135] http://www.crimedoctor.com/phishing-scam.htm (Retrieved on 17th February, 2016)
[136] Dr. B. Muthukumaran, "Cyber Crime Scenario in India" Criminal Investigation Department Review- January2008 also at http://www.gcl.in/downloads/bm_cybercrime.pdf (Retrieved on 17th February, 2016)

payment of Rs 12.85 lakhs to a petitioner who alleged a fraudulent withdrawal from his ICICI Bank account. Bank contended that the issue involved customer negligence and did not fall under the jurisdiction of the adjudicator. The Adjudicator held that an offence is made out under ITA 2000 and it falls under the jurisdiction of the adjudicator. The honorable adjudicator proceeded to accept the petitioners argument that the Bank had not exercised due diligence and therefore was liable under Section 85 of the Act to pay the compensations.[137]

Most methods of phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers, For example, the link http://www.google.com@membcrs.abc.com/ might deceive a casual observer into believing that the link will open a page on www.google.com, whereas the link actually directs the browser to a page on members.abc.com, using a username of www.google.com; were there no such user, the page would open normally. This method has since been closed off in the Mozilla and Internet Explorer web browsers, while Opera provides a warning message and the option not to follow the link.[138]

Nowadays Phishing attacks are becoming common form of risk in Internet based Banking. Banks have been largely forcing the customers to believe that the liability for Phishing should be borne by the customers because they were negligent in responding to the Phishing mail. However, the legal position can be different. Phishing is a result of multiple contraventions of Information Technology Act 2000 particularly after the amendments of 2008. It results in wrongful loss to the customer. The contravention therefore

---

[137] http://www.governancenow.com/news/regular-story/icici-bank-gets-rs-1285-lakh-lesson-e-security and also at http://www.naavi.org/ (Retrieved on 17th February, 2016)

[138] "Phishing, n." OED Online, March 2006, Oxford University Press. Oxford English Dictionary Online. and also at https://en.wikipedia.org/wiki/Phishing (Retrieved on 17th February, 2016)

attracts provisions of Section 43 for adjudication. Already, several complaints have been registered against Banks in Bangalore, Chennai and Hyderabad.

The Banks are basically being held liable under the age old Banking law that "Forgery cannot be held against the customer, however clever or undetectable the forgery is". Additionally, Banks are ignoring the law of the land through IT Act 2000 as well as the Guidelines of RBI and not using digital signatures for authentication of Internet transactions. This makes them negligent under Sections 79 and 85 making them liable for any offence attributable to a computer belonging to the Bank. Recently Bank of India has set precedence by accepting liability for Phishing in one the cases filed in Bangalore and repaying the amount along with interest to the customer who was a victim of a Phishing fraud.[139]

6.8 Denial of Service Attack

This is an act by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.[140]

In a typical connection, the user sends a message asking the server to authenticate it. The server returns the authentication approval to the user. The user acknowledges this approval and then is allowed onto the server. In a denial of service attack, the user sends several authentication requests to the server, filling it up. All requests have false return addresses, so the server can't find the user when it tries to send the authentication approval. The server

[139] http://www.naavi.org/cl_editorial_09/edit_dec_23_09_boi_phishing.htm (Retrieved on 18th February, 2016)

[140] Understanding Denial-of-Service Attacks (US CERT) http://www.us-cert.gov/cas/tips/ST04-015.html. also at http://www.cybercellmumbai.gov.in/html/cyber-crimes/denial-of-service-attack.html (Retrieved on 18th February, 2016)

waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again tying up the service indefinitely.[141]

Attacks can be directed at any network device, including attacks on routing devices and Web, electronic mail, or Domain Name System servers. A DoS attack can be perpetrated in a number of ways. There are three basic types of attack:

1. Consumption of computational resources such as bandwidth, disk space or CPU Time;

2. Disruption of configuration information, such as routing information;

3. Disruption of physical network components.

Distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods. Malware can carry DDoS attack mechanisms; one of the more well known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent. Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. It is important to note the difference between a DDoS and DoS attack. If an attacker mounts a smurf attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses, a thousand zombie systems to

[141] Manthan M Desai,"Hacking For Beginners: a beginners guide to learn ethical hacking" also at http://www.cnet.com/news/how-a-denial-of-service-attack-works/ (Retrieved on 18th February, 2016)

simultaneously launch smurf attacks against a remote host, this would be classified as a DDoS attack.[142]

The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down.[143]

Trinoo was the first well known Distributed denial of Service attack used against the University of Minnesota in August 1999. This two day attack involved flooding servers with UDP packets originating from thousands of machines. Source addresses were not spoofed, so systems running the offending daemons were contacted. However, the attacker responded simply by introducing new daemon machines into the attack. Trinoo was first found as a binary daemon on a number of compromised Solaris 2.x systems. Malicious code had been introduced through exploitation of buffer over-run bugs in the remote procedure call (RPC) services.[144]

6.9 Data Theft

The biggest case of data breach/data theft/identity theft was exposed in January, 2009, in which Albert Gonzalez, a 28-year-old American along with his two Russian accomplices, were arrested for masterminding a global scheme to steal data of more than 130 million credit and debit cards by hacking into the computer systems of five major companies including Hannaford Bros Supermarkets, 7-Eleven and Heartland Payment Systems, a credit card processing company.[145] Gonzalez has been said to be one of the nation's (U.S.) cyber-crime kingpins, by prosecutors. Previously, he was alleged to be the kingpin who masterminded a data breach of over 40 million

---

[142] Internet security by Wikipedians, Pediapress, p. 29 also at https://www.mywot.com/wiki/Denial_of_Service_Attack (Retrieved on 18th February, 2016)
[143] *Ibid*
[144] https://www.sans.org/security-resources/idfaq/distributed-denial-of-service-attack-tools-trinoo-and-wintrinoo/9/10 (Retrieved on 18th February, 2016)
[145] http://www.wsj.com/articles/SB125053669921337753 (Accessed on 01 March, 2016)

credit card numbers from TJX Cos and others, causing the parent company of TJ Maxx retail chain, losses of about US$ 200 million.

Data and information are valuable assets in this digital age. Business secrets, technical knowhow, designs, music, films, books, personal data including usernames, credit card numbers and passwords, are some forms of property that drive the information economy. Money, time, effort and creativity go into the creation and compilation of data and information. Stealing of data and information through hacking and other means, is the most prevalent cyber crime.[146]

Data is like a chameleon that plays comedy with our traditional law relating to theft. Theft is a crime that has existed in our law since time immemorial. Section 378 of the Indian Penal Code defines 'theft' in the following words:-

"378. Theft. - Whoever, intending to take dishonestly any moveable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft."

As per the aforesaid definition, there can be theft in law of only moveable property, which is required to be moved. The term 'moveable property' is intended to include corporeal property of every description except land and things attached to the earth or permanently fastened to anything which is attached to the earth.[147] Theft has been held to be an offence that applies only to tangibles. Electricity, for instance, has been held as not covered within the ambit of 'moveable property'. The Supreme Court in *Avtar Singh v. State of Punjab*[148] held that stealing of electricity is theft because of section 39 of the Electricity Act, not section 378 I.P.C. The Court said:

---

[146] Vivek Sood, Cyber Crimes, Electronic Evidence & Investigation – Legal Issues 137-139 (NABHI Publications, New Delhi, 2010) also at http://thegiga.in/LinkClick.aspx?fileticket=KX1_Imk_gDs%3D&tabid=589 (Accessed on 01 March, 2016)

[147] Indian Penal Code, 1860., s. 22

[148] AIR l965 SC 666

"With regard to the first reason that Section 39 of the Act extended the operation of Section 378 of the Code, it seems to us beyond question that Section 39 did not extend Section 37 8 in the sense of amending it or in any way altering the language used in it. Section 378, read by itself even after the enactment of section 39, would not include a theft of electricity for electricity is not considered to be moveable property. The only way in which it can be said that Section 39 extended Section 378 is by stating that it made something which was not a theft under Section 378, a theft: within the meaning of that section. It follows that if Section 39 did so, it created the offence itself and Section 378 did not do so. In this view of the matter we do not think it possible to say that the thing so made a theft and an offence, became one by virtue of Section 378".

Applying the law of theft to information and data is a comedy of sorts. When information and data are encapsulated in a tangible form, for instance, stored in a floppy, CD, or pen-drive, they are part of moveable property and hence can be said to be stolen if the medium (floppy, CD, or pen-drive) is moved without the consent of the person in possession. Also, if the computer itself is stolen, since data and information are a part thereof, they too can be said to be stolen. However, in the online environment, where data and information are intangible i.e. mere combinations of binary numbers, the legal definition of 'theft' falls short. Stealing of data and information online is no 'theft' in the eyes of section 378 I.P.C.

In this sense, the expression 'data theft' is a misnomer from the legal perspective. It is an expression of common parlance. For instance, if an employee dishonestly and without the consent of his employer sends/transmits critical data through e-mail to an e-mail account belonging to him or another, it would not amount to theft under the I.P.C. However, if he were to store the data in a CD and take it away, it would amount to theft.

Data/information theft can be said to be committed in six ways, in other words, it has the following species:

- The first unauthorized copying of data / information;
- Making unauthorized subsequent copies;
- Making a copy and dishonestly sending the data/information online;
- Unauthorized copying of data / information in a floppy, C.D. or pen-drive and dishonestly taking it away;
- Stealing the computer itself;
- Data / Information already reside in a movable storage medium (floppy, C.D. or pen-drive) that is dishonestly taken away.

Applying the definition of theft in the Indian Penal Code, 1860 to the above species, only the latter three constitute the offence of 'theft' under section 378.

Similarly, for the offence of dishonest misappropriation of property also (as defined in section 403 IPC), the property must be moveable i.e. tangible. As per the definition, whoever dishonestly misappropriates or converts to his own use any moveable property, shall be punished with imprisonment upto two years.

The I.T. (Amendment) Act, 2008 however brings into existence the offence of 'data theft' (even though not encapsulated in a medium such as CD, computer pen-drive or floppy). The following clauses of section 43 read with the new version of section 66 that makes the said clause a penal offence, incorporates the offence of 'data theft' in the true sense of the expression from the legal perspective:

"43. If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,

(b) Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer including information or data held or stored in any removable storage medium.

(c) Steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage."

Another form of data breach is breach of trust with respect to data and information. The I.T. industry primarily deals with data and information in some form or the other. A call center uses data to answer queries of customers of banks, telecom service providers etc. A software company develops software using data and information. A web-site compiles information and presents it online.

Data and information drive the I.T. industry. They are the inputs, raw material and outputs for the I.T. industry. Data and information may be entrusted to employees of the organization, its business associates, service providers, agents and other parties for specific purposes. Incidents of breach of data and information, by such trusted parties frequently confront the I.T. industry. Misappropriation of data / information by a person who holds it in trust would amount to criminal breach of trust under the Indian Penal Code.

In 2010, the two cases of data theft have come to light, first is *Travelocity.co.in v. ClearTrip.com* and second is *JustDial v. Infomedia*. In the first case Travelocity has filed an FIR with Gurgaon Police against CEO, Cleartrip and former MD of Desiya alleging criminal breach of trust, data theft, cheating, criminal misappropriation and criminal conspiracy. It was alleged that MD Desiya has pass on the company's intellectual property, trade secrets, sensitive data, proprietary technology source codes, their entire hotel business model and projections to the CEO of Cleartrip. In the second case it is reported that JustDial has obtained injunction against Infomedia 18 Limited for running website www.askme.in, as it was alleged that Infomedia 18 Limited had copied JustDial database onto its newly launched website: www.askme.in, thereby violating JustDial's database copyrights. The injunction was granted exparte by the Hon'ble High Court and further order has been made for search and seizure to be carried out at Infomedia's Delhi

and Mumbai offices, as prima-facie case was made out by the Just Dial officials.[149]

6.10 Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating; recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable.[150]

Electricity companies are the one who mostly suffer due to this kind of crime in India. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.[151]

6.11 Salami Attacks

A salami attack is a series of minor data security attack that that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can he considered a salami attack. Crimes involving salami attacks typically are

---

[149] http://www.cyberlawtimes.com/indian-web-portal-wars-travelocity-cleatrip-justdial-infomedia-askme-data-theft/(Retrieved on 18th February, 2016)
[150] http://www.niagarapolice.ca/en/community/computercrimeprevention.asp (Retrieved on 18th February, 2016)
[151] http://indiaforensic.com/compcrime1.htm (Retrieved on 18th February, 2016)

difficult to detect and trace. These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. A bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.[152]

To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first introduced a logic bomb into the bank's systems. The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither the account holders nor the bank official noticed the fault. It was brought to their notice when a person by the name of Ziegler opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday.[153]

6.12 E-mail Bombing

In internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelms the server. Mail bombing is the act of sending an e-mail bomb, a term shared with the act of sending actual exploding devices. Mail bombing is sometimes accomplished by giving the victim's e-mail address to multiple spammers. In the Russian internet community, there is

[152] Kabay, ME Salami fraud, www.nwfusion.com/newsletters/sec/2002/01467137.html.
[153] Smith RG, Grabosky PN and Urbas GF 2004. Cyber criminals on trial, Cambridge University Press.

another sense for mail bomb. There, mail bomb is a form of denial of service attack against a computer system.[154]

E-mail bombing refers to sending a large number of e-mails to the victim resulting in the victim's e-mail account(In case of Individual) or mail servers (in case of a company or an e-mail service provider) crashing. In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed. E-mail bombing is characterized by abusers repeatedly sending an e-mail message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact.[155]

E-mail spamming is a variant of bombing; it refers to sending e-mail to hundreds or thousands of users. E-mail spamming can be made worse if recipients reply to the e-mail, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users.[156]

6.13 E-mail Spoofing

E-mail spoofing is a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail

---

[154]A general overview of e-mail bombing is available at https://www.cert.org/historical/tech_tips/email_bombing_spamming.cfm? and also at http://www.worldwizzy.com/library/E-mail_bomb (Retrieved on 18th February, 2016)
[155] Atul Jain (ed.), Cyber Crime: Issues Threats and Management, Isha Books, 2005. http://cybercrime.planetindia.net/frequently_used.htm (Retrieved on 18th February, 2016)
[156] https://www.cert.org/historical/tech_tips/email_bombing_spamming.cfm? (Retrieved on 18th February, 2016)

spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. By changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. It is often associated with website spoofing which mimic an actual, well-known website but are run by another party either with fraudulent intentions or as a means of criticism of the organisation's activities."[157]

It is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. Spoofing can be used legitimately. Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency or a "whistle-blower" who fears retaliation. However, spoofing anyone other than you is illegal in some jurisdictions.[158]

E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include an authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, this precaution is not often taken. If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send messages. To send spoofed e-mail, senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could

---

[157] Deb Shinder, Understanding E-mail Spoofing, www.windowsecurity.com, April 6 2005 also available at http://searchsecurity.techtarget.com/definition/email-spoofing (Retrieved on 18th February, 2016)

[158] Tom Merritt, What is E-mail Spoofing? http://www.g4tv.com/techtvvault/features/17167/What_is_Email_Spoofing.html (Retrieved on 18th February, 2016)

send spoofed e-mail that appears to be from you with a message that you didn't write.[159]

Recently Flipkart CEO Binny Bansal's email account was spoofed. The Official statement from the company has stated that the CEO's e-mail account has been spoofed and the spoofed email does not originate from the real source but from a different source falsifying the name and address with an ulterior motive. The company also filed a police complained and released the statement that they have filed a case of email spoofing which involves use of a forged email header to make it look like a legitimate email. This case of email spoofing was immediately detected and a report was filed with police.[160]

6.14 Logic Bombs

In a computer program, a logic bomb is a programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command.[161] Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed.[162] Many viruses attack their host systems on specific dates, such as Friday the 13th or April fool's Day. Trojans that activate on certain dates are often called "time bombs". It is in effect a delayed-action computer virus or Trojan horse. A logic bomb, when

[159] E-mail Spoofing is a new form of spam, FAQ's on e-mail spoofing and Phishing, Available at http://www.mailsbroadcast.com/e-mail.broadcast.faq/46.e-mail.spoofing.htm (Retrieved on 18th February, 2016)
[160] http://indianexpress.com/article/technology/tech-news-technology/flipkart-ceo-binny-bansal-email-account-spoof-hack/ (Retrieved on 18th February, 2016)
[161] M. E. Kabay, Logic bombs, Part 1, Network World Security Newsletter, 08/12/02.
[162] Julian Layton, How does a Logic bomb work? available at http://computer.howstuffworks.com/logic-bomb.htm (Retrieved on 18th February, 2016)

"exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.[163]

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

6.15 Internet Time Theft

Theft of Internet hours refers to using somebody else's internet hours. Section 43(h) of the Indian Technology Act, 2000, lays down civil liability for this offence. It reads as, whoever without the permission of the owner or any other person who is incharge of a computer, computer system or computer network, charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, computer network is liable to pay damages not exceeding one crore to the person on office.[164]

Normally in these kinds of thefts of the Internet another person uses up surfing hours of the victim. This is done by gaining access to the login ID and the password. E.g. *Colonel Bajwa's case*[165] this case reported before the enactment of the Information Technology Act, 2000. In May 2000, the economic offences wing, IPR section crime branch of Delhi police registered its first case involving theft of Internet hours. In this case, the accused, Mukesh Gupta an engineer with Nicom System (p) Ltd. was sent to the residence of the complainant to activate his Internet connection. However, the accused used Col. Bajwa's login name and password from various places

---

[163] Meaning of Logic bombs at http://en.wikipedia.org/wiki/Logic_bomb. (Retrieved on 18th February, 2016)
[164] Information Technology Act, 2000., s. 43
[165] Cyber Crimes - Technical Issues, Internet Time Theft, Available at http://www.asianlaws.org/cyberlaw/library/cc/what_cc.htm (Retrieved on 18th February, 2016)

causing wrongful loss of 100 hours to Col. Bajwa. Delhi police arrested the accused for theft of Internet time.

On further inquiry in the case, it was found that Krishan Kumar, son of an ex army officer, working as senior executive in M/s Highpoint Tours & Travels had used Col Bajwa's login and passwords as many as 207 times from his residence and twice from his office. He confessed that Shashi Nagpal, from whom he had purchased a computer, gave the login and password to him. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber crimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested Krishan Kumar under sections 379, 411, 34 of IPC and section 25 of the Indian Telegraph Act. In another case, the Economic Offences Wing of Delhi Police arrested a computer engineer who got hold of the password of an Internet user, accessed the computer and stole 107 hours of Internet time from the other person's account. He was booked for the crime by a Delhi court during May 2000.[166]

6.16 Cyber Crime related to Intellectual Property Rights

6.16.1 Domain Name violations and passing off

A domain name identifies a computer or a sub Network of computers in the Internet. In simple terms, a domain name is a name-cum-address on the Internet, of any person or entity. A computer or device that is attached to the Internet has an address popularly known as Domain name. With the advancement of internet communication and growing e-commerce and its future potential, domain names today are serving as trade names or brands and carry with them the goodwill and reputation of the websites they represent. Domain names being used as business identifiers have attained importance and legal sanctity as a means of differentiation between e-players since e-

[166] http://indiaforensic.com/compcrime1.htm (Retrieved on 18th February, 2016)

commerce is conducted in the absence of personal interaction or the opportunity to inspect the goods.

In *Cardservice International Inc. v. Mc Gee*[167], it was held that the domain name serve same function as the trademark and is not a mere address or like finding number on the Internet and, therefore, it is entitled to equal protection as trademark. It was further held that a domain name is more than a mere Internet address for it also identifies the Internet site to those who reach it, much like a person's name identifies a particular person.

The word 'domain' as per Chambers 21st Century Dictionary means a territory owned or ruled by one person or Government.

Webster's defines it in different contexts as under:—

- A field of action, thought, influence;
- Territory governed by a single rule or Government;
- Region characterised by a specific features;
- Law;
- Land to which their superior title and absolute ownership.

Thus, in common parlance any title or name or mark or brand or identity in any field of activity or a trade name over which a particular individual has the exclusive, prior and lone claim is the domain name or trade name for any kind of activity. Trade mark is at par with a territory and the owner of any trade mark is placed in the same position as owner of territory.[168]Domain name registrations and protection of a trademark in relation thereto has been recognised by courts.

The law relating to passing off is fairly well settled. The principle underlying the action is that no man is entitled to carry on his business in such a way as to lead to the belief that he is carrying on the business of another man or to lead to believe that he is carrying on or has any connection with the business carried on by another man. The principles of common law govern

[167] Cardservice International Inc. v. Mc Gee, 42 USPQ 2d 1850
[168] Pfizer Products Inc. v. Altamash Khan, 2006(32) PTC 208 (Del);
Acqua Minerals Ltd. v. Pramod Borse, 2001 PTC 619 (Del)

actions of passing off. As held by courts, the purpose of this tort is to protect commercial goodwill to ensure that people's business reputations are not exploited. It is based on economic policy, the need to encourage enterprise and to ensure commercial stability.

There is a difference between statute law relating to trademarks and the passing off action; for, while registration of relevant mark itself gives title to the registered owner, the onus in a passing off action lies upon the plaintiff to establish the existence of the business reputation which he seeks to protect. The asset protected is the reputation the plaintiffs business has to the relevant mark. It is not always necessary that there must be in existence goods of that other man with which the defendant seeks to confuse his own. Passing off may occur in cases where the plaintiffs do not in fact deal with the offending goods.

With the advancement and progress in technology, services rendered in the Internet has also come to be recognised and accepted and are being given protection so as to protect such provider of service from passing off the services rendered by others. In an Internet service, a particular Internet site could be reached by anyone anywhere in the world who proposes to visit the said Internet site. As a matter of fact in a matter where services rendered through the domain name in the Internet, a very alert vigil is necessary and a strict view is to be taken for its easy access and reach by anyone from any corner of the globe. It is also observed that considering the vastness of the Internet and its relatively recent availability to the general public, many Internet users are not sophisticated enough to distinguish between the subtle difference in the domain names of the parties.

The degree of the similarity of the marks usually is vitally important and significant in an action for passing off.

The two marks/ domain names 'Yahoo', and 'Yahooindia' are almost similar except for use of the suffix 'India' in the latter. There is every possibility of an Internet user being confused and deceived in believing that

both the domain names belong to one common source and connection, although the two belong to two different concerns. As held by the Supreme Court, the word 'India' added to one mark is of no consequence. Thus there is every possibility of the Internet users to believe that 'Yahooindia' is another name in the series of Yahoo marks/ names and thereby there is every possibility of confusion being created and thereby preventing these users from reaching the Internet site of plaintiff, 'Yahoo.com'.[169]

In another case, the defendants were found manufacturing, selling or offering for sale the products like Supari and Chewing Tobacco under the trademark 'Yahoo'.[170]

Under the trademark INFOSYS, the plaintiff company was incorporated in the year 1981 and has earned a very high degree of goodwill having acquired the status of one of the leading exporters of computer software. Defendants use of trade mark/ name INFOSYS, also engaged in computer business, amounts to infringement of the plaintiffs registered trade mark numbers. Defendants hosted a website www.blitzerinfosys.com and mark INFOSYS was posted on such website prominently.[171]

Pen Books Pvt. Ltd. got registered the domain name 'penbooks.com' in 1999 but, due to some technical snags could not launch the website. The validity period of registration of the said name expired on 2-3-2001. When the plaintiff sought to launch the website again in 2002, it found that the domain name 'penbooks.com' stood registered in the name of defendant and it was advertised on the Internet for sale. The Court found such a registration in the name of the defendant to be an abusive registration of domain name in violation of the rights of trademarks and service marks. Considering the Uniform Domain Name Disputes Resolution Policy, the Court found that the domain name having been registered by the defendant for the purpose of

[169] Yahoo! Inc. v. Akash Arora, 1999 PTC (19) 201 : 1999 II AD (Del) 229 : 78(1999) DLT 285 also in Ruston Hornby Ltd. v. Zamindara Engineering co., AIR 1970 SC 1649
[170] Yahoo! Inc. v. Sanjay V. Shah), 2006(32) PTC 263 (Del)
[171] Infosys Technologies Ltd. v. Akhil Gupta, Decided on 21-11-2006 (Del)

selling or transferring the same was to be treated as having been registered in bad faith.[172]

The trade mark VIAGRA is registered in the name of plaintiff in 147 countries. Its application for registration of the trade mark in India is pending. The plaintiff having spent a lot of time, money and effort in developing the product and the trade mark VIAGRA as its registered owner does have a legitimate interest in protecting its brand. Defendant does not have any interest in the domain name 'viagra.in' apart from putting it up for sale. In any event, the domain name 'viagra.in' is, if not identical, confusingly similar to the trade mark VIAGRA and the domain name 'viagra.com' of which plaintiff is the proprietor. The domain name 'viagra.in' is inactive. The Court held that the conduct of the defendant, is nothing but of 'cyber squatting'. Squatting on an address in cyber space over which the rights and interests of the plaintiff far outweigh those, if at all, of the defendant.[173]

6.16.2 Software Piracy

Copyright subsists throughout India in the following classes of works:-

- Original literary, dramatic and musical;
- Artistic works;
- Computer Programme;
- Cinematograph films; and
- Sound recording.

In India, the Copyright Act, 1957 governs computer software. So as to keep pace with the advancement of science and technology especially in the field of communication and data processing, Parliament has amended the Copyright Act, 1957 in year 1995. 'Computer Programme' within the meaning of Section 2(ffc) of the Copyright Act is included in the definition of a literary work as per section 2(o) of the said Act. The definition of 'literary works' specifically includes computer programmes, tables and compilations including

[172] Pen Books Pvt. Ltd. v. Padmaraj, 2004(29) PTC 137
[173] Pfizer Products Inc. v. Altamash Khan, 2006(32) PTC 208 (Del);

computer databases. The term ‘computer programme’ as defined by Section 2(ffc) of the Copyright Act, means a set of instructions expressed in words, codes, schemes or in any other form including a machine readable medium, capable of causing a computer to perform a particular task or result. Computer programs are the product of an intellectual process. It may be copyrightable as intellectual property. Therefore, reading section 2(i), 2(ffc) and Section 13 and 14 of the Copyright Act, it becomes clear that a computer programme is by very definition original literary work, therefore law protects such copy right. Some common methods of copyright infringement in relation to computer software as stated are:—

- Reproducing the original owner’s software and packaging of that software, so that purchasers are deliberately misled into believing that the product they are buying is genuine software.
- Reproducing or ‘burning’ the original owner’s software onto a blank CD, where no attempt is made to represent that the copy is genuine.
- Reproducing a number of the owner’s programme on a single CD-ROM, known as a ‘compilation’ CD.[174]

Another form of piracy that is assuming alarming shape in the information technology age is that of internet piracy when software is downloaded from the Internet or distributed via internet without the permission of the copyright owner.

Due to fast expanding consumer base of computer products, it is a common knowledge that there is voluminous counterfeit and piracy of hardware and software of leading companies. Under Section 63 of the Copyright Act, any infringement of the copyright in a computer programme / source code is punishable. Therefore, prima facie, if a person alters computer programme of another person or another computer company, the same would be infringement of the copyright. What is a computer source code is defined in the Explanation to Section 65 of the Information Technology Act, 2000. The

[174] Microsoft Corporation v. Deepak Raval, 2006(33) PTC 122 (Del)

courts have frowned upon the conduct of the violators wilfully calculated to exploit the advantage of an established work and held that in such circumstances, the plaintiff would be entitled to compensation. In India also a positive trend has started. Here also courts are becoming sensitive to the growing menace of piracy and have started granting punitive damages even in cases where due to absence of the defendant's exact figures of sales under the infringing copyright and / or trade mark, exact damages are not available. The courts in India have followed the same path and applied the same principles as applied by the US, UK and Australian courts in awarding the damages.[175]

Microsoft Corporation, a company world famous for its business software such as Microsoft Windows, Microsoft Office etc. which are installed and used on million of computers all over the world, including India, also manufacturer a large range of computer peripherals (hardware). The company received information that the defendants are infringing their copyright by carrying on business of unauthorised hard disk loaded i.e. pre-loading various software's of the plaintiff company onto hard disc of the computer that were being assembled and sold by them. The software loaded onto the machine, naturally, were not accompanied by the Original Media, being the Compact Disc (s) / Floppy Discs, Certificates of Authenticity (COA), End User Licence Agreements (EULAs), User Instruction Manuals, Registration Cards and so on that accompany the plaintiff's genuine software. The defendant, inspite of notice, had failed to respond. The Court held it as wilful, intentional and flagrant violation by the defendant of plaintiff's copyrights in MS DOS, MS WINDOWS and trade mark in Microsoft.

Section 63-B of the Copyright Act, 1957, as inserted by the 1994 Amendment, makes an end user of an infringing copy of a computer program liable for corporal punishment.

---

[175] Aktiebolaget Volvo v. A.K. Bhuva, decided on 5-5-2006 (Del); Hero Honda Motors Ltd. v. Shree Assuramji Scooters, 2006(32) PTC 117 (Delhi); Time Incorporated v. Lokesh Srivastava, 2005(30) PTC 3.

Section 43(b) of the Information Technology Act, 2000 provides compensation and imposes a liability to pay damages by way of compensation if any person without permission downloads, copies or extracts any data; computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable medium. Section 43 covers two issues relating to 'Data Protection and Privacy' i.e. Unauthorised access to computer system and unauthorised downloading/copying of data.

6.16.3 Copyright and Digital Music

The rapid Increase of the internet has made it possible to transfer huge data of all types over the internet in a simple and cost effective way. Further compression technology has also played very important role in transferring data at fast speed and in less time.

In *A& M Records Inc. v. Napster Inc.*, [176] also known as Napster's case is considered to be the landmark first case where legality of digital music sharing over the internet was questioned. Napster, on the internet had changed the way people listen to music. People could download free software from defendant's website and this software lets them share music in the form of MP3 files. Basically Napster developed a software called Napster's Music Share Software, which is available free of charge from Napster's Internet site, and Napster's network server. It facilitated the transmission of MP3 files between and among its users, through peer-to-peer (P2P) file sharing, Napster allowed its users to:

(1) Store MP3 music files on individual computer hard drives available for copyright by other Napster users;

(2) search for MP3 music files stored on other users' computers;

(3) Transfer exact copies of the contents of other users' MP3 files from one computer to another via the Internet.

[176] 114 F. Supp 2d 896 (N.D. Cal 2000)

Napster became the rage among music fans particularly in Colleges and universities around USA. The use of Napster's site was so high that several colleges had to ban it from their networks not because it was illegal but because its heavy usage was taking up enormous amounts of bandwidth. For the young company there could hardly be any better news.

There was just one little problem. Recording companies that produce the music in the first place have copyrights on them and what Napster started doing was questionable and illegal. It is not that Napster was unaware of the possible legal problem but it was hoping its new technology would let it survive in the courtroom by using a "fair use" defense against copyright infringement charges since nobody sold the music to anyone else but merely distributed it for free. Therefore, Napster was hoping to strike a deal with the recording companies and actually work with them rather than fight with them.

However this did not happen. The Recording Industry Association of America (RIM) sued Napster for copyright violation. A complaint was filed against Napster for injunction as he was a contributory and vicarious copyright infringer.

Napster raised 'fair use' defense which includes uses for such purposes as criticism, comment, news reporting, teaching (including multiple copies for classroom), scholarship, or research. It is important to note that if a use is fair then it is not an infringement of copyright. It identified three specific uses in practice:

1. Sampling, where users make temporary copies of a work before purchasing;

2. space-shifting, where users access a sound recording through the Napster system that they already own in audio CD format; and

3. Permissive distribution of recordings by both new and established artistes.

The Court applied the following factors to decide whether fair doctrine can be applied:

1. The purpose and character of the use;

2. The nature of copyrighted work;

3. The amount and substantiality of the portion used in relation to the work as a whole; and

4. The effect of the use upon the potential market for the work or the value of the work.

The court held that Napster users are not fair users because:

1. Downloading MP3 files does not transform the copyrighted work;

2. Copyrighted musical compositions and sound recordings are creative in nature and thus need copyright protection;

3. Users engage in wholesale copying of copyrighted work because files transfer necessarily involves copying the entirety of the copyrighted work;

4. Harms the market in at least two ways: it reduces audio CD sales among college students and it raises barriers to plaintiff's entry into the market for the digital downloading of music.

On July 26, 2000, the District Court for the Northern District of California granted plaintiffs a preliminary injunction, thus prevented defendant Napster from engaging in, or facilitating, or distributing plaintiff's copyrighted musical compositions and sound recordings, without express permission of the right owners.

The Court held that a majority of Napster users use the service to download and upload copyrighted music and by doing that, it constitutes direct infringement of plaintiff's musical compositions, recordings. Regarding contributing copyright infringement, the Court held that: the record clearly shows that Napster had actually knowledge that specific infringing material was available using its system. That it could block access to the infringing material and but it failed to remove the material.

Therefore, it is liable for copyright infringement. Further the District Court, by an order, imposed an obligation: on the record company to notify

Napster of specific infringing files; and on Napster to constantly search its index and block all such particular files.

The record companies appealed but this order was upheld and it was reaffirmed that the plaintiffs were supposed to provide notice to Napster of its copyrighted music files before Napster was to prevent access to such objectionable content. That means that Napster still has to remove copyrighted material whenever it was made aware of its presence on its network. As Napster was unable to do this therefore, it was left with no option but to shut down its service in July 2001.

6.16.4 Rights of reproduction and Database

A database is a collection of data in cyberspace, which is organized so that its contents can easily be accessed, managed and updated. It is important to note that reproduction rights are equally affected if a copyright material of the author is reproduced in an electronic form without his consent and made part of a database. In *New York Times Co. v. Tasin*,[177] there was an agreement between six freelance authors and publishers whereby the articles of authors were to be published in three print periodicals. However, without the freelancers consent, two computer database companies placed copies of the freelancers' articles, along with all other articles from the periodicals in which the freelancers' work appeared, into three databases. The freelance authors' complaint alleged that their copyrights had been infringed by the inclusion of their articles in the databases. The publishers, in response, relied on the privilege of reproduction and distribution accorded them by Section 20l(c) of Digital Millennium Copyright Act, l998.

The US Supreme Court held that the Electronic Publishers infringed the author's copyrights by reproducing and distributing the articles in a manner not authorized by the authors and not privileged by Section 20l(c). It was further held that even the Print Publishers infringed the authors'

[177] 533 U.S. 483(2001)

copyrights by authorizing the Electronic Publishers to place the articles in the Databases and by aiding the Electronic Publishers in that endeavour.

In *Kelly v. Arriba Soft Corp.*,[178] the plaintiff, Leslie Kelly, a professional photographer had copyrighted many of his images of the American West. Some of these images were located on Kelly's website or other websites with which Kelly had license agreement. The defendant, Arriba Soft Corporation operated an internet search engine that displayed its results in the form of small pictures rather than the more usual form of text. Arriba maintained its database of pictures by copying images from other websites including plaintiff's website. By clicking on one of these small pictures, called thumbnails, the user could view a large version of that same picture within the context of the Arriba web page.

Subsequently plaintiff, Kelly discovered that his photographs were part of Arriba's search engine database, he filed a suit for copyright infringement. The District Court found that plaintiff; Kelly had established a prima facie case of copyright infringement based on Arriba's unauthorized reproduction and display of Kelly's works, but that this reproduction and display constituted a non-infringing fair use under Section 107 of the Digital Millennium Copyright Act 1998.

Kelly filed an appeal in the Circuit Court which held that "the creation and the use of the thumbnails in the search engine is a fair use, but the display of the larger image is a violation of Kelly's exclusive right to publicly display his works. This use of Kelly's image doesn't amount to copying them but, rather, importing them directly from Kelly's website. Therefor it cannot be copyright infringement based on reproduction of copyrighted works. Instead this use of Kelly's image infringes upon Kelly's exclusive right to display the copyrighted work publicly.

6.17 Cyber crime with Mobile and Wireless Technology

[178] 280 F. 3d 934 (9th Cir. 2002)

As it is clear that at present the mobile is so developed that it becomes somewhat equivalent to personal computer, as we can do a lot of work on our mobile phones which were earlier possible on the computers only, such as surfing, sending e-mails etc. there is also increase in the services which were available on the mobile phones such as Mobile Banking, mobile wallet and other economic transaction done over the phone through internet which is also prone to cyber crimes on the mobile. Due to the development in the mobile and wireless technology day by day, the commission of cyber crimes on the mobile is becoming a major threat along with other cyber crimes on the net.[179]

6.17.1 Types of Crimes committed through Mobile and Wireless Technologies

When a thing is made or a new invention is done or something has been explored which never earlier had been known to humans, the thing which is invented was surely with the intent to provide benefit to the mankind and for the growth and prosperity of the world. But the history tells us that most of the time anything invented, it was used for the good cause and the bad cause that is for constructive as well as destructive purposes. We can take a lot of example to understand this such as 'Nuclear Energy', when it was discovered it was not known to the scientists that its most large-scale use in the future will not be as an alternative source of energy for the benefit of mankind but in making nuclear bombs which will put question mark even on the very existence of humans, we can also take example of Internet, which was developed to facilitate the communication across the world, but we can see that it is now almost equally for beneficial activities and harmful once such as frauds, pornography, theft, hacking, harassment etc. This is the same case with Wireless Technology and The Mobile Phone system, which were also been misused a lot in illegal and destructive activities.[180]

---

[179] Ling Rich, The Mobile Connection: The Cell phone's impact on society, 2004

[180] Prof. R.K.Chaubey, *"An Introduction to Cyber Crime and Cyber law",* Kamal Law House, 2012. p. 569

Mobile telephones ore at the centre of a rapidly growing crime wave, the stolen mobile even used as a criminal 'Currency'. At the same time, the technological complexity of a phone fraud makes detection and prosecution difficult. Thus we need new law to deal with the crime related to mobile phone and problems arising therefrom.

6.17.2 Phreaking

Phreaking is a slang term coined to describe the activity of a subculture of people who study, experiment with, or exploit telephones, for the purposes of hobby or utility. The term 'phreak' may also refer to the use of various audio frequencies to manipulate a phone system. It is often considered similar, and therefore grouped in category with computer hacking. This is sometimes called the H/P culture (H for Hacking and P for Phreaking.) Most phreakers range from the ages of 12-17. Most stop after this because punishments can become more severe once the perpetrator is no longer a minor. [181]

Many Phreaking techniques can be implemented with small electronic circuits, easily made by hobbyists once the secret of their operation is known. The first circuit to generate the switching tones needed to reroute long-distance calls was nicknamed the blue box by an early phreak who had built one in a blue enclosure. Soon, other types of Phreaking circuits were given similar names. Dozens of other type of 'boxes' were invented. Modern Phreaking often involves taking advantage of companies Private Branch Exchange systems, especially those which are accessible via toll-free numbers, to make phone calls. Phreakers do not always do illegal things. In fact, they may be thought of as a hacker in the computing world Phreakers may just be interested in the telecommunication world, about the more unknown side of telephones.[182]

6.17.3 Mobile Phone Theft

---

[181] http://academickids.com/encyclopedia/index.php/Phreaking (Accessed on 17th February, 2016)

[182] *Ibid*

Increased pressure of competition in mobile telephony sector has led to competitive tariffs, which in turn have spurred telecom growth and increased teledensity. The cost of the handset is probably the main inhibiting factor at the low end of the market. Though this cost has also been falling steadily, there still is a gap between the prices in the grey market (consisting of stolen/smuggled handsets) and the legitimate market. In order to curtail the illegal grey market and protect consumer interest, some action is required to be taken to discourage this crime of handset theft.[183]

Mobile phone instrument theft is becoming a major problem in all countries and is a key driver behind city crimes and robbery. Globally this is seen as a major issue and the problem is being studied to find an effective solution. In the UK, a law (Mobile Phones Reprogramming Act 2002) has been made to curb the reprogramming of handsets. Reprogramming would make possible re-use while making it difficult to identify any theft of the handset. Other efforts are also going on, such as the establishment of a global Central Equipment Identifying Register (CEIR) at Dublin, Ireland, and a "Mobile Industry Crime Action Forum" representing Operators, Manufacturers and retailers for tackling mobile phone theft and related issues. In the European Union, data is being gathered by the UK through questionnaire responses to address the matter of mobile phone theft. These various initiatives, including responses to the questionnaire in EU, show that a number of collaborative efforts are needed to tackle the problem of mobile phone theft.[184]

Efforts need to be taken by various parties concerned, based on specific database, institutional structures, and co-operation among manufactures, Network Operators, and among Government agencies. In fact, there is a need for even collaboration among Governments to address this

[183] Preliminary Consultation Paper On Mobile Phone Theft, Telecom Regulatory Authority Of India, New Delhi, January, 2004. also available online at http://trai.gov.in/WriteReaddata/ConsultationPaper/Document/mobile%20theft%20rev.1.pdf (Accessed on 17th February, 2016)
[184] *Ibid*

matter. Based on an examination of the efforts being made internationally, it is possible to identify some of the main factors/agents that have emerged as being important for tackling mobile phone theft. In summary, these include:

1. Several countries do not hold mobile phone theft data. Database of the relevant phones which need to be tracked is an essential ingredient of any effective effort to curb the theft of mobile phones. A major effort is required to build up such a database, and co-operation of all concerned would be crucial for its effectiveness. In India, no authentic data is available regarding the number of mobile handsets stolen in a year. In those countries that have statistics on mobile phone theft, data is collected by the police, and the scale of the problem in some cases involves up to 330,000 stolen mobile phones a year.

2. There is an international market for stolen mobile phones and an acknowledgement that these phones are being exported. However, there is no hard evidence or intelligence on the import/export of stolen mobile phones. There have been no joint operations between police forces from different countries to date.

3. Reprogramming makes it difficult to identify the original phone, because through re-programming the identification number of the phone, i.e., the International Mobile Station Equipment Identity (IMEI), is altered. Reprogramming is undertaken by independent mobile phone retailers/repair shops and private individuals. However, again, there is no hard intelligence on the scale and nature of reprogramming activity.

4. Reprogramming activity is illegal in a few countries and legislation is planned or under consideration in some others.

5. There has been limited joint working across Ministries to tackle mobile phone theft to date.

6. In most countries, discussions with the mobile phone industry on addressing the problem of mobile phones have either not taken place or have

only just begun and are at an early stage. Further actions to address mobile phone theft have therefore not yet been agreed.

7. In some countries all network operators have joined the global database of stolen and lost phones whilst in others no network operators are participating in the Central Equipment Identifying Register (CEIR).

8. Discussions have either not taken place or are only just beginning. No forward actions have been agreed yet, either in terms of making the International Mobile Station Equipment Identity (IMEI) tamperproof/tamper-resistant or in enhancing mobile phone handset security in other ways.

The issue of mobile phone theft needs to be addressed through a concerted effort made globally. The more countries take action, the greater the combined impact of this action. Countries need to work together collaboratively to tackle this shared problem as lasting change can only be secured through effective multi-country co-operation, such as the process initiated among European countries. During the period when efforts are being made for such collaboration, we should begin certain efforts within our own jurisdiction and look for various possible solutions.[185]

6.17.4 Use of mobile and wireless technology in Terrorist activities

Along with other crimes one of the most dangerous applications of the wireless technologies and mobile phones is their use by the terrorists in performing their activities. With the help of these latest technologies the terrorists were keeping in contact with their peers more easily than in the past when communication is the biggest barrier in successful implementation of a plan. Now the terrorist groups around the world is well equipped with the latest technology communication gadgets such as 'Satellite Phone', the communication on which is very hard to trace. Advanced mobile technology, cooperation between international mobile communications providers and

[185]Preliminary Consultation Paper On Mobile Phone Theft, Telecom Regulatory Authority Of India, New Delhi, January, 2004. p. 4-5 also available online at http://trai.gov.in/WriteReaddata/ConsultationPaper/Document/mobile%20theft%20rev.1.pdf (Accessed on 17th February, 2016)

international financial institutions, and the lack of regulations make for a swift, cheap, mostly untraceable money transfer known as "m-payments" anywhere, anytime, by anyone with a mobile telephone. Since both terrorism and m-payments are global, the m-payment service provider, as all those monitoring terror financing, should have immediate real-time access to an integrated, closely monitored list of all individuals, organizations, businesses, and countries suspected of links to terrorists.[186]

With the use of Sim cards issued on fake addresses the terrorist can easily get in contact with their masterminds and receives instructions and after that they dispose off the Sim card and there will be no chance for the investigation agencies to trace their location once the card is destroyed. In an interrogation of a terrorist in Kashmir after a recent arrest disclose a new fact that the terrorists is now using a mobile phone as a timer device in a bomb, the boy tells the mechanism that they tied up the mobile phone to the bomb and set the mobile phone on 'Vibration Mode' and the bomb lied to the mobile is sensitive to the frequency of the vibration of the mobile, then when they want to detonate the bomb they used to call on the mobile tied to bomb (obviously the Sim used in the phone is one which earlier be issued on false identification and the number of which is not known to others) and then due to the mobile was in vibration mode so it not rings but vibrate, due to that vibration the bomb explodes. This is only an example of on what levels the latest communication techniques can be used by the terrorists in their activities.96 To understand that how efficiently these latest techniques is used by the terrorists we can take the example of most wanted terrorist for the USA, Osama Bin Laden, he used to give messages on the internet, releases his audio and video tapes and gives instructions to his subordinates on his satellite phone, even then one of the most developed country, both in economy and

[186] The flip Side - Terrorists use mobile payment systems to transfer money, Available at http://www.mgovworld.org/topstory/the-flip-side-terrorists-use-mobile-payment-systems-to-transfer-money/. (Accessed on 17th February, 2016)

information technology, USA is not able to catch him even when they tried fully and spend millions of dollars for this.[187]

6.17.5 Rechipping and cloning of mobile phones

The electronic serial number (ESN) of an analogue, or the International Mobile-Electronic Identity number (IMEI) of a digital, mobile phone is its unique identity and was originally intended to be inviolably incorporated into the phone. However, the security features which protect the number can be overcome and a new set of numbers installed. The change of identity is called 're-chipping' and can be achieved on analogue phones in a number of ways. Sometimes, the ESN can be altered directly from the keypad using supposedly secret combinations of keystrokes; in other cases, connection to a computer can allow the phone chip to be re- programmed. The software to do this is available via advertisements in specialist magazines or even available free over the Internet. Re-chipping is not illegal and was started to bypass the service providers when reconnecting a secondhand phone, replacing a faulty one or upgrading to a new phone. Once available, however, the equipment could be readily applied to give a stolen phone a new identity so it can be connected to a network, and to clone another mobile phone.[188]

A clone is an analogue mobile phone which has been programmed to impersonate one owned by a legitimate subscriber by using its ESN and telephone number (these numbers are usually obtained by interception with a 'scanner' radio, theft of a dealer's or service provider's records or directly from the impersonated phone). New types are coming to the UK from the USA and Hong Kong: 'tumbling' phones automatically seek an identity from

[187] Jim Boulden, Mobiles used in high-tech terror, CNN, Apr 4, 2004 http://www.cnn.com/2004/TECH/04/04/mobile.terror/index.html. (Accessed on 17th February, 2016)

[188] "mobile telephone crime" available at http://www.parliament.uk/documents/post/pn064.pdf (Accessed on 17th February, 2016)

a preprogrammed list, and the most recent 'magic' phones act as their own scanners copying identities from nearby phones in use.[189]

Mobile cloning is copying the identity of one mobile telephone to another mobile telephone Mobile cloning is also known as cell phone piracy and has been taking place throughout the world since decades. Mobile phones have become a major part of our everyday life. On the one hand, India's mobile phone market has grown rapidly in the last decade on the back of falling phone tariffs and handset prices, making it one of the fastest growing markets globally. On the other the number of mobile phone subscribers is exceeding that of fixed-line users.[190]

Today millions of mobile phones users, be it Global System for Mobile communication (GSM) or Code Division Multiple Access (CDMA), run the risk of having their phones cloned. And the worst part is that there isn't much that you can do to prevent this. Such crime first came to light in India in January, 2005 when the Delhi police arrested a person with 20 cell phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally where ii he cloned CDMA based phones. He used software for the cloning and provided cheap international calls to Indian immigrants in west Asia. A similar racket came to light in Mumbai resulting in the arrest of four mobile dealers. Each year, the mobile phone industry loses millions of dollars in revenue because of the criminal actions of persons who are able to reconfigure mobile phones so that their calls are billed to other phones owned by innocent third persons. Often these cloned phones are used to place hundreds of calls, often long distance, even to foreign countries, resulting in thousands of dollars in air time and long distance charges. Cellular telephone companies do not require their customers to pay for any charges illegally made to their account, no matter how great the cost. But some portion of the cost of

[189] Duggal Pawan, Mobile Law, Universal Law Publishing Co. Pvt. Ltd. 2nd Edition available at https://pavanduggalonmobilelaw.wordpress.com/kinds-of-mobile-crimes/ (Accessed on 18th February,2016)

[190] http://articles.economictimes.indiatimes.com/2005-05-18/news/27482396_1_phone-number-sim-subscriber (Accessed on 18th February,2016)

these illegal telephone calls is passed along to cellular telephone consumers as a whole. Many criminals use cloned cellular telephones for illegal activities, because their calls are not billed to them, and are therefore much more difficult to trace. This phenomenon is especially prevalent in drug crimes. Drug dealers need to be in constant contact with their sources of supply and their confederates on the streets. Traffickers acquire cloned phones at a minimum cost, make dozens of calls, and then throw the phone away after as little 'as a day' use. In the same way, criminals who pose a threat to our national security, such as terrorists, have been known to use cloned phones to thwart law enforcement efforts aimed at tracking their whereabouts.[191]

6.17.6 SMS spoofing

SMS spoofing is like e-mail spoofing, which looks to originate from your acquainted number but in reality it is spoofed, and send from some evil minded individual. We can take this by an example. Suppose if a woman receive a Short Messaging Service (SMS) in her cellphone in the middle of a night from the mobile of her spouse asking her to bring cash as he has met with an accident. The chances are that she would check the mobile number and if she confirms that the cell is her husband's then she would rush out with cash. If this could be the response then the chances are that she is not aware of "Mobile Spoofing". Using web-based software, a cyber criminal could send anyone a message from any person's cell without even touching his mobile and no cellular service provider can say that it was a spoofed or faked one.[192]

---

[191] What is mobile phone cloning?, Laxmi Devi, India Times News Network http://articles.economictimes.indiatimes.com/2005-05-18/news/27482396_1_phone-number-sim-subscriber (Accessed on 18th February, 2016)

[192] The new phony crime: SMS spoofing, PTI, Jul 11, 2004 http://timesofindia.indiatimes.com/The-new-phony-crime-SMS-spoofing/articleshow/773923.cms (Accessed on 18th February, 2016)