Vol.03,Issue03,March2015

INTERNATIONAL JOURNAL OF RESEARCH PEDAGOGY AND TECHNOLOGY IN EDUCATION AND MOVEMENT SCIENCES (IJEMS) ISSN: 2319-3050

THE TECHNICAL AND LEGAL PERSPECTIVE OF CYBER STALKING

[1]PARVEEN SADOTRA [2]JASBIR KOUR

[1]Teaching Assistant, & *C.E.H,* Govt. Degree College, R.S. Pura, J&K, INDIA
[2]Teaching Assistant, Govt. Degree College, Kathua, J&K, INDIA

ABSTRACT

Nowadays cyber crime is one of most concerning issues for all the developed and developing countries including India, This paper addresses the issue of Cyberstalking and internet harassment, and what legal remedies an internet user has when confronted with this form of behavior. The paper will commence with a discussion of on-line harassment including the way in which the internet facilitates this behavior. In this paper I had covered some type of cyber crime with the help of print and electronic media by quoting some current cases happened related to cyber crime. In next section , statistics of crime cases are discussed which were happened in last few years and compared crimes happened in past years and also discussed what type of crimes are on increase and decrease. On-line harassment is similar to real-world stalking in the way that it can be disturbing to the victim specially females. At the same time the unique environment of the internet creates "remoteness" on the part of the stalker, and provides a false sense of security arising from the apparent anonymity that is present on the internet. The paper will also discuss various approaches to the problem and demonstrate the various ways that current legislation and the common law can be used to deal with on-line harassment in our country. In addition the paper will provide some preventive measures for an internet user avoid with this crime.

Key words: *Cyber Defamation, Cyber Stalking, IT Act- 2000, ITAA-2008, Sections, Stalker.*

INTRODUCTION:

Technology opens our lives up in ways that weren't possible even less than a decade ago. Young generation laugh themselves silly when they hear elder people waxing nostalgic about the days when they pulled over to the side of the road to use a public pay phone, or called someone on the phone for directions ("What? No cell phone? No GPS navigation?"). Today you can chat with someone whether they're in the next room or in another country with ease, via a variety of technologies. It's all fast and amazing.

On the flip side of that good fortune is that same technology has also provided a way for people to do bad things.

What is Cyber Stalking?

Cyber stalking, simply put, is online stalking. It has been defined as the use of technology, particularly the Internet, to harass someone. Common characteristics include false accusations, monitoring, threats, identity theft, and data destruction or manipulation. Cyberstalking also includes exploitation of minors, be it sexual or otherwise.

Cyberstalkers use a variety of techniques. They may initially use the Internet to identify and track their victims. They may then send unsolicited e-mails, including hate, obscene or threatening mail. Live chat harassment abuses the victim directly or through electronic sabotage (for example, flooding the Internet chat channel to disrupt the victim's conversation). With newsgroups, the Cyberstalkers can create postings about the victim or start rumors that spread through the bulletin board system. Cyberstalking is a course of conduct that takes place over a period of time and involves repeated, deliberate attempts to cause distress to the victim.[1]

LEGAL FRAMEWORK OF CYBER STALKING IN INDIA:

The word 'stalking' was not commonly known in India, until Priyadharshini Mattoo's case (1996) hit the headlines. Eve teasing, a colloquial word for gender harassment is popularly known and Tamil Nadu Prohibition of Eve-Teasing Act, 1998 on that was developed after the brutal killing of a girl named Sarika Shah in Chennai. Though, stalking is there in the past, it was not acknowledged with this terminology and it was always merged with Eve teasing. On the other hand, stalking is much graver than Eve teasing and it is an obsessive behavior. After the Mattoo's case, the Indian Criminal Justice System awoke and the National Commission for Women is ready with a draft Bill (Sexual Assault Prevention Bill) to make the Indian Penal Code more effective against the menace of stalkers. Research studies related to stalking in India are sparse and there is a need to study this phenomenon in depth. This paper presents some results from a study of stalking victims among Girl College students at Tirunelveli City, Tamil Nadu, India. In-depth questionnaire data are drawn on to investigate the course and nature of prolonged

stalking in 150 self-defend victims. Findings indicate a pattern of repeated intrusions, the stalking harassment methods, lack of reporting behavior, and effects of stalking on the victims.

The December 2012 brutal Delhi rape had given birth to numerous issues. This included knee jerking awakening regarding the safety of women and a feeling of insecurity due to too many laws but too less execution of them. The incidence had also showcased the need of new sensible laws which can protect women not only in theory, but also in practice. The best result of this painful incidence is probably the Justice Verma committee report on proposal to amend the criminal law of India. The report did promise to fill in many gaps which were left for so long by numerous law amendment committees. Undoubtedly one of the notable moves by this committee was giving legal recognition to the offence of Stalking.

The Indian IT Act 2000 which was amended in 2008 does not directly address stalking. But the problem is dealt more as an "intrusion on to the privacy of individual" than as regular cyber offences which are discussed in the IT Act 2008. Hence the most used provision for regulating cyber stalking in India is section 72 of the Indian information technology act (Amended) , 2008 which runs as follows;

Section 72: Breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register,correspondence,information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. And also section 72A of the Information Technology Act, 2000(amended in 2008), which runs as follows:

Section 72A:Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008): Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about

another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

In practice, these provisions can be read with section 441 of the Indian Penal Code, which deals with offences related to Criminal trespass and runs as follows: Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property , or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate , insult or annoy any such person, or with an intent to commit an offence, is said to commit criminal trespass.

If the cyber stalking is done only to annoy the victim and is not resulted to serious offences like severe defamation, sexual crimes, identity theft or even grave crimes like terrorism, it is treated as a bailable offence.

However, after the December, 2012 Delhi gang rape incidence, the Indian government had taken several initiatives to review the existing criminal laws. A special committee under Justice Verma was formed for this purpose and basing upon the report of the committee, several new laws were introduced. In this course, anti-stalking law was also introduced. The Criminal Law Amendment Ordinance, 2013 added S.354D to the Indian Penal Code to define and punish the act of stalking. This law is as follows:

S.354D of the IPC (as has been added by the Criminal Law Amendment Ordinance, 2013):

1. Whoever follows a person or contacts or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person or whoever monitors the use by a person of the internet, email or any other form of electronic communication or watches or spies a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person or interferes with the mental peace of such person, commits the offence of stalking.

Provided that the course of conduct will not amount to stalking if the person who pursued it shows

i. that it was pursued for the purpose of preventing or detecting crime and the person accused of stalking had been entrusted with the responsibility of prevention or detention of crime by the State , or

ii. that it was pursued under any enactment or rule of law, or to comply with any condition or requirement imposed by any person under any enactment, or,

iii. That in the particular circumstances, the pursuit of the course of conduct was reasonable.

2. Whoever commits the offence described in S.354D (1) shall be punished with imprisonment of either description for a term which shall not be less than one year but shall extend to three years and shall also be liable to fine. [2]

CYBER STALKING AND TYPES OF CYBER STALKING IN INDIA:

Stalking, involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Stalking is illegal in Georgia, even if an overt threat of death or bodily injury has not been made. Whether or not a stalker makes a threat has no bearing on whether or not he/she poses a threat. [3]

Types of stalkers

There are three types of Cyber stalker. Here are those:

1. Intimate partner stalkers
2. Delusional stalkers
3. Vengeful stalkers

Types of Cyber Stalking

Cyberstalking may not be such a common form of cyber bullying, but it does occur on a daily basis all over the world. It can be very scary and annoying to be cyber bullied because it is the type of bullying that involves someone individually sending messages through text messages, emails, or social media messages. The worst thing about this form of bullying is the fact that it can turn to physical bullying, so it must be stopped as soon as possible.

1. Email Stalking
2. Internet Stalking [4]
3. Computer Stalking [4]

Motives of Cyberstalkers

In many cases, the cyber stalker and the victim have had a prior relationship and the Cyberstalking begins when the victim attempts to end the relationship. However, given the enormous amount of personal information available via the Internet, strangers can easily locate "private" information about a potential victim. [5]

- Sexual harassment is the most common form of Cyberstalking. Women are more likely than men to be victims. Victims receive unsolicited private messages in any chat forum that, for example, are derogatory toward women in general.

- Love obsessions sometimes start in real life and carry over into cyberspace, but they also develop from online romances. Once they realize the fantasy cannot come true, they begin sending death threats to their victims.

- Hate/revenge vendetta Cyberstalkers begin their harassment disguised as a flame war, or verbally abusive dialogue. These Cyberstalkers are rude, obnoxious, and have no problem hurling their obscene remarks at others. They are empowered by their anonymity and will not let go.

- Power/ego Cyberstalkers have nothing against you at all. They are just showing off their technological skills at your expense.

- Pedophile Cyberstalkers contact children in chat rooms, posing as teenagers or children of similar ages.They begin sending pornographic images to their victims, extracting personal information from their victims, and attempting to set up a meeting with their victims, which the pedophile expects will lead to sexual activity.

The Characteristics of the victims of cyber stalking are:

- Male or female depending on the age group
- In 18 - 32 year olds, females predominate
- Often involved in a real or imagined romantic or sexual relationship
- May be a member of a targeted minority group or special group
  - ethnic, racial and religious minorities
  - gays and lesbians
  - cancer or other patients with serious illnesses
  - adoptive or birth parents
  - political or special interest group

AIMS AND OBJECTIVES OF THE RESEARCH WORK:

Following are the aims and objectives of the research work

- To analyze the nature and extent of stalking victimization among women
- To assess the stalkers relationship with the victims and the stalker harassment methods
- To examine the responses and support for victims of stalking
- To examine the impact of victimization
- Explore Women's experiences with cyber stalking

- Understand emotional and behavioral reactions to cyber stalking
- Probe what teens think would be the most effective ways to prevent or put a
- stop to cyber stalking
- Determine how women define cyber stalking and what other terms they use to describe it

SCOPE AND LIMITATIONS:

Scope

Although there is no comprehensive, nationwide data on the extent of Cyberstalking in India, some researchers compile statistics on the number and types of complaints of harassment and/or threats involving their subscribers and individual law enforcement agencies have compiled helpful statistics. There is, moreover, a growing amount of anecdotal and informal evidence on the nature and extent of Cyberstalking.

The scope of Cyberstalking is affecting more adolescents than people are aware of. Various studies indicate that over half the women knew someone that had been Cyber stalked. This is an indication that Cyberstalking has risen and has become an increasingly critical issue of concern. With this problem on the rise, it is hoped that we can find more ways to help prevent Cyberstalking and also have a more stable foundation of consequences.

Limitations

There are many limitations in probe and research of Cyber Stalking in India as well as world wide

Information Technology Act 2000

Indian IT Act 2000 was introduced in year 2000. There was an amendment done in 2008 in respect of Cyberstalking but this act is still not yet sufficient enough for punishing all the cyber Stalkers. [1]

Geographical area.

Before a law enforcement agency can investigate a cybercrime case, it has to have jurisdiction. The first thing that must be determined is whether a crime has taken place at all. In some cases, there is no law on the book that covers the particular circumstance. In other cases, the wrongful action that took place is a civil matter, not a criminal one. This might be the case, for instance, if you entrusted your data to a company and that company lost it.

The next, and in the case of cybercrime the stickiest point, is to determine the geographic jurisdiction. This is more difficult in cybercrime cases than in other types of crime because often the perpetrator is not in the same city, state or even country as the victim.

Why is geographic jurisdiction such a big problem? Law enforcement agencies are only authorized to enforce the law within their jurisdictions. Thus jurisdictional issues frequently slow down or completely block the enforcement of cybercrime laws.

All the Cases of Cyber stalking are not being reported

One of the main limitations in Cyber stalking is that, in most of the cases it's not being reported or complained.

Nature of the evidence

Yet another thing that makes cyber stalking more problematic to investigate and prosecute in comparison to most "real world" crimes is the nature of the evidence. The difficulty with digital evidence is that, after all, it is actually just a collection of ones and zeros represented by magnetization, light pulses, radio signals or other means. An investigator can contaminate the evidence simply by examining it, and sophisticated cybercriminals may set up their computers to automatically destroy the evidence when accessed by anyone other than themselves.

In cases such as child pornography, it can be difficult to determine or prove that a person downloaded the illegal material knowingly, since someone else can hack into a system and store data on its drive without the user's knowledge or permission if the system isn't adequately secured.

Law enforcement response: the challenge of anonymity

Another complication for law enforcement is the presence of services that provide anonymous communications over the Internet. To be sure, anonymity provides important benefits, including protecting the privacy of Internet users. Unfortunately, Cyberstalkers and other cybercriminals can exploit the anonymity available on the Internet to avoid accountability for their conduct. [13]

HYPOTHESIS AND LIMITATIONS:

A good model for research investigation is very important. Such a model is useful not just for law enforcement. It can also benefit IT managers, security practitioners, and auditors. These people are increasingly in the position of having to carry out investigations because of the increasing incidence not only of cybercrime, but of breaches of company policies and guidelines (e.g. the abuse of Internet connections in the workplace). Cyber stalking is a new type of crime increasing in India and worldwide. So unfortunately there is no any good model present to undertake research and analyze the study. This paper presents an extended model of Cyberstalking investigations which identifies the activities of the investigative process and the major information flows in that process, an important aspect of developing supporting tools. This survey does not intend to cover cyber generated or cyber assisted attacks on governments and corporate bodies and child sexual harassment through internet. This survey is meant to analyze only individual victimization of adults and awareness among adult internet users about cyber victimization. Due to time limitation, purposive sampling method was adopted. This study is only a preliminary study; a full fledged study is planned and no generalizations should be inferred on the findings of this baseline report.

RESEARCH METHODOLOGY:

To compile our study on Cyber stalking we referenced various sources. We also took help of World Wide Web and various published books and journals. In addition to these published sources, we also referenced various websites in order to ensure the most up to date information. During the course of research and compiling these statutes from the Indian penal codes, we also

found a few additional statutes listed in the Table of Contents of the state's penal codes that were relevant to this analysis. After compiling a list of all statutes, we eliminated redundancies, any statutes specifically focused on cyber stalking, and any statutes that did not include a cyber component (e.g., stalking statutes that prohibited physical personal contact and did not include electronic communication as a type of personal contact).

We also prepared a questionnaire and collected data from 100 people from various cities online and offline. After collecting the data from questionnaire we analyzed and compiled our study. Our findings are given in key findings section of this work. The method used here allowed us to make quantitative statements about qualitative data by analyzing the prevalence of certain themes across the Country.

Considerations in selecting a research problem:

During our research of this work following points were considered: -

- Interest of the person a research endeavor is usually time consuming, and involves hard work and possibly unforeseen problems.

- Measurement of concepts: During our research and study work, we made sure that we are clear about the indicators and measurement of concepts in our study.

- Magnitude of the research: It is extremely important to select a topic that we can manage within the time and resources at your disposal. Narrow the topic down to something manageable, specific and clear.

- Level of expertise: Make sure that you have adequate level of expertise for the task you are proposing since you need to do the work yourself.

- Relevance: Ensured that our study adds to the existing body of knowledge, bridges current gaps and is useful in policy formulation. This will help you to sustain interest in the study.

- Availability of data: Before finalizing the topic, we made sure that data are available.

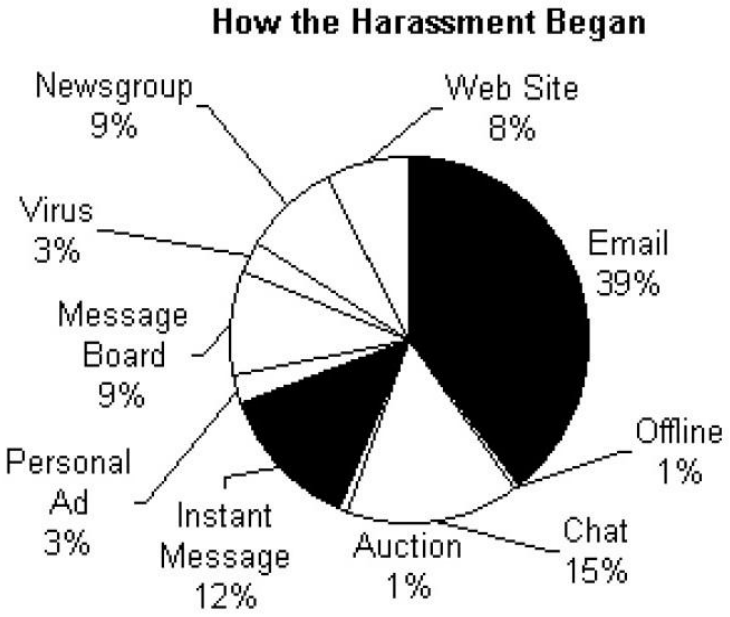
- Ethical issues: How ethical issues can affect the study population and how ethical problems can be overcome should be thoroughly examined at the problem formulating stage

FINDINGS IN RESEARCH:

Key findings

Cyber Stalking & Bullying is a not only problem in India but it's a Global Epidemic growing at fast pace where victims are harassed and there are many ill effects on the victims.

Following graph shows us an insight as how harassment began: -



Prevalence of technology

- Cyber defamation, sending threat messages etc are rampant in India. Sexual crimes in the internet are growing.

- Using bullying words in the cyber space by Indian internet users is becoming rampant.

- Very few respondents, especially women prefer to report the victimization to the police as they feel this may bring in future victimization; however, many are aware of reporting options provided by ISPs or social networking websites and some users also use these options.

- Women are more prone to victimization than men in the cyber Space.

- Most women receive mails from unknown men with disturbing contents, requests for friendship etc and such mails may be the results of data mining.

- Many women are victims of several types of harassment meted out by their former partners including former boyfriends

- Most women receive hate messages sexual / nonsexual teasing remarks, offensive comments etc due to their feministic perceptions expressed both in blogs / forum walls etc; and also for marital status, profile pictures, profile statements etc exhibited in the main profile page.

- As previously stated, Cyberstalking is increasing; however the true prevalence is currently unknown. The majority of stalking statistics come from the offline stalking population.

- Cyberstalkers use an impressively wide variety of technological means to deliver their abuse. Emails, phone calls, text messages and social networking sites are all deployed with equal enthusiasm across work, home, university or school.

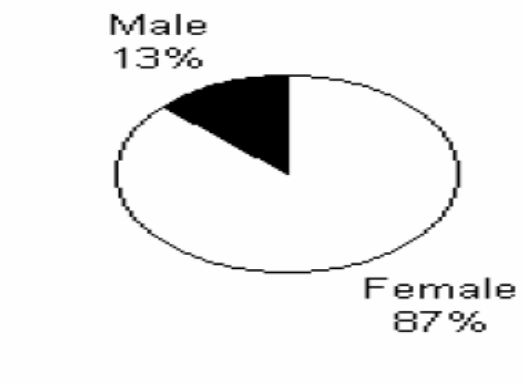
- Stalkers use technology to invade multiple aspects of their victims' lives, leaving them feeling they have no escape. The data shows that victims of multiple modes of harassment are more likely to experience more severe and adverse psychological impacts.

Victims

Currently, there are limited studies on the victims of Cyberstalking. Although, anyone has the potential to become a victim of offline stalking or Cyberstalking, several factors can increase the statistical likelihood of becoming a victim. Although studies have shown that the majority of victims are female of average socio-economic status, studies have also shown that offline stalking is primarily a crime against young people, with most victims between the age of 18 and 30. Stalking as a crime against young people may account for the high prevalence of Cyberstalking victims within universities. In addition, Working females are also being targeted by stalkers. We also found that the majority of victims of online harassment/Cyberstalking are between 18 and 30 years of age. [15]

Gender of Victim

Majority of victims are females aged between 18 to 30



Overall impact of Cyberstalking

- The psychological effects of Cyberstalking can be devastating, producing verifiable psychological trauma, regardless of whether the victim ever actually meets their harasser. The data collected by the Survey confirms that victims of electronic harassment report symptoms of post-traumatic stress disorder, as well as other adverse impacts on their day-to-day life.

- The fears created by cyber harassment behaviors are varied and extreme, varying for the individual affected. Data suggests that men are more likely to fear damage to reputation, whereas women are more likely to focus on fear of physical harm.

- Cyberstalking damages multiple aspects of victims' lives, from study to professional activity to their relationships with others. Survey respondents reported changing or losing jobs, isolating themselves by giving up social activities, and having important relationships break up.

- One clear message from the project is that many victims of cyber harassment are frustrated by a perceived lack of available help and support. Police and internet service providers are identified as primary centers of responsibility, in terms of providing preventative measures (such as effective security technologies); providing an active response to stop harassment; and providing support to those affected by Cyberstalking.

- This adds to the growing debate surrounding calls for legislative change which will allow police to act, and compel ISPs to provide formal processes and services to deter harassers and support their victims.

CONCLUSION/RESEARCH FINDINGS:

Following are the findings of our study in cyber stalking: -

- Cyberstalking is a real and a fast increasing problem in India as well as worldwide
- The true prevalence of Cyberstalking is currently unknown.
- Legal acts aimed to protect against Cyberstalking remain limited within the cyber-world.
- Studies show similarities between offline stalking and Cyberstalking.
- Most offenders are motivated to stalk/cyber stalk by failed relationships either offline or within the cyber-world.
- Most victims of stalking/Cyberstalking are young and female.
- No evidence to suggest the effects of Cyberstalking are any different than offline stalking.
- India is becoming increasing vulnerable to internet crimes such as Cyberstalking.
- Implementation of risk identification and risk management is necessary to better understand and prevent Cyberstalking.

CONCLUSION

The scenario of cyber stalking in India needs to be studied in detail. It is ironic that even though cyber victimization includes abuse of fundamental rights and also gender harassments, hardly any solid step has been taken to curb this. Most ISPs and social networking sites adhere to western cyber cultures and cyber rules and regulations which may give rise to opportunities to experiment with the personal freedoms, especially freedom of speech and expression and right to privacy. In the Indian social value system, some of such cyber cultures may give rise to severe abuse of fundamental rights guaranteed by our constitution. Matured adult internet users must understand that what is offensive in the real space, must be maintained as offensive in the cyber space also. Cyber socializing has opened the gateway to a global village which may form its own culture, rules and ethics. But that in no way should encourage abuse of personal rights and freedom.

Bibliography & References

1. http://www.in.norton.com/cyberstalking/article
2. http://www.dot.gov.in/act-rules/information-technology-act-2000
3. http://www.combatviolenceagainstwomen.org/stalking.html
4. http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm
5. http://www.cla.purdue.edu/people/engl/blackmon/101cresources/cyberstalking.htm
6. http://www.typesofbullying.org/category/types-of-bullying/cyber-bullying/
7. http://www.indianchild.com/cyberstalking.htm
8. http://www.nicfs.nic.in
9. http://www.spectacle.org/795/baker.html
10. http://www.indiankanoon.org/doc/107460954/?type=print
11. http://www.crimelibrary.com/criminal_mind/psychology/cyberstalking/5.html
12. http://www.indiancaselaws.files.wordpress.com
13. http://www.crime-research.org/library/Cyberstalking.htm
14. https://explorable.com/privacy-in-research
15. http://www.ukessays.com › Dissertations › Information Technology
16. http://www.cybervictims.org
17. https://www.takebackthetech.net/be-safe/2-cyberstalking-and-how-prevent-it
18. Book Hacking Made Easy 2nd Edition by Rajendra Maurya