MAPPING CYBER CRIMES AGAINST WOMEN IN INDIA

Dr. Shalini Kashmiria, (Ph.D Business Law)
Lecturer Guest Faculty, Department of Laws,
Himachal Pradesh University, Shimla-5, India

ABSTRACT

THE Delhi metro railway station CCTV footage incidence dated 8th July 2013, is the knee jerking example of cyber victimization of women in India and a big question mark on nations law and order situation. Being a victim of cyber crime is the most traumatic experience for a women posing major threat to her security. Moreover with the advent of information technology and internet, cyber crimes with the all the benefits of anonymity, reliability and convenience have become a global phenomenon. As per United States report on Internet and Computing Trends, Indians are the second largest sharers of personal information over the internet after Saudi-Arabians. With increasing popularity of chat rooms and vulnerability of personnel data to criminal access, women in India have become soft targets of variety of cyber crimes such as pornography, sexual defamation, morphing, spoofing etc.With the objective of protection and promotion of e-commerce, Government of India enacted the Information Technology Act 2000, but in terms of computer socializing communication and cyber crimes, this act is a mere gap filler.

This paper is an attempt to highlight cyber crimes against women in India which is a completely new phenomenon. To make the paper effective, a comparative analysis has been done between the cyber laws regulating cyber crimes in India, United Kingdom and United States of America. Secondary data source has been used for data collection and the research methodology adopted is doctrinal. The study discusses in detail the various crimes against women and the legal framework regulating these crimes in India. Finally the study provides with appropriate suggestions where necessary.

Key words: Cyber crimes, Women, Pornography, Sexual Defamation, Information Technology Act, 2000.

Introduction

THE Delhi metro railway station CCTV footage incidence dated 8th July 2013, is the knee jerking example of cyber victimization of women in India and a big question mark on nations

law and order situation. Being a victim of cyber crime is the most traumatic experience for a women posing major threat to her security. Moreover with the advent of information technology and internet, cyber crimes with the all the benefits of anonymity, reliability and convenience have become a global phenomenon. As per United States report on Internet and Computing Trends, Indians are the second largest sharers of personal information over the internet after Saudi-Arabians. With increasing popularity of chat rooms and vulnerability of personnel data to criminal access, women in India have become soft targets of variety of cyber crimes such as pornography, sexual defamation, morphing, spoofing etc.With the objective of protection and promotion of e-commerce, Government of India enacted the Information Technology Act 2000, but in terms of computer socializing communication and cyber crimes, this act is a mere gap filler.

This paper is an attempt to highlight cyber crimes against women in India which is a completely new phenomenon. To make the paper effective, a comparative analysis has been done between the cyber laws regulating cyber crimes in India, United Kingdom and United States of America. Secondary data source has been used for data collection and the research methodology adopted is doctrinal. The study discusses in detail the various crimes against women and the legal framework regulating these crimes in India. Finally the study provides with appropriate suggestions where necessary.

Relationship between Cyberspace and Internet

Cyber space is short hand for the web of consumer electronics, computers and communication networks that interconnect the world. The term first appeared in William Gibsons science fiction 'Neuromancer' published in 1982. This cyber space is "the total interconnectedness" of human beings through computers and telecommunications, without regard to the physical geography. On the other hand internet was cloned from the word "interconnection" and "network". Internet is the internetwork of hundreds of connecting networks made up of different types of computers all over the world that can share messages and information with each other.[1]The internet is currently the biggest network for linking computers, but cyber space as a concept, is independent of the internet. Cyberspace communication began before the Internet and World Wide Web, and

[1] Hemant Goel, *Law and Emerging Technology (Cyber Law)*, New Era Publication, Haryana, 2007.

cyber space interaction and communication will continue to take place after the internet is no longer the network of choice. [2]

Cyber Crime and its Classification

In layman language computer wrongs includes both civil wrongs and crimes. 'Cyber Crime' is used in generic sense which tends to cover all kinds of civil and criminal wrongs related to computers. It would include any tort or civil wrong done which relates to a computer as well as any criminal activity relatable to a computer. [3]

Based on commission of crime, cyber crimes can be broadly classified in three categories.

- **Cyber Crimes against person:** There are committed against individuals disturbing him physically or mentally. Such offences include various crimes such as transmission of child pornography, illegal accesses with computer as a medium, e-mail or cyber stalking, dissemination of obscene or defamatory material etc.
- **Cyber Crimes against all forms of property:** These crimes are committed to affect the property or a person by any electronic media causing damage to him. This includes unauthorized computer intervention through cyberspace, computer vandalism and the transmission of harmful programs and/or illegal possession of computerized information etc.
- **Cybercrimes against State or Society:** Cyber terrorism is one distinct kind of criminal activity falling under this category and turns out to be very destructive when an individual "cracks" into a website maintained by the Government or its Defense Department. These crimes include trafficking, financial crimes, sale of illegal articles, on-line gambling etc

Synoptic view of classification of cyber crimes

	Crimes against person or individuals		Crimes against property		Crimes against State or Society
1	Harassment via email	1	Computer vandalism	1	Intention to extract secret informationfrom computer system
2	Cyber Stalking	2	Virus transmission	2	Cyber terrorism
3	Dissemination of obscene material	3	Denial of service attacks	3	Distribution of private software

[2] Indira Gandhi National Open University, "Cyber Space Technology and Social Issues", *Indira Gandhi National Open University School of Law*, Vol. MIR-011, No.2, October 2008, pp. 42-43.
[3] Indira Gandhi National Open University, "Regulation of Cyber Space", '*Indira Gandhi National Open University School of Law*, Vol. MIR-012, No.3, October 2008 at 6.

4	Defamation	4	Unauthorized access over computer system	4	Polluting youth through indecent exposure
5	Unauthorized control/access over computer system	5	Intellectual property crime	5	Illegal human trafficking online.
6	Indecent exposure	6	Internet time theft	6	Financial scams and frauds
7	e-mail spoofing	7	Sale of illegal articles	7	Sale of illegal articles
8	Pornography including (Child pornography)	8	Hacking	8	Online gambling

Source: Adapted from

* Farooq Ahmad, *Cyber Law in India*, New Era Law Publications, New Delhi, 2008.
* Vishwanath Paranjape, *Cyber Crimes and Law*, Central Law Agency, Allahabad, 2010.
*Aparna Viswanathan, *Cyber Law: Indian and International Prespectives*,Lexis Nexis Buttersworths,Nagpur,2012.

Cyber protection to women in United Kingdom

It is to be noted that gender sensitive cyber crime took a lead role in the late 90,s in United Kingdom when stalking of female celebrities over the internet became a major problem. In United Kingdom cyber harassment and offences against women are covered by the protection of harassment act1997. Unlike United States of America United Kingdom does not have women specific regulations to cover up cyber offences originating from domestic violence unauthorized access to computer resource and hacking. All these offences are regulated by the Computer Misuse Act, 1990 which is applicable to both men and women. This act penalizes three kinds of offences namely;

- Unauthorized access to computer material or to enable any such access to secure unauthorized access.,
- Intention to create further menace with such unauthorized access.,
- Unauthorized modification of computer material.

The penalties for the offences mentioned above include imprisonment for a term and 12 months and a monetary fine not exceeding statutory maximum or both. [4].

Cyber protection to women in United States of America

Studies have shown that United States of America has the highest number of cyber specific legislations. The U.S Communication and Decency Act, 1996 differentiates child pornography and have both federal and state laws to regulate cyber crimes. Similarly Computer Fraud and Abuse Act, 1860 regulates the offence of hacking which is again encompassed by Title 18, USC 1030 which defines it as an "unauthorized access".

[4] (-),'Cyber Space Regulation for Protecting Women in UK',(2013)www.igi-global.com,*at* http://www.igi-global.com/chaptr/cyber-space-regulation-protecting-women/55535(last accessed 15january 2014)

Section 223(a) Title 47, USC makes it an offence to use a telecommunication device in interstate or foreign communications to:

- Make, create solicit and initiate the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy or indecent, with the intent to annoy, abuse, threaten or harass another person.,
- Make, create solicit and initiate the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene knowing that the recipient of such communication is under 18yearsof age.,
- Make a telephone call or utilize a telecommunication device without disclosing the identity to annoy , abuse, threaten or harass any person at the called number or wo receives the communication.,
- Make or cause the telephone of another repeatedly or continuously to ring with intent to harass any person at the called number.,&
- Knowingly permit any telecommunication facility under his or her control to be used to commit any of the previously listed activities.

The penalties for these offences include fines, imprisonment or up to 2 years or both[5].

The Information Technology Act, 2000

The Ministry of Information Technology was formed in 1999, burdened with the enormous duty of making India IT superpower by 2008. In less than a year, India witnessed the enactment of its first statute relating to Information technology on the pattern of Model Law on Electronic Commerce, 1996, adopted by the United Nation commission on International Trade law (UNCITRAL). The electronic transaction Act of 1998 Of Singapore also significantly guided the framing of the Act. The Information Technology Act, 2000 was passed by the parliament on May 15, 2000, approved by the President on June 9, 2000 and notified to come into force on October 17, 2000.The Act, seeks to protect this advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and forming regulatory authorities. [6] The Information Technology Act, 2000 initially consisted of XIII Chapters & 4 Schedules and 94 Sections. Two schedules have been deleted by the Information Technology (Amendment) Act, 2008. At present it has 2 Schedules. Chapters IX & XI covers up offences and penalties. Studies have shown that the United States and United Kingdom are the two traditional giants who are giving a tough defiance to the Silicon onslaught. United States of

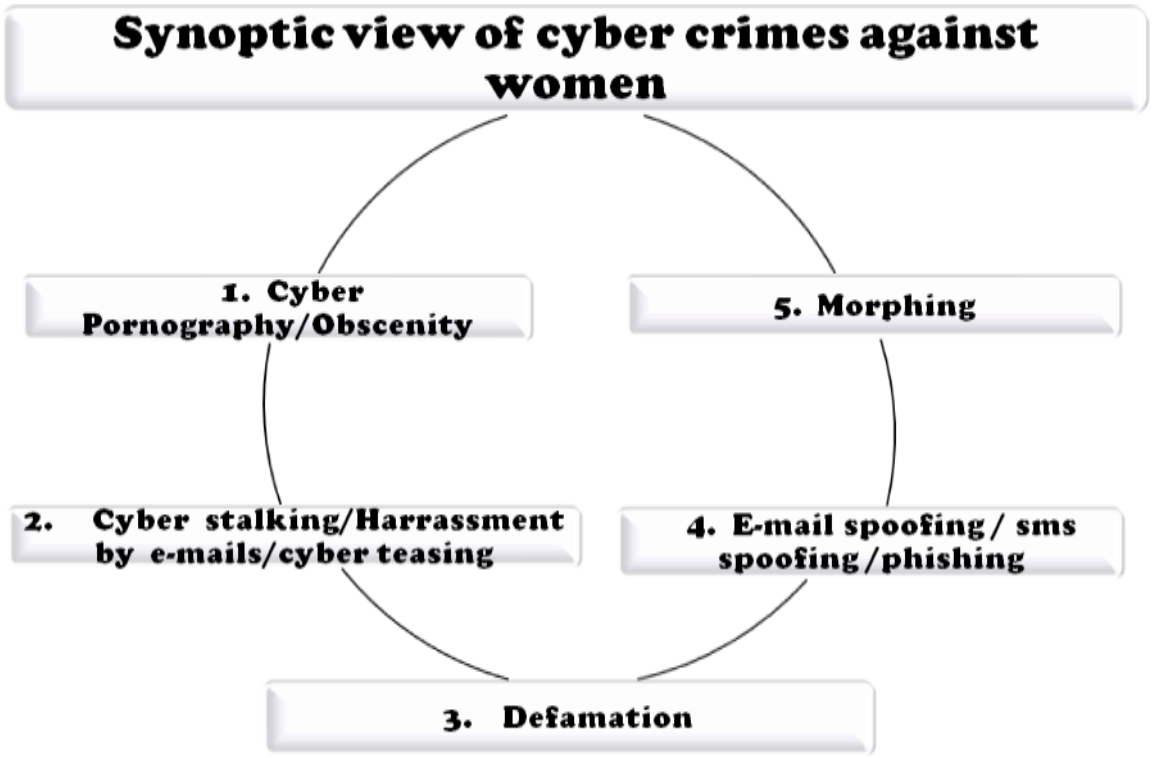
[5] Shobna Jeet, "Cyber Crimes against women in India:Information Technology Act,2000,"*Elixir Criminal Law* 47 (2012) 8891-8895.
[6] K.P. Malik, *Computer and Information Technology Law*, Allahabad Law Agency, Haryana, 2010.

America bags the highest number of cyber specific legislations followed by UK having technology specific legislation apart from having cyber laws. The Communications Decency Act, 1996 of United States of America differentiates between pornography and child pornography. Similar differentiations have been provided under the United Kingdom Obscene Publications act, 1959. Although no such differentiation exists under Section 292 of Indian Penal Code, 1860 but the IT (Amendment) Act, 2008 has made child pornography as specific offence under Section 67-B[7].

Information Technology Act, 2000 and Cyber Crimes against Women

The Information Technology Act, 2000 nor defines 'cyber crimes' neither uses this expression, but only provides the definition of and punishment for certain offences. Thus two kinds of definition of cyber crimes can be given. In narrow terms cyber crime consists of only those offences which are mentioned under the Information Technology Act,2000, whereas broadly speaking cyber crime can be said to be an act of omission, commission or committed on or through or with the help of internet, whether committed directly or indirectly and which is prohibited by any law for which punishment corporal or monetary is provided. In this context it can be concluded that Information Technology Act, 2000 provides punishment for only certain offences and is not exhaustive of all cyber crimes.[8]

[7] *ibid*.
[8] *supra* note7,at p.38



Source: Adopted from

S.K.Verma and Raman Mittal, *Legal Dimensions of Cyber Crime*, Indian Law Institute, New Delhi, 2004.

- *Cyber pornography/ Obscenity/ Sexual defamation*: Of all the crimes committed on the internet pornography appears to be the one having serious moral implications. Being a victim of pornography is the most traumatic experience for a woman. In layman language pornography refers to predominantly sexually explicit material, lascivious in nature intended primarily for the purpose of arousal of sex desires or erotic activity over the internet and includes pornographic websites, e- magazines containing porn stuff which could be downloaded from the internet, transferrable porn pictures, photos writings etc.[9]Because of the advantage of lack of territorial restrictions, anonymity and fastest means of communication pornographic materials can be reproduced more quickly and cheaply on new media like hard disks, floppy discs and CD-ROMs. Apart from still pictures and images, full motion video clips and complete movies are also available. Another great disadvantage with a media like this is its easy availability and accessibility to children who can now log on to pornographic web-sites from their own houses in relative anonymity and the social and legal deterrents associated with physically purchasing an adult magazine from the stand are no

[9] *supra* note3,pp. 237-238

longer present pornography industry is contributing approximately $ 20 billion annually to the global economy.[10]For example In India Videsh Sanchar Nigam Limited (VSNL) and number of other internet service providers such as Reliance, Vodafone, Airtel , cyber cafes, online portals etc provides for various kinds of internet schemes without restrictions on the nature of persons permitted to avail these services. Moreover the social websites like Facebook , Twitter, Watsup, Orkut, free music downloading sites etc do not check the kind of material that is being uploaded and downloaded. They do not have any parameter to differentiate between what we call as an art or pornography. What is more shocking is children (between 8-16 years) indulgence in viewing porn sites. Approximately twenty six popular children's characters such as Pokemon, Action Man, My Little pony reveals thousands of links to porn sites.[11].

The most embarrassing aspect of pornography industry is the child pornography. The Air Force Bal Bharti , Delhi Cyber Pornographic Case(2001) and the Bombay Swiss Couple Case (2003) are the leading examples in this context.[12]It is to be noted that Traditional law of obscenity is contained under sections 292-293 of Indian Penal Code, 1860.Section 292[13] deals with the sale of obscene books and section 293[14] provides punishment to person dealing in cyber pornography that is accessible to person under twenty years of age with imprisonment up to three years and fine upto two thousand rupees on first conviction and with imprisonment up to seven years and fine up to five thousand rupees on second or subsequent convictions. The IT Act, 2000 was deficient in dealing with obscenity and consist of a single section67 dealing with the crime. IT (Amendment) Act, 2008amended section 67. The combined effect of sections 66-E, 67, 67-A and 67-B obscenity has been brought under the legal regime and child pornography has been separated from mainstream pornography.[15] Section 67[16] provides that whosoever publishes or transmits obscene material in electronic form shall on first conviction be punished with imprisonment up to three years and fine which may extend up to five lakh rupees and on second or subsequent convictions, imprisonment up to five years and fine up to ten lakh rupees. Section 67-A[17]

[10] Talat Fatima, *Cyber Crime*, Eastern Book Company, Lucknow, 2011.
[11] *supra* note13, at p.238.
[12] Vishwanath Paranjape, *Cyber Crimes and Law*,Central Law Agency, Allahabad, 2010.
[13] Section 292 of the *Indian Penal Code*, 1860.
[14] Section 293 of the *Indian Penal Code*, 1860.
[15] *supra* note 15, pp.126-127
[16] Section 67 of the *Information Technology (Amendment) Act*, 2008(10 of 2009).
[17] Section 32 of the *Information Technology (Amendment) Act*, 2008(10 of 2009).

deals with mainstream pornography and provides punishment for publishing or transmitting of material containing sexually explicit act, etc in electronic form with imprisonment up to five years and fine up to ten lakh rupees on first conviction and with imprisonment up to seven years and fine up to ten lakh rupees on second and subsequent convictions. Section 67-B[18] is related to child pornography. This section provides punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form or creates text , digital images, collects, seeks , browses, downloads , advertises, promotes, exchanges or distributes material in electronic form depicting children in sexually explicit act or entices or induces children for online relationship with one or more children or facilitates abusing children online with imprisonment up to five years and fine up to ten lakh rupees on first conviction and imprisonment up to seven years and fine upto ten lakh rupees on second or subsequent conviction. Other acts having an impact on cyber pornography are indecent representation of Women's Act, 1986 and Young Persons (Harmful Publication) Act, 1950.[19]

- *Cyber stalking / Harassment by e- mails/Cyber teasing/Cyber bullying/Cyber flirting:* According to Oxford Dictionary Stalking means "pursuing stealthily".[20] In simple terms, it refers to extension of physical form of stalking where electronic medium such as computer, internet, e-mail or any other electronic device is used to pursue, harass or contact another person in an unsolicited manner. I generally involve harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's house or place of business, making harassing phone calls, leaving written messages or objects or vandalizing a person's property.[21]These crimes are done with the sole motive of gaining control over the victim and thus targets women in most of the cases. Domestic violence victims are one of the most vulnerable groups to traditional stalking. So it's no surprise they are vulnerable to cyber stalking as well. It's a myth that if women "just leave" they will be okay. Cyber stalking is a way to continue to maintain rigid control and in still fear into a domestic partner, even when she has already left the relationship.

  Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & Internet safety. Their main targets are the mostly females, children, emotionally

[18] Section 32 of the *Information Technology (Amendment) Act*, 2008(10 of 2009).
[19] *supra* note 3, at p.240.
[20] *supra* note 17, at p.30.
[21] *supra* note 3, at p.240.

weak or unstable, etc. It is believed that Over 75% of the victims are female. The motives behind cyber stalking have been divided in to four reasons, namely, for sexual harassment, for obsession for love, for revenge and hate and for ego. Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. Cyber stalkers target and harass their victims via websites, chat rooms

Cyber stalking can be categorised as follows

- On-line harassment and stalking that continues over the internet.
- On-line harassment and stalking that is carried out off-line. Hereunder stalker attempts to trace the telephone number or residential address of the target.

This crime is committed by collecting all the necessary personal information about the target such as his/her name, age, family background, residential address, telephone number, working place , daily retinue etc and put this information on social websites , porn sites pretending as if the victim is himself/herself posting this information and invite people to contact him/her. Generally stalkers use indecent language to lure people. Famous incident to quote is Manish Kathuria case. The recent being the case of Manish Kathuria who was recently arrested by the New Delhi Police. He was stalking an Indian lady, Ms Ritu Kohli by illegally chatting on the Web site MIRC using her name. He used obscene and obnoxious language, and distributed her residence telephone number, inviting people to chat with her on the phone. As a result of which, Ritu kept getting obscene calls from everywhere, and people promptly talked dirty with her. In a state of shock, she called the Delhi police and reported the matter. For once, the police department did not waste time swinging into action, traced the culprit and slammed a case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli.[22]

It is to be noted that under IT Act, 2000 there is not even a single section exclusively dealing with cyber stalking. Herein computer is merely used as a tool for committing the offence in the sense that the offender might be causing alarm by sending messages via internet to the victim, threatening injury to him, his property or reputation. Section 503[23] Indian Penal

[22] *supra* note 17, at p. 31.
[23] Section 503 of the *Indian Penal Code*, 1860.

Code, 1860 deals the crime of criminal intimidation and provides that whosoever threatens another with any injury to his person, property or reputation or the person, property or reputation of anyone in whom the person is interested or with the intent to cause alarm to that person or to cause that person to do any act which he is not legally bound to do or to omit to do any act which he is legally entitled to do , as the means of avoiding the execution of such threat. Cyber stalking is simply criminal intimidation.[24]

- *Cyber defamation:* Under Indian legal system, defamation is tortuous liability as well as crime and refers to an act of imputing any person with the intent to lower his reputation in the eyes of right thinking person's of society or cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation s nothing else but method of defaming someone with the help of computer or internet.ua[25]On-line mode of defamation is more dangerous than off-line mode both quantitatively and qualitatively. With a single click a defamatory statement/ message reaches numerous people and qualitatively defamatory message can be posted as per convenience in a news group such as the lawyers' group. Worst example of cyber defamation is corporate cyber smear which a false of disparaging rumour regarding a company, its management, its stock which is posted on internet. In maximum cases it has been noticed that the purpose of sending defamatory e-mails to the victim is to satisfy the lust of the criminal which may be either for money or satisfying his illegal or unlawful demand or for avenging rivalry and must be published. [26]

  Section 499[27] 0f the India Penal Code, 1860 read with section 4[28] of IT Act, 2000 deals with cyber defamation. Section 499 provides that anyone by words intended to be read publishes any imputation concerning any person intending to harm or knowing or having reason to believe that such imputation will harm, the reputation of such person is said, subject to exceptions provided in the section to defame a person. Section 4 of IT Act, 2000 give legal recognition to electronic records. Therefore if any defamatory information is posted on the internet either through e-mails or chat rooms or chat boards, such posting would be covered under the section 499 requirement of publication and would amount to cyber defamation.[29]

[24] *supra* note 3, pp.240-241.
[25] *supra* note 17, pp.34-35.
[26] *id.*, pp.233-235.
[27] Section 499 of the *Indian Penal Code,* 1860.
[28] Section 4 of the *Information Technology Act,* 2000.
[29] *supra* note 3, pp.234-234.

- *E-mail spoofing/ sms spoofing/ phishing*: A spoofed e-mail may be said to be one, which misrepresents its origin. This is a technique which uses the spamming technique with latest technological advancements. Falsification of name / or e-mail address of the originator of the mail is usually done by e-mail spoofing also called as phishing. Anti spamming Act, 2001 provides penalty for intentionally initiating the transmission of bulk of unsolicited e-mails with the knowledge that the message falsifies Internet Domain, header information, date or time stamp, originating e-mail address, or other identifier. This Act is supported by Unsolicited Commercial E-mail Act, 2001.Hereunder the perpetrators deceive the victim by putting him under the belief that the message received by him is from an authentic source.

  Internet Spoofing is a technique which is used for the purpose of gaining unauthorised access to computer, whereby the intruder sends a message to a computer with an Internet Protocol (IP) address indicating that the message is coming from a trusted port. This is done by link alteration by adding hackers address before the actual address in any e-mail or page that has a request going back to the original site.SMS spoofing is made possible when several mobile operators integrated their network communication within the internet so that anybody could send SMS from the internet using forms at the websites of mobile operators or even through e-mail.[30]To take an example the criminals set up bogus Automated Teller Machines (ATM) in public places or shopping malls asking the user to enter their PIN codes. Once the card gets into the machine, it would malfunction and return the card to the owner. Thus the criminal gets enough information to copy the victim's card and uses its duplicate to draw money from the ATM.[31]

  In India there is no legal provision dealing with spoofing as it is not an independent crime and is used as *modus operandi* to commit other crime. The faulty SMS induces the victim to act accordingly and thus, making him pray to some other regular crime.[32]In a sense it can be considered a variation of digital forgery where one attempts to impersonate by sending a false electronic record which though purported to have been made /or signed by the latter person, but in fact it is not so. As the nature of this crime resembles with that of section 463 of Indian penal Code, 1860 related to crime of forgery. Examples of spoofed e-mails which are quite common in day to day affairs

[30] *supra* note 15, pp.222-225.
[31] *supra* note 17,at p.41.
[32] *id*., pp.224-225.

- Fake e-mail from a system administrator requesting the users to change their password to a specified string and threatening to suspend their account if they ignore it.
- E-mail claiming to be from a person with authority asking the customers to send a copy of their password or other sensitive information.
- E-mail from a fake credit card company asking for personal details, credit card number and password to access online account.[33]

- *Morphing/ Hacking*: Morphing is editing the original picture by unauthorised users or fake identity. Fake users take help of social websites to download female's pictures and re-post/upload them on different websites by creating fake profiles after editing it. This amounts to violation of I.T Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC also. Section 43[34]of IT Act,2000 deals with computer sabotage and provides that if any person without permission of owner/person in charge of computer does any of the following act such as unauthorized access to any computer, system, network, or data stored in computer, system or network, disrupts any computer, system or network, denial of any access to any person legally authorized to access, provides assistance to any person or facilitates access to any computer, system or network in contravention of provisions of Act/regulation/rules made there under, charges service availed by a person to the account of another person is liable to pay damages by way of compensation to the person so affected an amount which may extend rupees one crore..Section 66A[35] provides punishment for sending offensive messages through communication service, etc. According to this section whoever knowingly send by means of computer resource or a communication device grossly offensive message, false information, any electronic mail message for the purpose of causing annoyance, inconvenience, danger, obstruction etc will be punishable with imprisonment up to 3 years and with fine. Section 66 C[36] deals with identity theft and provides that whosoever dishonestly or fraudulently making use of electronic signature, password or any other unique identification feature of any other person will be punishment with imprisonment upto 3 years and fine up rupees 1 lakh or both. Section 66D[37] deals cheating by personation and provides that whosoever does

[33] *supra* note 3, at p.260.
[34] Section 43 of the *Information Technology Act*, 2000 as amended by Section 21 of the *Information Technology (Amendment) Act*, 2008.
[35] Section 66A inserted by the *Information Technology (Amendment) Act*, 2008.
[36] Section 66C inserted by the *Information Technology (Amendment) Act*, 2008.
[37] Section 66D inserted by the *Information Technology (Amendment) Act*, 2008.

cheating by personation by means of any communication device or computer resource, shall be punishable with imprisonment upto 3 years and fine of Rs. 1 lakh or both.

Section 66 E[38] deals with (Privacy violation) and provides that whosoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent shall be punishable with imprisonment upto 3 years and fine of Rs. 2 lakh or both.

Conclusion

No doubt Information technology act, 2000 has been passed by the Indian Parliament with the objective to facilitate to prevent 'Cyber Crimes'. But the reality is that it is not a separate code for electronic transactions. It has only a gap filling role and it does not provide a separate legal regime and does not cover up the issues that have cropped up by the use of Internet especially cyber stalking, morphing and e-mail spoofing. In a sense this Act and its latest amendment of 2008 have the following drawbacks namely there exists no statutory definition explaining the term cyber crime in any law in the respective countries. The IT Act, 2000 divides computer vandalizing and computer offences in two different chapters. Chapter IX related to Penalties Compensation and Adjudication under the IT Act, 2000 is purely civil in nature but the IT (Amendment) Act, 2008 has made it punishable by providing under Section 66 for imprisonment if any of the acts mentioned under section 43 (a)—(f) are done either dishonestly or fraudulently.[39] The Communications Decency Act, 1996 of United States of America differentiates between pornography and child pornography. Similar differentiations is provided under the United Kingdom Obscene Publications Act, 1959.Although no such differentiation exists under Section 292 of Indian Penal Code, 1860 related to criminal intimidation but the IT (Amendment) Act, 2008 has made child pornography as specific offence under Section 67B. [40]Tn United States, the Computer Fraud and Abuse Act, 1986 deals with the offence of hacking under Section 1030(a)(5)(A) and defines it as an "unauthorized access". In United Kingdom, the Computer Misuse Act, 1990 although does not use the term "hacking" but it is covered under the heading "unauthorized access". In India earlier this term was used under Section 66 of the IT Act, 2000 but now been replaced by a new section as such the word "hacking" has been dropped by the IT (Amendment) Act, 2008.[41] As for as law with respect to the liability of online

[38] Section 66E inserted by the *Information Technology (Amendment) Act*, 2008.
[39] *supra* note 15,pp 453-454.
[40] *ibid*.
[41] *ibid.*

intermediaries is concerned, the United States of America shows liberal attitude towards them as compared to United Kingdom and India. [42]Cheating by personation has not been defined and it is not clear whether it refers to cheating as referred under the Indian Penal Code, 1860 as conducted by communication device or whether it is creating a new category of offence. Moreover the term fraud is neither defined under the IT Act, 2000 nor under the Indian Penal Code , 1860.It more being recognized as a mental condition under Indian Penal Code,1860.[43]Cyber Regulation Appellate Tribunal (CRAT) is one man commission with law degree as an essential qualification. On contrary IT offences involves highly complex phenomenon which is beyond the understanding of common man and requires IT expertise in the field. Indian police is not well equipped to handle cyber crimes related investigations. Moreover wide powers have been given to police by the act as anyone can be searched and arrested without warrant at any point of time in public place. Moreover Indian police is still a layman in terms of modern spying technologies. There exist many cyber crimes that can be prosecuted both under the civil and criminal procedure system. As consequence of confusion regarding civil liability, criminal liability and jurisdictional issues the justice is often delayed. Several areas of It Act, 2000 are not clear. For example, meaning of 'wrongful loss", "destroy", "attestation", "delete and hacking' has not be explained. Punishment provided under the IT Act, 2000 for various cyber crimes is very nominal and therefore must be increased so as to have deterrent effect. It is to be noted that maximum offences under the Act which are carrying penalties above 3 years imprisonment have been made cognizable but they have also been made billable offence whereas lesser offences have been made compoundable. Cyber defamation has to be defined clearly under the IT Act, 2000 which is lacking. Sections 67, 67A, 67B, and 67C does not cover any book, pamphlet, paper writing, drawing, painting, representation or figure in electronic form if there is any public good defence available with the accuse which means that if he is able to prove that such pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or other object of general concerned or if it is kept for confide religious purposes. Thus even publishers or transmitter of obscene material which is prepared in electronic form like e-books, e-magazines and blogs can avail public good defence under IT Act,

[42] *id*., at p, 457.
[43] Parkash Pamesh, 'Short Note on IT (Amendment) Act, 2008: The Centre for Internet and Society' (2011) www.cis-india.org, *at* http://www.cis-india.org/internet -governance/publications/it-act/short-note-on-amendment-act-2008 (last accessed 20 October 2012.)

2000 .[44]Act consists of single section related to liability of Network Service Provider and Breach of Privacy which is not satisfactory in terms of handling the problem.[45]Thus, we conclude that to guard again the sophisticated skills of cyber criminals, a global culture of cyber security needs to be developed which intrun required besides good policing and legislation, tough ICT based majors uniform in applications beyond jurisdiction because information and communication flow across boundaries, as such much of the traffic escapes national frontiers. In this direction the European Union has taken certain initiative in the form of European Convention on Cyber Crimes, 2001 supported by many other international organizations such as the World Intellectual Property Organization (WIPO), the Copy Right Treaty, 1996, to which many countries like United States of America, European Union and Canada are signatory. Thus India also needs certain majors like United States Internet Crime Complaints Centre (IC3) and Cyber Police in China[46] for reporting and tracing out domestic crimes on Internet. In this direction the following suggestions can be made.

Suggestions

While a lot can be said of the merits and demerits of the IT Act, 2000 …… still there is room for some improvement too and in this regard following suggestions can be made.

- Avoid furnishing personal details such as family background ,picture related to the people with whom you are socializing, your private moments etc on social websites like Facebook, Google+, Twitter, LikedIn as it can be easily misused.,
- While in hotels , restraints or changing rooms in mall , always check for two way mirror,
- Always make two kinds of online presence one for social networking and other official. Try to use dummy profile presence while using internet.,
- Need to adopt Uniform Law worldwide because Cyber crime is not only a national problem but also an international problem. There is need to adopt specific laws on jurisdiction and international co-operation following European Convention on Cyber Crime, 2001;
- We need training of law enforcing agencies and IT professionals to curb the menace;
- Maximum punishments under the Act are bailable thus there is a necessity to increase punishment so as to have deterrent effect ;

[44] Rajak Brajesh, *Pornography Law must not be tolerated*, Universal Law, New Delhi, 2011.
[45] M.Das Gupta, *Cyber Crime in India*, Eastern Law Publishers, Kolkata, 2009.
[46] Zibber Mohhuddin, 'A Paper Presented on Cyber Laws in Pakistan: A situational analysis and way forward' (2006) www.supremecourt.gov.pk, *at* http://www.supremecourt.gov.tk/ifc/article/10/5.pdf (last accessed 12 November 2011).

- Need to have strong and practicable security policy handling mobile technology and wireless technology along with computer technology and multimedia technology;

- Need of specialized cyber crimes court with expertise, in the field of information technology;

- There must be clear cut and uniform guidelines for the ISP and NSP fixing liability and accountability;

- There is need to have uniform law on cyber spamming so as to protect women and children of nation.

- Societal trauma related to cyber crime against women wherein women as victim is considered more as an accused in her own case than victim must be removed.

- Police authorities investigating the cases related to cybercrimes must not only be given IT Training but also be trained in dealing women victims psychologically.

Thus there is dire necessity of psychological up gradation of women victims which require sensitization of police authorities.