CYBER CRIME: A CRITICAL STUDY

Written by ***Rohit Prakash***

4th year BA LLB Student, Christ (Deemed To Be) University

ABSTRACT

Stalking is a particular form of harassment. It may be repeatable or persistent. The cyberspace is being taken up by a new form of crime that includes repetitive attempt by one person to contact another thereby causing a sense of threat in mind of such other person. This emerging crime is popularly known as 'cyber stalking'. The author has made an attempt to deal with the issues of cyberstalking which is a newly coined phenomenon. In first chapter there is discussion on cyberstalking and then, in the third chapter the author explains the difficulties of enforcing the stalking offences in India and after that the difference between the perceptive and non-perceptive legislation and lastly the author also explains about the nature of cyberstalking and also about the situations of victims of cyberstalking. The author in the last chapter has given concluding remarks followed by some suggestions and preventive action that one could take as prevention is better than cure.

INTRODUCTION

Stalking is particular form of harassment. It may be repeatable or persistent. It may be targeted at one individual by another. This behavior may be sinister in nature e.g. threatening telephone calls, death threats and physical assaults are prime examples. Others may be quite innocuous in themselves but when sufficiently repeated are often likely to provoke feelings of harassment and intimidation in the target, examples include walking past the targets home or workplace and sending letters or flowers to the target, repeated excess unwanted telephone calls-regardless of content, a stranger engaging the target in an unsolicited conversion in a public place such as at a bus stop. Thus stalking cannot dividing into staking behaviors and non-stalking behavior. E.g. telephoning the target after one initial meeting/ agreeing with the target's every word (even when she is obviously wrong). Unasked for offers of help, lifts in his

car, etc. Stalker activity may vary in term of intensity within individual cases and may be variable over time.

CYBER STALKING IN INDIA

Manish Kathuria was stalking Ritu Kohli by illegally chatting on a chat website called MIRC using her name. - He used obscene, obnoxious language and distributed her residence phone number, inviting people to chat with her phone, as a result of which, Ritu kept getting anonymous obscene calls from people all around the world. In a state of shock, she called the Delhi police and reported the matter. For once the police department did not waste time into swinging into action, and a case has been registered under section 509 against Manish Kathuria for outraging the modesty of Ritu Kohli.

Kidnapping of 16yrs old girl at Mumbai: - Akbar khatri, from his school, by a paedophilic lady chat friend of his, in order to sell him to child traffickers at Pakistan. Another case registered at Mumbai in the year 2000, was of a 16-year-old girl who was reported to be missing from her home after she befriended a boy in Moradabad through internet chat.

The 'web' is lurching with 'spiders' like sex maniacs pedophiles and other terrifying avatars of cyber stalkers, crouching to prey on unsuspecting young children, teenagers or even sometimes middle-aged adults.

DIFFICULTIES OF ENFORCING THE STALKING OFFENCES

a) *Establishing credible threat* – Most existing laws on stalking and cyber stalking apply only to behavior that constitutes a direct or credible threat and causes the victim to be fearful of his or her safety, which may make prosecution difficult. First, it can be difficult to establish 'credible threat' if no actual threat of violence from the cyber stalker is evident. Secondly many cyber stalker do not threaten their victims directly or overtly or in 'person'; they might post the name, address and phone number of their victim on the internet, in newsgroups or advertisements, or may impersonate their victim in a chat room although these behaviours can be interpreted as harassment, it may be difficult to prosecute the perpetrators because they may not have made a 'direct' threat against the victim.

b) *Anonymity / identities* – another obstacle to the enforcement of legislation is the identity of the cyber stalker. Due to the sophistication of the technology, the internet has created the possibility for anonymous cyber stalking. The stalker could be a former friend or lover, a total stranger met in a chat room or simply a teenager playing a practical joke. It hardly needs stating that the inability, to identify the source of the harassment or threats hinders police investigation of cyberstalking. Anonymity prevents businesses and the government from monitoring internet users. However, some forms of anonymous communications can be eradicated. Internet protocol will improve the ability of law enforcement officers to track cyberspace communications through unique identifiers attached to every computers IP number. Companies such as Microsoft, apple, sun MCI WorldCom and IBM have already endorsed IPv6, and the Internet Assigned Number Authority, which is responsible for allocating Internet addresses, issued numbers based on the new standard for the first time.

c) *Issue of privacy:* - In the USA, for example, the CCPA, 1938. Prohibits disclosure of cable subscribers records to law enforcement agencies unless the agency has a court order has provided advance notice to the subscriber. Under the CCPA, a law enforcement agency investigating a cyber stalker has to provide the individual with notice that his or her subscriber records have been requested. This law was passed before the use of ISPs. The purpose of the law was to prevent the police from abusing their powers by checking on the viewing habits of cable subscribers without the knowledge of the persons being investigated. The law was designed to protect privacy, but now that cable companies are ISPs it can hinder police investigation of cyber stalkers. Put simply if the police give a suspected cyber stalker notice that they will be checking his or her ISP records, the cyber stalker has the opportunity to destroy evidence. Although it may be appropriate to prohibit the indiscriminate disclosure of cable records there is a growing feeling among commentators that the government should allow law enforcement officers to have access to a person's file without his or her prior knowledge if that person is suspected of cyberstalking (USDJ 1999).

d) *Jurisdiction and statutory authority*: - although the internet may be borderless for the cyber stalker, law enforcement officers are constrained by geographical

boundaries. This makes investigating and arresting a cyber stalker outside their jurisdiction extremely difficult.

e) *Individual responsibility*: - USDJ, has made suggestions that internet users can follow to prevent cyberstalking and to protect their privacy as under: -

- Do not share personal information as part of any user profiles
- Log off or surf somewhere else if a situation online becomes hostiles
- Block or filter messages from the harasser
- Report any form of cyberstalking to the police
- Do not use your real name or nickname as your screen name of user id.

Moreover, the IT act does not have cyber stalking provision in this act and the Central Government must enact such law looking to experience of the countries.

EXTENT OF CYBER STALKING

Thirty-nine percent of the cases involved e-mails; 16 percent chat rooms; 13 percent instant messaging programs: 9 percent message boards; 9 percent newsgroups : 9 percent a website (other than message boards); 3 percent a virus attack : and 4 percent other ways. A common place for cyber stalking is at the 'Edu' or educational sites for colleges and universities cyber angels- an international online safety organization that assists victims and police, and provides information on all aspects of online safety, privacy and security- estimates that as many as 80,000 Canadians are cyber stalked annually.

NATURE OF CYBER STALKING

a) *E-mail stalking:* - electronic mail (E-mail) is an electronic postal service that allows individual to send and receive messages or information in a manner of second. This sophisticated use of telephone lines allows communication between two people who may or may not know each other but can 'speak' to each other using a computer and a keyboard. In general, e-mail is an insecure method for transmitting information or messages. Everyone who receives an e-mail from a person has access to that person's e-mail address with some online services such as AOL; a person's screen name is also

an e-mail address. It is unsurprising, then, that e-mail is a favoured medium for cyber stalkers.

b) *Chat stalking:* - A chat room is a connection provided by online services and available on the internet that allows people to communicate in real time via computer text and a modem. Cyber stalkers can use chat rooms to slander and endanger their victims. In such cases, the cyber stalking takes on a public rather than a private dimension. As live chat has become more popular among users of the internet with tools such as internet relay chat (IRC), it has also become more popular as a medium through which stalkers can identify and pursue their prey.

c) *Bullet Board System:* - A Bulletin Board System (BBS) is a local computer that can be called directly with a modem. Usually they are privately operated and offer various services depending on the owner and the users. A bulletin board allows user to leave messages in group forums to be read at a later time. Often a BBS is not connected to a network of others computers, but increasingly BBSs are offering internet access and so cyber stalking are using bulletin boards to harass their victims.

d) *Computer stalking:* - With computer stalking, the cyber stalker exploits the internet and the windows operating system in order to assume control over the computer of the targeted victim. An individual 'windows based' computer connected to the internet can be identified, allowing the online stalker to exercise control over the computer of the victim. The cyber stalker can communicate directly with his or her target as soon as the target computer connects to the internet.

e) *United States and other countries*: - United States now has legislation designed to deal with real- life stalking, but there have proved to be number of difficulties in applying these state laws to e-mail harassment. California was the first state to pass a stalking law in 1990, and all the other states have since followed. The federal government has passed a number of important pieces of legislation that can be used to prosecute cyber stalkers although, as we shall see, none are comprehensive and all contain loophole. The federal statute makes it a crime, punishable by up to five yrs. in prison and a fine of up to $250,000, to transmit any interstate or foreign communication containing a threat to injure the person another. Thus; it includes threats transmitted via the telephone, e-mails, pagers or the internet. Certain forms of cyber stalking also can be prosecuted under federal statute. Congress has also passed the ISPPA,1996 under this

act, it is illegal to travel across a state line with the intent to injure or harass another person or, as a result of such travel, to cause that person reasonably to fear for his or her safety. The federal government has further passed an amendment (CDA) to the Communications Act, 1934 changing the language to include computers as a telecommunications device, the legislation clearly targets activities that could be considered cyber stalking stating that anyone who commits the following is guilty of crime.

PRESCRIPTIVE VERSUS NON-PRESCRIPTIVE LEGISLATION

The victims of stalking also play important roles in the way that stalking may be legally defined. Anti-stalking laws frequently require the victim to display negative effects of stalking, or else require that a reasonable person would be likely to experience negative consequences in the same situation. These negative effects may take the form of substantial emotional distress.

PROTECTIVE CHILDREN AGAINST ONLINE

In 1998, President Clinton signed a bill into law protecting children against online stalking. The statute makes it a federal crime knowingly to communicate. But although this law can provide protection for children against predators, it doesn't cover harassing phone calls to minors in which there is no intent to entice or solicit the child for illicit sexual purposes. the NIJ was asked by congress to develop a Model stalking code. Shri Joanna R. Adler in Forensic Psychology has observed about the model.

Outside USA, similar variations exist between countries with regard to what legally constitutes stalking or harassment. In England and Wales, a broad approach has been adopted where 'a person must not pursue a course of conduct which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other'

In Ireland, however a definition of harassment is provided as follows:-

"Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her shall be guilty of an offence.

SPECIFIC CRIMINAL OFFENCES.

The term stalking has no legal status in the UK and although the protection from act is informally referred to as the 'anti-stalking law', it doesn't actually use or define the term stalking. Furthermore, the legal test as to whether a person is guilty of harassment is once again based on the judgment of 'reasonable person' unlike most criminal offences which require some degree of intent.

The 1997 act created two specific criminal offences to deal with the problem of harassment. The first is an indictable offence involving fear of violence. This offence requires proofs that the victim was put in fear of violence, regardless of whether or not the offence intended to do so, and carries a maximum sentence of five years imprisonment. The second is the summary offence of criminal harassment which doesn't require the victim to have been put in fear of violence, and could result in a maximum sentence of six months imprisonment in jail.

VICTIMS OF STALKING

The Majority of victims are females (75%). The 1998 British Crime Survey found 16-19yrs old to be most at risk. And this survey also found stalking prevalent to be the highest among victims with a relatively low household income. Stalking victims are more frequently found among single persons although married person and those in other partners are not exempt from stalking victimization, particularly if they were students and living in privately rented accommodation. These risks appear to be greater for young single women in high status occupations, or celebrities etc. It is observed that domestic doesn't necessarily and with the conclusions of a relationship but may continue in form of stalking.

VIRTUAL OR ELECTRONIC FORM OF PHYSICAL STALKING

Cyber stalking is a virtual or electronic form of physical stalking. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, or persistent unwelcome contact with another individual for example, following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalism of property.

Cyber stalking could be in various forms such as threatening, victims over the internet, sending harassing e-mail or in extreme cases, even trying to make contact in person, against the will of

the victim. It could be worse in certain cases where the cyber stalker knows personal details and whereabouts of the victims, wherein the victims phone number could be displayed across the Net, most commonly on pornographic or telephonic chat line websites and in extreme cases, even by displaying morphed photographs of the victim on pornographic pictures.

CONCLUSION

It is in all respects accurately said that on the off chance that you need to get change the present situation, you have to beat the old model of managing the circumstance and fabricate another model that is viable and productive. Cyberstalking is a recently instituted term. It has gained consideration of the lawmaking body and legal executive as of late. There have been numerous occasions where the requirement for powerful enactment was felt as it turns out to be hard for the authorization organizations to manage such cases. Cyberstalking is demonstrated to be a grave offense. It has extremely broad effect on the psychological and physical strength of the person in question. Through this article, the writer has made an endeavor to talk about the expression "cyberstalking" in detail alongside its tendency and extension. A few people contend that it is an all-encompassing variant of digital stalking or another type of stalking yet it seems, by all accounts, to be more than that. It is another type of wrongdoing itself. We have seen that the aim of the stalker is to disturb and undermine his/her unfortunate casualty. Hence, it includes crime. Numerous nations have enactments regarding this matter. None of the current arrangements are equipped for managing the cases productively. India does not have any immediate enactment regarding the matter. Information Technology Act and Indian Penal Code have scarcely any arrangements that could be identified with this cybercrime and subsequently the stalker can be reserved under those arrangements. These are the lacuna in the authoritative methodology pursued by the nations to address this wrongdoing. There are not really any revealed cases on the grounds that the police experts don't take up the case in light of the implementation issues as the stalker and the injured individual may have a place with various nations therefore, it ends up hard to choose as to law of which nation is to be pursued. We ought not exclusively rely on the administrative arrangements however ought to proactively make an endeavor to don't offer ascent to such circumstances.

REFERENCES

I. Abhiraj Thakur, Cyberstalking: A Crime or A Tort, Jun. 21, 2016.

II. Amy C. Radosevich, Thwarting the Stalker: Are Anti-Stalking Measures Keeping Pace with Today's Stalker? 2000 U. Ill. L. Rev. 1371 2000.

III. B. Spitzberg and G. Hoobler, Cyberstalking and the Technologies of Interpersonal Terrorism, 4(1) NEW MEDIA & SOCIETY 71 (2002).

IV. BH Spitzberg and WR Cupach, The State of the Art of Stalking: Taking Stock of the Emerging Literature, 12 AGGRESSION AND VIOLENT BEHAVIOUR 64 (2007).

V. Divij Joshi, India's Criminal Law Amendment to include Cyberstalking, Harassment and Voyeurism, CIS, (2013).

VI. Divij Joshi, The Criminal Law Amendment Bill 2013 — Penalizing 'Peeping Toms' and Other Privacy Issues, CIS, (2016).

VII. Dr. Swati Mehta, Cyber Forensics & Admissibility of Digital Evidence, (2012).

VIII. P. Shah, Cyber Stalking & the Impact of its Legislative Provisions in India, (2013).

IX. Subhajit Basu, Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis, 3(2) EUR. J. L. & TECH. 1 (2012)

X. Venkat Bal Subramani, Conviction for Cyberstalking & Revenge Porn Survives First Amendment Challenge, (May 8, 2014).

XI. Vijay Mukhi and Karan Gokani, Observations on the Proposed Amendments to the IT Act 2000, AIAI.