Legal Implications of Cyber Crimes on Social Networking Websites

Nikita Barman

"The surge in the use of social networking sites over the past two years, has given cyber thieves and child predators new, highly effective avenues to take advantage of unsuspecting users."

-Gordon Snow, Assistant Director of the FBI's Cyber Division

Abstract- The purpose of the research paper is to show how laws enacted under different statutes regulate cyber crimes occurring on social networking websites. Even though it appears that social media has got the world closer, there is a flipside to it. Many offenders use this vulnerable means to commit offences related to computer, computer system or computer networks.

Social Networking websites are used as a means for communication and interaction among people across the globe, be it reuniting with old ones or meeting new people. The hitch with this kind of social media involves several other aspects, rather than just meeting new people and exchange of ideas. The cyber offenders use this as a medium to commit offences related to privacy, defamation, misrepresentation of identity or cheating by personation, obscenity, sending offensive messages, cyber terrorism so on and so forth. Many people have fallen prey to these offences due to lack of awareness and overuse of these social networking websites. The fear of lagging behind in this technology race has led to the increase in the statistics of these crimes.

The researcher would want to delve into the main components of the offences relating to technology which take place on an everyday basis on these social networking websites. Also, the researcher would also want to examine the cases relating to the cyber offences happening on these social networking websites, which have got the attention of the public. To conclude the researcher would want to make observations about how law and the courts have together to worked in providing justice to the victim.

Index Terms- Social networking websites, cyber crimes, legal provisions.

I. Introduction

The internet has the ability to disseminate information and communicate almost instantaneously has caused upheaval in many facets of our lives. Concurrently, the Internet provides extremely effective tools and mechanisms for individuals and groups who seek to conduct unlawful activities. Technological advancement has given rise to criminal activities by people who are often sophisticated and expert practitioners. With the easy access to the most powerful medium of expression, the crime rate has gone up multi- folds. The Web contains many things and the most fascinating are the Web Pages, where each page is an interactive publication that includes videos, music, graphics and text. Latest technology has enhanced the possibilities of invasion into the privacy of individuals which is at a great risk as the Internet can be used to amass huge amount of data regarding people, profile it in various ways, sell it and deal with it. Making a network secure involves outsmarting intelligent, dedicated and well funded adversaries. Network security has loomed as a massive problem since there are millions of citizens using Internet for banking, shopping, filing tax returns and anything which can be done in this virtual world.

The information Technology Act, 2000 is based on the General Assembly Resolution[1] which recommended all States to give favourable consideration to the Model Law on Electronic Commerce during enactment or revision of their laws. This Act unfolds the various aspects of information technology to promote efficiency in the delivery of government services by means of reliable electronic records. Though the enactment has an international perspective, the municipal or national perspectives of information technology should not be ignored.

Social Networking Websites

Social Networking Websites is a term used to describe websites which act as a platform for interaction among people across the globe. The Oxford Dictionary defines a social network as "A dedicated website or other application which enables users to communicate with each other by posting information, comments, messages, images, etc." A Social Networking Website may be in a variety of forms such as a forum, chat room, blogs etc. through which people communicate, exchange ideas and multimedia such as pictures, videos and audios. When a user creates a profile on a particular social networking website, it allows him to share and discuss information and media with either the people on his friend list or with public at large. Social Networking relies upon users building up their own network of contacts on the sites, which in turn introduces them to new contacts. On many social networking websites it allows them to be found more easily, and for new contacts to be recommended or introduced, helping to grow the user network.[2] As the user network has increased, the risk related to the privacy of information and media which the user has uploaded has augmented. The crime rate on these networks is accelerating with addition of each user.

Cyber Crimes

[1] Resolution A/RES/51/162 adopted by the General Assembly of the United Nations on 30th January, 1997.

[2] Michael Peacock, *Drupal 7Social Networking*, PacktPublishhing, United Kingdom, 2011.

Cyber Crime can be explained as any criminal violation or an unlawful act taking place on the computer. According to the Information Technology Act, 2000, 'cyber' may be said to include a computer, computer system or a computer network. Hence, any illegal act which involves a computer, computer system or a computer network is cyber crime. The Information and Technology Act, 2000 does not explicitly define the term cyber crime. An offence is an act prohibited and made punishable by fine and/ or imprisonment.[3] So, any offence taking place on the computer can be said to be a cyber offence. When crime takes place on the Internet there is exchange of information between computers connected to a network where some computers provide information, some seek for information and there are some which provide for smooth exchanges and route the flow of information. Internet can augment criminal conduct under the following situations:

- Conduct in a manner so adversely affecting a computer such as hacking, cracking, illegal downloading of information stored on a computer, virus or a worm attack to name a few.
- Conduct affecting a person-maybe an industry, government or a private individual which could include crimes like child pornography, spamming, defamation, threats, posting a copyright material etc.

The Information Technology Act, 2000 differentiates between cyber contraventions and cyber offences. A violation of law or rule of procedure will be a contravention which may or may not be punishable with a liability to pay a penalty as the offender faces civil prosecution. However, an offence is an act prohibited and made punishable by fine and/ or imprisonment as the offender faces criminal liability.[4]Contravention can be said to be generic whereas offence is specific. The difference between the two terms is about the degree and the extent of criminal liability.

Computer Crimes can be classified into the following categories[5]:

A. Conventional crimes through computer which includes cyber defamation, digital forgery, cyber pornography, cyber stalking/ harassment, internet fraud, financial crimes, online gambling, and sale of illegal articles.
B. Crimes committed on computer networks include hacking/unauthorized access, denial of service.
C. Crimes relating to data alteration/destruction being virus/worms/Trojan horses/logic bomb, theft of internet hours, data diddling, salami attacks, steganography.
D. Crimes relating to electronic mail such as spamming/bombing, spoofing.

Cyber crimes familiar to social networking websites are cyber defamation, cyber obscenity pornography, cyber stalking, hacking, privacy infringement, internet fraud, unauthorized disruption of computer system through virus and using any person's copyright.

Cyber Defamation

According to the Black Law's Dictionary, defamation[6] can be defined as "an intentional false communication, either published or publicly spoken, that injures another's reputation or good name". Defamation includes the common law torts of libel (involving written or printed statements) and slander (involving oral statements) which can be committed via Internet medium.

Ingredients of defamation are:

i. Publication of the statement;
ii. Statement makes reference to the plaintiff;
iii. Statement is communicated to some person or persons other than the plaintiff himself;
iv. Statement reaches the plaintiff; and
v. Statement causes actual or presumed damage to the plaintiff.

The difference when defamation happens on the Internet is that the defamatory imputation is published in electronic form. The issues related to defamation on the internet include as to time of occurrence, the mode of publication, where the publication took place, i.e the jurisdiction, who will be liable for the publication of the alleged defamatory statements.

- Time of occurrence is when the process of publication is complete and when the statement reaches the plaintiff.
- The mode of publication or transmission on the internet is in electronic form which include generating, sending or receiving defamatory emails, online bulletin board messages, chat room messages, making remarks, sending or uploading pictures on social network websites etc.
- The place of publication or where the jurisdiction lies is the place where the defamatory statement is made and that place is the one in which that particular information is downloaded and not where the statement is uploaded or where the publisher's server resided. This was made apparent in *Joseph Gutnick* v. *Dow Jones & Company Inc.*[7].
- The liability of the Internet Service Provider depends on its functional attributes as the Internet service provider may act as an information distributor, i.e a carrier or information publisher. The Information Technology Act, 2000 does not recognize any of the above categories. Cognizance is taken under section 79 of the said Act which expresses the legislative intent of granting immunity to the network service provider.

Cyber defamation is covered under section 499 of the Indian Penal Code read with Section 4 of the Information Technology Act, 2000. Section 499 lays down when the actual defamation takes place while section 4 of the IT Act provides for legal recognition of 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

[3] Section 2(n) of the Code of Criminal Procedure,1973 and Section 40 of Indian Penal Code,1860.
[4] Section 2(n) of the Code of Criminal Procedure, 1973 and Section 40 of Indian Penal Code, 1860.
[5] S.K. Verma and Raman Mittal (Ed.), *Legal Dimensions of Cyberspace*, Indian Law Institute, New Delhi, 2004, p.233.
[6] Black's Law Dictionary, 6thEdn., 1990.
[7] [2001] VSC 305.

section 499 requirement of publication and would amount to defamation.

Cyber Obscenity and Pornography

Internet has brought with it vast knowledge and information for the individual and cyber obscenity and pornography is not distant to it. Easy accessibility and wide reach and availability of obscene material on the Internet have made it more convenient for individuals. Various tests of obscenity were laid down, the first being in *Regina* v.*Hicklin*[8] as the tendency to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall. In India, the a modified version of the *Hicklin* test was established in the case of *RanjitUdeshi*v. *State of Maharashtra*[9]in which the Supreme Court held that obscenity without a preponderating social purpose or profit cannot have constitutional protection of free speech and expression and obscenity in treating sex in a manner appealing to the carnal side of human nature or having that tendency. It further interpreted the word 'obscene' as that which is 'offensive to modesty or decency, lewd, filthy and repulsive. The Supreme Court in its subsequent cases such as *Samaresh Bose* v.*AmalMitra*[10], took a departure from the *Hicklin* test of "the most vulnerable person" and followed the "likely audience" test. In the case of *Ajay Goswami* v. *Union of India*[11], the Supreme Court observed that the test for judging a work should be that of an ordinary man of common sense and prudence and not an out of ordinary or hypersensitive man.

Cyber pornography refers to stimulating sexual or other erotic behavior over the Internet which includes pornographic websites, pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, writings, etc. The geographical restrictions no longer exist and therefore, foreign publications can easily enter the local territories in a matter of seconds. The Internet has no geographical boundaries and jurisdictional prescriptions, cyber pornography cannot be put to leash by domestic legislations.

Cyber pornography has been formally institutionalized with the recognition of '.xxx' domain by ICANN (Internet Cooperation for Assigned Names and Numbers)[12].

Child pornography on the Internet has been a matter of great concern as they are amongst the biggest users and beneficiaries of the Internet and constitute the most vulnerable group and are the worst sufferers of cyber pornography.[13] Article 9 of the 'Convention on Cybercrime' merely imposes a duty upon the parties to offences of producing, offering or making available, distributing or transmitting, procuring or possessing child pornography intentionally and making the offenders criminally liable. Section 67B of the IT Act, 2000 criminalizes all kinds of online child pornography.

[8] (1868) 3 QB 360.
[9] AIR 1965 SC 881.
[10] (1985) 4 SCC 289.
[11] (2007) 1 SCC 169.
[12] "Here it comes: Porn sites to get .xxx", *Times of India*, 26-06-10.
[13]VivekSood, *The Fundamental Right to Internet*, Nabhi Publication, 2011.

II. Cyber Stalking

Cyber stalking involves the act to pursue, harass or contact another in an unsolicited fashion using the electronic medium such as the Internet, e-mail, or other electronic communications devices to stalk another person.

Earlier there was no legislation against cyber stalking, but with The Criminal Law (Amendment) Act, 2013 section 354D was added which provided for criminalizing stalking and punishment for committing the offence of stalking.

Cyber stalking or e-mail harassment is an electronic augmentation of real life stalking and internet is a perfect forum where a person can terrorize his or her victim as anonymity leaves the cyber stalker in an advantageous position. This anonymity can be achieved by using a number of methods such as finding and using obsolete versions of computer software called 'Mail Deamons' or entering false users details during online registration of free guest accounts[14]. Cyber stalking my involve electronic sabotage where a cyber stalker may send hundreds of threatening or harassing e-mail messages by using sophisticated software that sends e-mail messages at regular or random intervals without perpetrator being physically present at the computer terminal.

Hacking

Hacking is when a computer system is accessed without the express or implied permission of the owner of that computer system. The New Hacker's Dictionary defines a hacker as such a person 'who enjoys exploring the details of programmable systems and how to stretch their capabilities; one who programs enthusiastically, even obsessively.' Hacking is usually a pre-planned process, where first a target computer system is identified; it's security features are studied; tools are developed(passwords and programs) to gain unauthorized access and impair the normal(programmed functioning of a computer or a computer system or computer network. In this kind of crime the computer is a tool as well as the target. It is one of the most popular and fastest rising crimes and has accelerated with the help of Internet.

The meaning and scope of hacking under section 66 of the IT Act, 2000 is beyond than the mere 'illegal or unauthorized access' but that should have been done fraudulently and dishonestly.

III. Privacy Violation

The internet has many data collection mechanisms which collect a variety of information about surfers like the goods purchased, sites visited, and personal information and so on. It is possible to create profiles on the information collected from a range of sources, which can be paired with information about the user's computer. This leads to creation of a personal profile attached to a particular computer.[15]

The main ways of data collection are:

i. Cookies

[14]Clake G, "What is Cyberstalking?", Unpublished SCU Cyberlaw essay, 2000.
[15] Yee Fen Lim, Cyberspace Law, 2nd Edn., Oxford University Press,New Delhi,2007,p. 127.

ii. Web bugs
iii. GUID(Globally Unique Identifier)
iv. Email and document bugs
v. Spy ware
vi. Online digital profiling

The privacy of an individual can be infringed if there is unauthorized access to his account on a social networking website without his knowledge and the person obtains private information without the permission of the person. Privacy is infringed when for example a hacker accesses a person's profile by hacking his account on a particular social networking website. There is no direct legislative provision with respect to privacy infringement on the internet but the IT Act, under sections 72 and 72A provides for penalty for breach of confidentiality and privacy and punishment for disclosure of information in breach of lawful contract respectively.

Internet Fraud

One or more components of the Internet such as chat rooms, e-mail, message boards, or websites are used to refer to any type of fraud scheme. Fraudulent solicitations are presented to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or others connected with the scheme. [16] Fraudulent activities can be conducted on social networking websites by persons impersonating to be somebody who they are not in order to commit an offence. Impersonating someone and then taking out information and other personal details also amounts to fraud. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way which involves fraud and deception, typically for economic gain. One can personally profit at other's expense if personal information like bank account number, credit card number, telephone calling card number or any other valuable identifying data falls into wrong hands.

IV. Virus Attacks

Virus attack the computer when programs transmitted are designed in a way to destroy, alter, damage, or even send across data residing in the computer. This transfer can be done by email, or sending messages on social networking websites asking the person to open the link and thereafter the virus attacks the computer system. Section 43 (c) of the IT Act, 2000 lays down the liability to pay compensation to the person who is affected by introduction of any computer contaminant or virus into any computer, computer system or computer network.

V. Copyright Infringement

Copyright is protecting original works of authorship that are fixed in any tangible medium of expression. Copyrighted material include the categories of literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphical and sculptural works, motion pictures and audiovisual works, sound recordings, architectural works and computer programmes. Any work copied on the Internet or from the Internet without acknowledging or giving credit to the original author will amount to copyright infringement and the person will be liable of the offence.

VI. Legislative Provisions for Protection against Cyber Crimes on Social Networking Websites

The Information Technology Act, 2000 provides for legal sanctity to the electronic era and enumerates offences committed in electronic form and their punishments. The main aim during the enactment of this said Act was to cover e-governance and facilitating e-commerce by providing infrastructural facilities for creation, promotion and use of digital signatures and also to provide for electronic records. The meaning and nature of the offence given under the Indian Penal Code can also be relied upon incase the particular offence is not defined under the IT Act, 2000. The Indian Penal code and other legislations have also been amended according the IT Act, 2000. The legislative provisions of specific offences committed on the Internet specifically on social networking websites are as follows:

I. Cyber defamation

Any person who defames another person on a social networking website can be made liable under sections 499-502 of the Indian Penal Code, 1860 and the question of intermediary liability of the particular social networking website arises. The word defamation under section 499 is defined as 'whoever by words, either spoken or intended to be read, or by signs or by visible representations, makes or 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 to defame that person[17]. There are however exceptions given to this above definition. Defamation in electronic form has been included in the Code by making it prominent that defamation could happen by means of 'signs' and 'visible representation'. Instances of defamation in electronic form includes generating, sending or receiving defamatory online bulletin board messages, chat room messages, e-mails, music downloads, video streaming, digital photographs on the Internet. Other instances which would amount to defamation in the electronic form would include sending defamatory SMS, MMS, photographs and videos on the mobile phones. Therefore the Code is sufficient to tackle online defamation matters.

Section 66A (a) provides for imprisonment of up to 3 years with fine to any person who sends, through a computer resource or a communication device any information that is grossly offensive or has menacing character.

Publication as already established takes place where the information is downloaded which happens when a file is retrieved from a remote computer, computer system or a computer network. For creating liability for defamation on the online medium, first cognizance needs to be taken under section

[16] Fraud Section, Criminal Division, U.S. Department of Justice, available at http://www.internetfraud.usdoj.gov/ (last viewed on 12.08.2014).

[17] Section 499 of the Indian Penal Code(45 of 1860).

79 of the IT Act, 2000 which expresses the legislative intent of the network service provider for granting immunity.

Cases

1. In the case of *Godfrey* v. *Demon Internet Ltd.*[18], someone unknown posted on the defendant ISP's newsgroup, squalid, obscene and defamatory of the plaintiff who was residing in England. The posting was on 13th January, 1997 whereas the plaintiff sent a letter by fax on 17th January, 1997 and the posting remained until the expiry on 27th January, 1997. Morland,J. ruled that whenever the Defendants transmit postings (including those defamatory postings) from the storage of their news server, publication of that posting takes place to any subscriber who uses the ISP and accesses the newsgroup which contains that posting. Thus every time any of the Defendants' customers accesses 'soc.culture.thai' newsgroup and sees the posting defamatory of the Plaintiff there is a publication to that customer.
2. Visaka Industries Ltd., a construction materials company, filed a case against Google India for criminal conspiracy, defamation and publishing content which is defamatory in 2011 alleging that a blogger named Gopala Krishna used Google's Blogspot.com, to spread false and defamatory information about the Company. The blogger stated that the company had connections with the Congress party and therefore the company could manufacture asbestos. Google India argued that it couldn't be held liable for content posted by users on a platform which is hosted by its parent company Google Inc..The Andhra Pradesh High Court held Google India to be liable and therefore it filed an appeal in the Supreme Court which is still pending. This judgment was criticized on the grounds that if Supreme Court upholds the decision of the High Court then Google will be liable for criminal activities on the Internet and therefore many blog sites, social media sites would be affected by the outcome of the case.
3. In 2012, two girls were arrested from Maharashtra for posting comments criticizing the bandh after Shiv Sena leader's death. The Arrest was made under section 66A for sending offensive message by means of a computer resource. This arrest was highly condemned as it the girls were neither disrespecting anyone nor were they promoting hatred towards any community, was just expression of an opinion. This did not make a proper case for the arrest of two girls under IPC section 295A {later changed to IPC Section 505(2)} and the IT Act Section 66(A). These arrests led to curbing the freedom of speech which is fundamental right. The Maharashtra Government told the Supreme Court that the arrest of the two girls was in haste and unwarranted.
4. Pakistan had filed a case against Facebook, Twitter and other social networking websites, for posting "blasphemous materials". This material was posted as groups on these social networks encouraged users to submit their caricatures or depictions of Prophet Mohammed. The court observed that the content was uploaded in Pakistan itself and these websites should remove the content with immediate effect.
5. Parle Agro Pvt. Ltd has filed a case against social networking websites Facebook Inc., Twitter Inc. and online search company Google Inc. for a user post that alleged its mango beverage Frooti was "contaminated". Parle Agro accused the social networking websites and online search engine of promoting the "defamatory" statement. The court is still to hear the matter on record in the Bombay High court and give a decision on the same.[19]

II. Cyber obscenity and pornography

The Information Technology Act, 2000 provides for all aspects of cyber obscenity and punishes for:

i. Violation of privacy(section 66E)

This section has made violation of bodily privacy an offence. A person is charged of an offence under this section when he or she intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent. The offender is punishable with imprisonment which may extend to three years or with fine not exceeding two lakh rupees of with both.

ii. Publishing or transmitting obscene material in electronic form(section 67)

A person shall be punishable with imprisonment up to 3 years and maximum of 5 lakh rupees of fine in case of first conviction and five years of imprisonment and fine up to ten lakh in case of second conviction, when he publishes or transmits in electronic form any material which is lascivious or appeals to the prurient interest and has a tendency to deprave or corrupt persons who are the likely audience to read, see or hear the matter contained or embodied in electronic form. Knowledge of obscenity is not an ingredient of the offence and therefore to escape liability one has to prove lack of his knowledge that the obscene material has been published or transmitted in electronic form.

iii. Publishing or transmitting of material containing sexually explicit act etc. in electronic form(section 67A)

When publication or transmission of any material containing sexually explicit act or conduct takes place in electronic form, an offence under this section takes place and the offender is punishable on first conviction with imprisonment with may extend to five years and with fine which may extend to ten lakh rupees and second or subsequent conviction with imprisonment up to seven years and with fine which may extend to ten lakh rupees.

[18] (1999) 4 All ER 342 (HC).

[19] *Parle Agro Pvt. Ltd* v. *Praveen Kumar and Ors*Suit No. 409 of 2013.

iv. Child pornography(section 67B)

Namely five instances of online child pornography have been criminalized :

a. Publishing or transmitting or sauing to publish or transmit material in any electronic form which depicts children in sexually explicit act or conduct;
b. Creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging or distributing material in any electronic form depicting children in obscene or indecent or sexually explicit manner;
c. Cultivating, enticing, or inducing children to online relationship with one or more children for and on sexually explicit act or in a manner that they may offend a reasonable adult on the computer resource;
d. Facilitating abusing children online, and
e. Recording in any electronic form own abuse or that of others pertaining to sexually explicit act with children.

The offender is punishable on first conviction with imprisonment with may extend to five years and with fine which may extend to ten lakh rupees and second or subsequent conviction with imprisonment up to seven years and with fine which may extend to ten lakh rupees.

Cases:

1. The first case involving the conviction of a person for posting obscene messages on the internet was *Tamil Nadu*Vs*SuhasKatti*[20] in which the accused was a family friend of the victim and was eager to marry her but she got married to someone else. When she got divorced he again pursued her for marriage but she refused. He started harassing her and posted her number of Yahoo! Messenger Groups and posted obscene information and details regarding her. The victim started getting annoying phone calls in the context of the people believing that she was soliciting. He was later convicted under section 67 of the Information Technology Act, 2000 and was sentenced with imprisonment and fine.
2. In *Avnish Bajaj* v. *State*[21], the petitioner was the Managing Director of the website Bazee.com which was an online shopping forum. A seller placed on the website a listing offering an MMS video clip for sale. To avoid the filter's he placed the listing in the category of books and magazine. The item description was "DPS Girl having fun". A complaint was made to the website owner and after 2 days of the complaint the website wrote to the seller that the content has been removed due to the violation of user agreement. The court opined that "the entire text of the listing was obscene. There was a prima facie case under section 67 of the Act since the interested buyer had to go through the chain of process before he buys the product."

III. Cyber Stalking

There is no explicit provision for protection against cyber stalking but the Criminal Law (Amendment) Act, 2013 added 'stalking' as an offence under section 354D of the Indian Penal Code which states that

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 bad 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 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.'[22].

A person can also be charged under Section 66A (a) & (b) of the IT Act, 2000 for sending any information which is grossly offensive or has menacing character or he knows to be false but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or will, persistently, by means of a computer resource or a communication device.

Case:

1. India's First Case of Cyber stalking was registered by the Delhi Police in 2001 where a lady named RituKohli complained that a person was using her identity to chat over the

[20] C.C.NO.4680/2004.
[21] 150 (2008) DLT 769.
[22] Inserted by Criminal Law (Amendment) Act, 2013 (No. 13 of 2013).

Internet at the website "www.mirc.com" and was also deliberately giving her telephone number to other persons encouraging them to call RituKohli at odd hours. As a result of which, Mrs. Kohli received an estimate of 40 calls, national as well as international, during odd hours within 3 days. A case was registered under section 509 of the Indian Penal Code.

IV. Hacking and Virus Attacks

It is a computer trespass where the hacker enters the computer resource without permission of the actual owner. Section 43 of the IT Act, 2000 makes unauthorized access to a computer resource a cyber contravention. The notion of mensrea is brought into the purview of section 66 of the same Act by using the words 'dishonestly or fraudulently'. When any computer related offence given under section 43 of the Act is committed dishonestly or fraudulently, it is made 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.

V. Privacy Violation

Section 72 of the IT Act, 2000 has conferred powers to certain class of persons who are have secured access to electronic record, book, register, correspondence, information, document and the like material and they shall not disclose this information or material without the consent person concerned. The section is to prevent the person from taking unfair advantage of the information it has and disclosing it without the knowledge of the consent of the disclosing party. Unauthorized disclosure by the concerned person shall lead to imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or with both. Section 72A was introduced for protection of information given by a user to the service provider. This section provides that if a service provider which is providing services to a person, discloses his or her personal information without his or her consent and in breach of a lawful contract with the intent or with the knowledge that it is likely to cause wrongful loss or wrongful gain to any other person he shall be liable to be punished with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

These sections have to be read with the reasonable restrictions given under Article 19(2) on right to 'freedom of speech and expression' as enumerated under Article 19(1) (a) of the Constitution of India.

Article 21 of the Constitution provides for right to privacy and a writ can filed in the court if any act on the Internet infringes this Fundamental right.

VI. Internet fraud

Section 66C is for the protection of the privacy and their personal information or data of all or any online user. It is to protect the authentication of details of any person in the form of electronic signatures, passwords, PINs, biometric identifiers or any such other unique identification feature. Cheating by personation using a computer resource is also an offence under the IT Act, 2000 and is made punishable with imprisonment which may extend to three years and fine which may extend to one lakh rupees. Any person who by deception, fraudulently or dishonestly induces that person to accept, agree, transact or deliver any data, information or to consent that any person to retain any data, or intentionally induces that person to do or omit to do, using any communication device or computer resource commits the offence under the aforesaid section.

VII. Intermediary Liability

The main issue with respect to cyber crimes on social networking websites is with respect to its liability while dealing with the offences taking place on these service providers. Before any liability can be attached to them, the concept of what exactly an intermediary is and its function needs to be looked into.

Intermediary is a network service provider who may act as an information carrier or information publisher. An intermediary creates an interactive wired world as well as acts as an important link in transmitting, distributing and publishing on the World Wide Web. An intermediary, with respect to particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record. Intermediaries can be categorized as information carriers which simply transmit the electronic message without scrutinizing it which are mainly 'access only' intermediaries such as airtel.in; information publishers publish as well as transmit the information which are 'enhanced intermediaries' like google.com; or information sellers which publish, transmit and sell the information or the product and also take reasonable care in relation to its publication. Social networking websites like Facebook.com, Myspace.net, Youtube.com and blogging sites like Twitter.com publishes its own in-house content and may also buy from other content providers or third parties or third parties uploading their own content on the website which acts as a platform provided by such service providers. Intermediaries being facilitator of third party information, data or communication link may be held liable for copyright infringement, trademark infringement/dilution, privacy violations, obscenity, defamation, child pornography, spamming etc. Civil and criminal proceedings along with injunction to block/ remove the offending material can be initiated against the intermediaries. Section 79 of the IT Act, 2000 provides for exemption from liability of the intermediary in certain cases. When the intermediary performs the limited function of only access to the communication system or when it does not initiate the transmission or when it observes due diligence while discharging its duties, then the intermediary is exempt from any liability. 'Third party information' is meant to be any information dealt with by a network service provider in his capacity as an intermediary.

VIII. Conclusion

The Internet is a mammoth network of computers and that has made it a boon as well as a bane. On one hand everything has become so easy and convenient from shopping to cooking to playing games etc, on the other hand this has made cyber offenders to take advantage of the situation of this over dependency of people on the Internet.

The legislative provisions for protection and punishment against these crimes are to be interpreted with practicality. The vague and ambiguous provisions of certain laws should be interpreted liberally and in accordance with the norms of the society. While construing the provisions of section 66A of the Information Technology Act, 2000 a lot of controversy has been generated towards the violation of Freedom of Speech given under Article 19(1) of the Constitution of India, which is fundamental to India's democracy. The government has issued an advisory to states on how to implement the controversial Section 66(A) of the IT Act. No less than a police officer of a rank of DCP will be allowed to permit registration of a case under provisions of the Information Technology Act that deals with spreading hatred through electronic messages. In the case of metropolitan cities, such an approval would have to come at the level of Inspector General of Police.[23]

It can be concluded that more stringent laws should be made and implementation of these laws should be the main concern. There is lack of awareness among many individuals using the social networking websites and more often than not they are hesitant to take action against the offenders committing the offence.

Authors

First Author – Nikita Barman

[23] H S Gill, "Information Technology Act Section 66(A): An Analysis", available at http://strategicstudyindia.blogspot.in/2013/01/information-technology-act-section-66a.html (viewed on 13-09-2014)