CSE 4003 - CYBER SECURITY

(A1+TA1)

DIGITAL ASSIGNMENT 1

A REPORT ON CYBERSTALKING

SUBMITTED TO :Prof.Umadevi KS

SUBMITTED BY :15BCE0673 Jayitha Devineni

CYBER STALKING,A NEW CRIME: EVALUATING THE CURRENT SITUATION

I. INTRODUCTION

The Internet is a powerful tool that has brought in a new information age. If purposely misused, however, the internet can be terrifying, and even deadly. Imagine the fear generated by the following e-mail messages sent over and over again from someone who remained anonymous, but seemed to have specific knowledge of the recipient's personal life:
"I'm your worst nightmare. Your troubles are just beginning."
Or, imagine the terror experienced by a woman who discovers a website with the following message and realizes that she is the "her":
"Oh great, now I'm really depressed, hmmm ... looks like it's suicide for me. Car accident? Wrists? A few days later I think, 'hey, why don't I kill her, too? =)"

The above messages are examples of cyberstalking. Generally defined,stalking involves repeated harassing or threatening behavior. Today, advances in technology have created a new crime: cyberstalking. While there is no universally accepted definition, cyberstalking involves the use of the Internet, e-mail, or other means of electronic communication to stalk or harass another individual.

According to legaldictionary.com,
Cyberstalking involves using electronic means, including the Internet, to stalk or harass a person or group of people. Cyberstalking can include many things including threats, solicitation for sex, false accusations,defamation,slander,liberal,identity theft, and vandalism. Cyberstalking is often used in conjunction with offline stalking, as both are an expression of a desire to control, intimidate, or manipulate a victim. A cyberstalker may be someone the victim is familiar with, or a complete stranger, and is a criminal offense. ***(Fig.1)***

a. Main targets of cyberstalkers

Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators or paedophiles. A cyber stalker does not have to leave his home to find, or harass his targets, and has no fear of physical violence since he believes he cannot be physically touched in cyberspace.**[1]**

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 weak or unstable, etc. It is believed that Over 75% of the victims are female, but sometimes men are also stalked. The figures are more on assumed basis and the actual figures can really never be known since most crimes of such natures go unreported. **(Fig.2)**

b. Categories of cyberstalkers

Cyber stalkers can be categorized into 3 types:

1)The common obsessional cyber stalker

The common obsessional stalker refuses to believe that their relationship is over. One cannot be misled by believing this stalker is harmlessly in love.

2)The delusional cyber stalker

They may be suffering from some mental illness like schizophrenia etc & have a false belief that keeps them tied to their victims. They assume that the victim loves them even though they have never met. A delusional stalker is usually a loner & most often chooses victims who are married woman, a celebrity or doctors, teachers, etc.. Those in the noble & helping professions like doctors, teachers etc are at often at risk for attracting a delusional stalker. Delusional stalkers are very difficult to shake off. **[2]**

3)The vengeful cyber stalker.

These cyber stalkers are angry at their victim due to some minor reason- either real or imagined.Typical examples are disgruntled employees. These stalkers may be stalking to get even & take revenge and believe that “they” have been victimized. Ex-spouses can turn into this type of stalker.

d.Motivations of cyberstalkers

1)Sexual Harassment

Sexual harassment is also a very common experience offline. The internet reflects real life & consists of real people. It’s not a separate, regulated or sanctified world. The very nature of anonymous communications also makes it easier to be a stalker on the internet than a stalker offline.

2)Obsession for love

One of the problems with obsession stalking is that since it often starts as real romance, much personal information is shared between persons involved. This makes it easy for the cyber stalker to harass their victim. Sometimes, an obsession can also be a fixation by a stranger on another user for no valid reason. Since these obsession stalkers live in a dream world, it is not always necessary for

the target to have done anything to attract her (or his) attention in the first place. Obsession stalkers are usually jealous and possessive people. ***(Fig.3)***

(Contd..)

3)Revenge & Hate.

Revenge vendettas are often the result of something you may have said or done online which may have offended someone. Vendettas often begin with arguments where you may have been rude to another user. Sometimes, hate cyber stalking is for no reason at all (out of the blue)- you will not know why you have been targeted nor what you have done, and you may not even know who it is who is doing this to you & even the cyber stalker does not know you. **[3]**

4)Ego & Power Trips

These are harassers or stalkers online showing off their skills to themselves and their friends. Most people who receive threats online imagine their harasser to be large and powerful. But in fact the threat may come from a child who does not really have any means of carrying out the physical threats made. ***(Fig.4)***

II. CYBERSTALKING VS OFFLINE STALKING

While cyberstalking is as recent a phenomena as the Internet itself, even offline stalking is a relatively new crime. Generally, the goal of a stalker is to exert "control" over the victim by instilling fear in her; and often such conduct leads to physical action.Some experts believe that cyberstalking is synonymous with traditional offline stalking because of the similarities in content and intent.

Similarities that are pointed to include: a desire to exert control over the victim; and, much like offline stalking, cyberstalking involves repeated harassing or threatening behavior, which is often a prelude to more serious behavior. While these similarities do exist, cyberstalking differs from offline stalking infive important ways as follows :

1. Cyberstalkers can use the Internet to instantly harass their victims with wide dissemination.

The Internet is a borderless medium that allows instantaneous and anonymous distribution of one's message. In this cyber-age, websites, e-mail, chat rooms, anonymous electronic bulletin boards, instant messaging, and other web communication devices allow cyberstalkers to quickly disseminate intimidating and threatening messages. Moreover, Internet content can be widely distributed to a larger, more public forum than any conventional form of offline stalking and it can be done so inexpensively and efficiently.

For example, an offline stalker may harass the victim by repeatedly telephoning the victim. However, every telephone call is a single event that requires the stalker's action and time. This behavior can easily snowball online because, with only one action, the stalker can create a harassing e-mail message that the computer systematically and repeatedly sends to the victim thousands upon thousands of times (e.g., an "e-mail bomb").**[4]**

2. **Cyberstalkers can be physically far removed from their victim.**
Offline stalking often entails situations where the stalker is physically near the victim.The seemingly unlimited reach of the Internet makes cyberstalking distinct from offline stalking in three ways. First, it provides cyberstalkers a cheap and easy way to continue to contact their victim from anywhere in the world. Second, there is a sinister element to the secrecy of the cyberstalker's location.Finally, the physical location of the cyberstalker can create several jurisdictional problems. Because cyberstalking can easily take place across state lines, state prosecutors mayconfront jurisdictional problems in enforcing any state laws. **[5]**

3. Cyberstalkers can remain nearly anonymous.
There is a common misperception that cyberstalking is less dangerous than offline stalking because it does not involve physical contact. However, the opposite is true.While a potential stalker may be unwilling to personally confront the victim,the anonymity of the Internet allows individuals, who may not otherwise engage in offline stalking, to send harassing or threatening electronic communication.The environment of cyberspace allows individuals to overcome personal inhibitions.Anonymity makes it difficult to identify, locate, and arrest stalkers. In fact, cyberstalkers can use technologies to strip away many identifying markers from their communications.***(Fig.5)***

4. Cyberstalkers can easily impersonate the victim.
Unlike offline stalking, the cyberstalker can easily take on the identity of the victim and create havoc online. While pretending to be the victim, the cyberstalker can send lewd e-mails, post inflammatory messages on multiple bulletin boards,and offend hundreds of chat room participants. The victim is then banned from bulletin boards, accused of improper conduct, and flooded with threatening messages from those the stalker offended in the victim's name.

5. Cyberstalkers can encourage "innocent" third-party harassment.
Cyberstalkers can incite other "innocent" third parties to do their stalking for them.For example, in California, a fifty-year-old defendant used the Internet to solicit the rape of a twenty-eight-year-old woman who had rejected the defendant's romantic advances. The defendant then terrorized her by impersonating her in various Internet chat rooms and posting her telephone number, address, and messages that she fantasized of being raped. Because of these messages, on separate occasions, at least six men knocked on the woman's door saying that they wanted to rape her.
In many ways, the Internet makes many of the frightening characteristics of offline stalking even more intense. It provides cyberstalkers with twenty-four-hour access, instantaneous connection, efficient and repetitious action, and anonymity. It is for these reasons that the laws should be updated to deal with this new crime. ***(Fig.6)***

III. EXAMINING THE CRIMINAL ELEMENTS OF CYBERSTALKING

Cyberstalking and offline stalking should share the same intentional mental state requirement; but to be effective, cyberstalking statutes should criminalize conduct that either puts a "reasonable person" in fear of bodily harm or causes severe emotional distress.Furthermore, the cyberstalking statute should specifically address situations where the cyberstalker entices third parties to harass for them.

1.The "intentional" mens rea requirement.

As far as cyberstalking is concerned, this "intentional" mental state requirement is appropriate. The point of cyberstalking laws, much like offline stalking statutes, should be to stop individuals from purposefully causing another to fear. Like an offline stalker, a cyberstalker should have to "intentionally" engage in conduct that causes his target to fear for her safety (or should have known would cause fear for her safety).**[6]**

2. The need to criminalize a "course of conduct" that would cause a "reasonable person" to fear for her safety.

Firstly, most offline stalking statutes require the conduct be "repetitive." In other words, to be in violation of the law, thestalker has to engage in conduct at least more than once in such a way that causes the victim to fear. It is appropriate to require that the cyberstalker engage in "repeated" conduct; e.g., e-mailing a harassing message more than once; or posting a message on a website that causes others to harass the victim more than once. **[7]**Moreover,punishing merely one instance of harassing conduct may unjustly penalize one who acts once out of anger, verses one who engages in a series of terrifying acts.The second consideration is where the real issue arises when offline stalking laws are applied to cyberstalking.

3. Criminalizing situations where the cyberstalkers entice "innocent" third-parties to harass.

One of the most apparent differences between cyberstalking and stalking is that cyberstalkers can entice third parties to do the work for them. Currently, only Ohio has taken the approach to specifically crinminalize such behavior.So that neither cyberstalkers nor victims are unclear that this conduct is criminal, statutescriminalizing cyberstalking should directly provide that no person should use the Internet to cause anotherto engage in conduct that would cause a reasonable person to fear for her safety.

(Fig.7)

IV. CURRENT LAWS DEALING WITH CYBERSTALKING

Prior to February 2013, there were no laws that directly regulate cyberstalking in India India's Information Technology Act of 2000 (IT Act) was a set of laws to regulate the cyberspace. However, it merely focused on financial crimes and neglected interpersonal criminal behaviours such as cyberstalking (Behera, 2010; Halder & Jaishankar, 2008; Nappinai, 2010).

In 2013, Indian Parliament made amendments to the Indian Penal Code, introducing cyberstalking as a criminal offence.Stalking has been defined as a man or woman who follows or contacts a man or woman, despite clear indication of disinterest to such contact by the man or woman, or monitoring of use of internet or electronic communication of a man or a woman. A man or a woman committing the offence of stalking would be liable for imprisonment up to three years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to five years and with fine.

Cyberstalking Legislation

The IT Act needs to be amended to take into account cyber-stalking and cyber-bullying, which are the two most under-reported offences in Indian schools and colleges. "Nine of 10 victims of cyber-stalking are women. The IT Act's section 66A gave some protection against cyber-stalking." That law, however, was challenged as sweeping and draconian, and struck down by the Supreme Court in March.

Apar Gupta, an advocate who argued against 66A in the court, disagrees, saying there's enough in existing laws to tackle cyber crimes like stalking and vicious trolling, especially "after Nirbhaya". "It isn't that cops have problems just with cyber-crime complaints," he says. "They are reluctant to file most complaints, because it increases their burden."**[5]**

Experts and victims both agree that it's very challenging to do anything about vicious trolling online."I faced all the harassment, even the court summons," Ms Krishnan says. "Nothing happened to my abusers. So I would think 20 times before making a police complaint. Even when I write to Twitter pointing out a gang-rape threat, Twitter writes back saying it doesn't violate their community guidelines." ***(Fig.8)***

V . PROBLEMS WITH CRIMINALIZING CYBERSTALKING

There are at least two potential concerns related to criminalizing cyberstalking. First, anytime speech is involved, many constitutional issues arise.Second, to date, the cyberstalking data that has been collected is somewhatuncertain. While each of these potential concerns merit more discussion, theydo not create a complete barrier to criminalizing cyberstalking.

A. Constitutional Considerations

As with offline harassment laws, cyberstalking laws need to be relatively broad to be effective. However, they cannot be so broad as to impinge upon the rights of free speech protected under the First Amendment. Thus,any interpretation of existing harassment laws and changes in stalking statutes should keep in mind that, as with offline stalking, cyberstalking should generally involve conduct reasonably understood to constitute harassing and threatening behavior.**[7]**
Constitutional concerns are not implicated when statutes prohibit the matter and means of the telephone call and have an element of specific intent to harass the person called. Thus, telephone harassment statutes that have a specific intent element are constitutional when they prohibit repeated, anonymous, or late-night calls.Likewise, statutes related to cyberstalking should focus on specific intent, conduct-based behavior such as repeated transmission of e-mails (e-mail "letter bombs"), or use of lewd language with the intent to harass.

Thus, as long as statutes aimed at cyberstalking contain the following two elements, it will probably not be unconstitutionally vague or overbroad:
(1) "willfully" harasses, follows, engages in conduct, etc. ensures that the perpetrator has the requisite specific intent to commit a crime, and
(2) a provision stating that the law does not include "constitutionally protected activity," including, but not limited to "picketing and organized protests."

B. Lack of Cyberstalking Data

An evidence of whether cyberstalking is indeed becoming a societal problem is largely anecdotal and informal. In fact, law enforcement agencies from different jurisdictions report widely different statistics on stalking via the Internet. However, those jurisdictions that have computer crime departments tend to report a larger number of cyberstalking incidents. The lack of data is partly because many cyberstalking victims do not report the conduct to law enforcement, and partly because law enforcement agencies have not had adequate training in how to deal with it.187 However, there are some reports that suggest that cyberstalking is ever-growing. **[8]**

(Fig.9)

VI. CYBERSTALKING CASES IN INDIA

CASE I

In India’s first case of cyberstalking, Manish Kathuria 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 slamed a case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli.

CASE II

When a Mumbai court recently sent Yogesh Prabhu, 36, an executive in a private company, to jail for three months, it was a tiny landmark.This was India's first conviction for cyber-stalking since cyber-laws came into existence in 2000. In March 2009, Prabhu had sent a series of emails from an anonymous address to a colleague who had earlier rejected his proposal. "I would go to a movie, and then get an anonymous email saying, How was the movie, you enjoyed it?" says the woman, whose identity is protected by law.The police tracked down the IP address of the sender, and arrested Prabhu a month later.

This isn't, however, the first cyber-stalking case in India. That was in 2001, when Manish Kathuria was arrested by the Delhi police for impersonating a woman in an internet chatroom. Kathuria was charged under a section of the Indian Penal Code (IPC) for "outraging the modesty" of his victim Ritu Kohli: he would pretend to be her, use obscene language, give out her home phone number and invite callers. That IPC section, however, did not cover internet crimes, and Pavan Duggal, Delhi-based cyber-law expert who worked on the case, explains that it finally fizzled out when a frustrated Ms Kohli moved out of India. ***(Fig.10)***

VII. PROTECTING YOURSELF AGAINST CYBERSTALKING

People who believe they are victims of cyberstalking. The first step should be to demand the stalker to stop all contact and stop the harassing actions. Additionally, in order to facilitate prosecution of the perpetrator, the victim should:**[3]**

- Save all e-mails, messages and other communications for evidence. It is vital that these are not altered in any way and that the electronic copies are kept, rather than only printouts.
- Save all records of threats against the victim's safety or life. This includes any written or recorded threats and logs of the date, time and circumstances of verbal threats.
- Contact the perpetrator's internet service provider. Internet service providers (ISP) prohibit their users from using their service to harass others. Contacting the ISP may result in discontinuation of the harasser's internet service and will put the ISP on notice to maintain record of the harasser's internet use.
- Keep detailed records of contacts with ISP and law enforcement officials. It is important to keep a log of all reports made to any agency or provider, and to obtain copies of the official reports when available.

(Fig.11)

VIII. CONCLUSION

As technology changes, so should the laws. For example, with the increased and daily use of cars, the laws had to change to make driving under the influence of alcohol a crime. Similarly, the stalking and harassment laws should be reviewed to ensure that they are adequate to address the new crime of cyberstalking.

Cyberstalking is a crime with issues that are distinct from offiine stalking such that current state and federal laws are inadequate to deal with all aspects of cyberstalking. Thus, cyberstalking laws should be enacted that have the reasonable person standard and also explicitly deal with situations
where the cyberstalker dupes "innocent" third parties to do the stalking.Clear federal and state laws which specifically prohibit cyberstalking may address this problem. If victims knew of the laws, they might be more encouraged to report incidents. And, if cyberstalkers knew of the laws, they might be less likely to stalk victims online. Moreover, clear cyberstalking laws would give guidance to law enforcement agencies on how to appropriately respond to reported incidents.

At the end of the day, it is important to recognize that the new age of the internet is creating a host of cybercrimes; cyberstalking is one of them. Statues should be evaluated to ensure the technology, as fast-paced as it is, does not go beyond the reach of the law.***(Fig.12)***

IX . LIST OF FIGURES

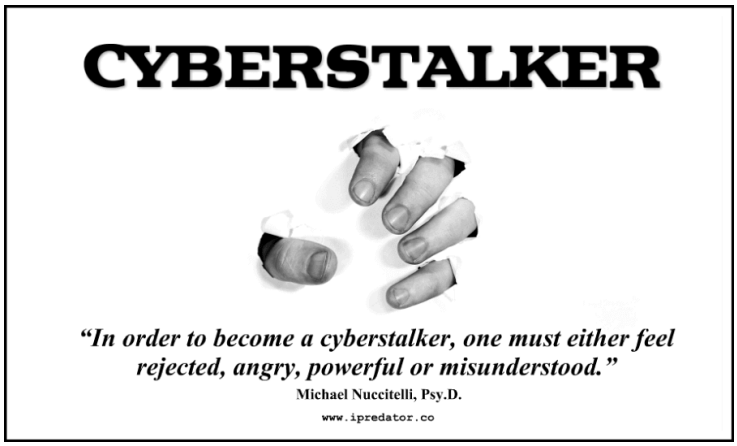

Fig.1 Describing why does a person opt for cyberstalking

Fig. 2 A cybersatlker maybe may be on the other side of the earth or a neighbour or even a relative! And a stalker could be of either sex.

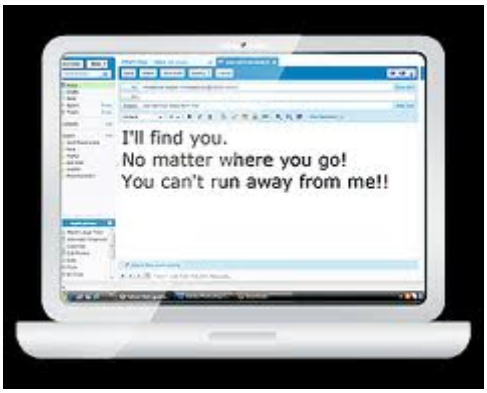

Fig.3 Death threats via email or through live chat messages are a manifestation of obsession stalking.

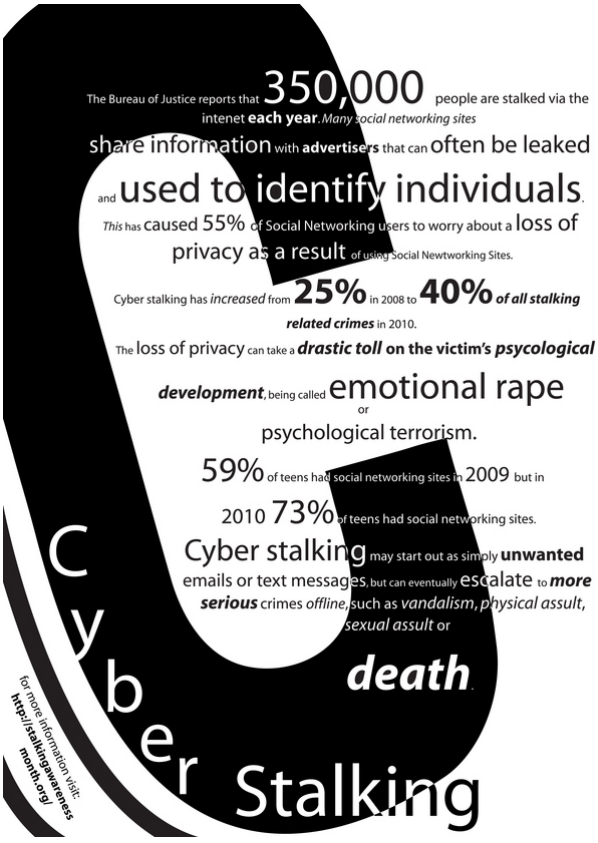

Fig .4 is estimated that there are about 2,00,000 real-life stalkers in America today. Roughly one in 1,250 persons is a stalker – and that is a large ratio. Of course, no one knows the truth, since the Internet is such a vast medium, but these figures are as close as it gets to giving statistics. Out of the estimated 79 million population worldwide on the internet at any given time, we could find 63,000 internet stalkers travelling the information superhighway, stalking approximately 4,74,000 victims.

Fig.5 Cyberstalkers can use the Internet to terrify their victims no matter where they are; thus, they simply cannot escape.

Fig .6 The possibilities open to cyberstalkers are as endless as the borders of the ubiquitous Internet.

Fig . 7 NO ONE has a right to harass, threaten and disturb you. Once harassment becomes a threat against you, then the harasser has also broken the law .

Fig.9 Since 1997,f(r)iend or fiund ? you never know who you are dealing with !

Fig .10 A comic strip depicting woman empowerment to raise their voice against cyberstalking.

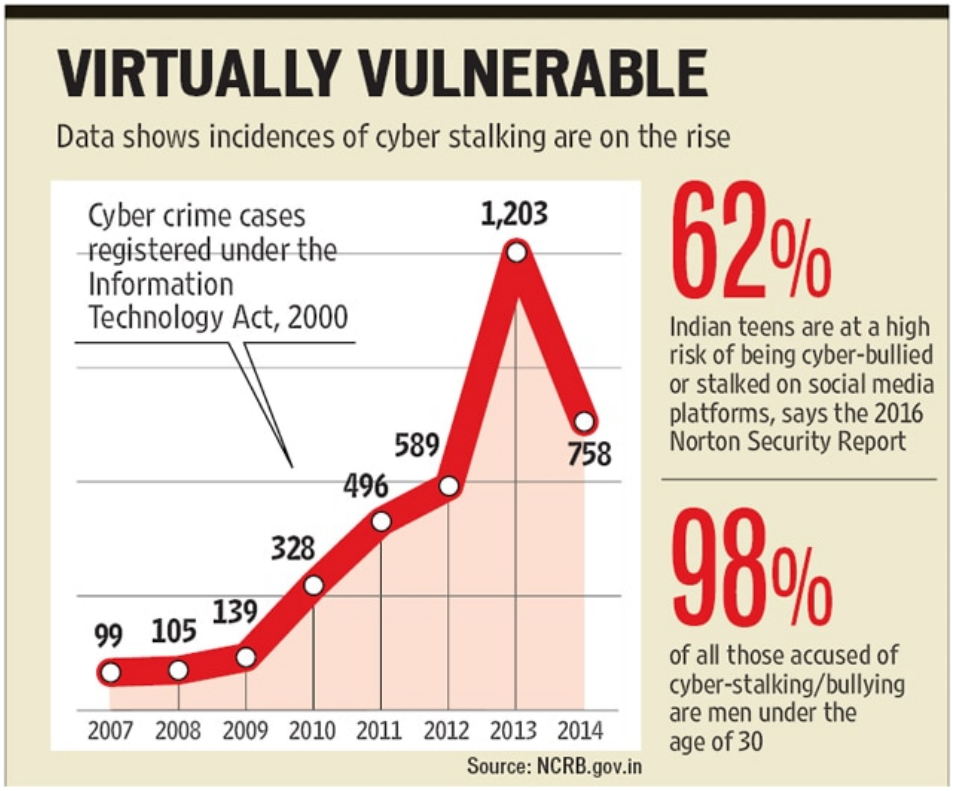

Fig.11 Cybercrime reports data

Fig.12 Poster

X. REFERENCES

[1] Cyber-stalking: the Regulation of Harassment on the Internet
[2]Cyber Stalking : A Challenge for Web Security
[3]https://preesha.wordpress.com/2010/10/15/introduction-to-cyberstalking/
[4]www.legaldictionary.com
[5]www.cybercrimeindia.com
[6]Sinwelski, S., & Vinton, L. (2001). Stalking: The constant threat of violence. Affilia, 16, 46-65.
[7]Goode, M. (1995). Stalking: Crime of the nineties? Criminal Law Journal, 19, 21-31
[8]Meloy, J. R., & Gothard, S. (1995). Demographic and clinical comparison of obsessional followers and offenders with mental disorders. American Journal of Psychiatry, 152(2), 25826.
[9]Fremauw, W. J., Westrup, D., & Pennypacker, J. (1997). Stalking on campus: The prevalence and strategies for coping with stalking. Journal of Forensic Sciences, 42(4), 666-669
[10]No Law to Tackle Cyberstalking. (2004). The Economic Times. http://ecoonomictimes.indiatimes. com/articleshow/43871804.cms