VOLUME 5 ISSN: 2456-9704

STALKING THE STALKER SAVINGS THE VICTIM

By Maahi Mayuri
From New Law College, Pune

ABSTRACT

With the rise in Information Technology, emergence of new ways of communication, social networking becoming indispensable and innovations in the field of computers, cyber crimes are gaining momentum, and it is now emerging as one of the most vulnerable crimes. Thus, India facing it becomes inevitable. It is now becoming more common than physical annoyance. Hence it becomes vital to look into its types, analyse its incidents and thus look into the related laws. By this research, we aim to provide a more clear understanding of the definition of cyberstalking, its prevalence, characteristics of both the victims and offenders of this crime, the modus operandi of the crime and the goal is to answer the question whether the India Judiciary is efficient enough to tackle the problem.

Keywords: CyberStalking, CyberStalker, Ingredients of CyberStalking, Information Technology Act

1. INTRODUCTION

Increased dependence of humans on Information Technology has brought with it, some boons as well as curses. We find new technologies and innovations everyday. But the growing global village, does have a dark side to it. The evil of cyber stalking has spread its roots deep down in almost every digital aspect.

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten, embarrass or harass. . Internet has thus become an easy medium for frauds, sexual exploitation, exploiting or harassing. It most commonly happens with with females, teenagers or children.

Cyber stalkers do not fear physical violence since they cannot be physically reached in the virtual world. From a friend, a colleague, a relative, or even a stranger, anyone could be a cyber stalker. Those on the target list most commonly involve those who are Internet addicts, emotionally weak or unstable. But, this does not limit its scope, even a person of ordinary prudence, with no internet addiction could fall prey to cyber stalking. Most of the cyber stalking incidents go unreported and hence their true number can never be truly known.

VOLUME 5 ISSN: 2456-9704

2.1 NATURE OF STUDY

The mode of reseach is non emperical, i.e Doctrinal in nature wherein Secondary Data has been relied upon. It is based on information and interpretations.

2.2 SCOPE OF RESEARCH

This research covers the problem of cyber stalking as a whole prevalent in India, as well as its legal remedies. This research aims to develop a clear understanding of cyberstalking, its types, prevalence, characteristics of victims and offenders, its modus operandi and its redress under the Indian Judicial System.

3. IMPORTANCE AND SIGNIFICANCE

The 21st century is the era of Information and Communication Technology. With everything going digital, it thus becomes necessary with its associated evil. Cyberstalking being one of the most prevalent and vulnerable crimes, among cyber crimes, it thus becomes necessary to look into the problem.

4. LITERATURE REVIEW

- Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi (2015. "*Cybercrime, Digital Forensics and Jurisdiction*". Springer.
- Zona, M.A., Sharma, K.K., & Lane, M.D. (1993). "*A Comparative Study of Erotomanic and Obsessional Subjects in a Forensic Sample*"
- Christopher Reed (2000). "*Internet Law; Text and Materials*" Cambridge University Press
- Bocjj Paul (2003). "*Victims of cyber stalking: An exploratory study of harassment perpetrated*" via the Internet First Monday, volume 8, number 10 (October 2003),
- URL: http://firstmonday.org/issues/issue8_10/bocij/index.html
- Vakul Sharma (2011). "I*nformation Technology-Law and Practice,3rd Edn.* New Delhi:Universal Law Publishing Co Pvt.Ltd.

5.1. AIMS AND OBJECTIVES

1. To study the rising problem of cyberstalking in India
2. To analyse the psychological reasons behind cyberstalking
3. To analyse the redress available for cyberstalking under the Indian Judiciary

5.2. RESEARCH QUESTIONS

1. What is Cyberstalking?
2. What are the psychological reasons behind the phenomenon?
3. Are the provisions in the Indian Judiciary enough to deal with the problem?
4. What can be done to improve the condition?

VOLUME 5 ISSN: 2456-9704

6. HYPOTHESIS

We thus hypothesize that provisions available under the Indian Judiciary & the IT Act are not stringent enough to efficiently deal with the offence of cyberstalking.

7. CYBER STALKING AND ITS PREVALANCE

7.1. WHAT IS CYBER STALKING?

Numerouse have been made to define cyberstalking by a various experts and legislators.

Elements

1. Involves the use of Internet or other electronic means. Computer is essentially an element of cyber criminality and it is either a tool or target of cybercrime.
2. Cybercrime can be committed without any physical contact.
3. The use is to stalk, harass or exploit an individual, a group, or an organization.
4. Identity of the person using cyber stalking space remains unknown
5. It is a form of cyberbullying
6. May include false accusations, defamation, slander or libel.
7. May also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.
8. May be accompanied by real-time or offline stalking.
9. It transverses jurisdictional boundaries. Presence of the offender is not required and crime can be committed from anywhere in the world with a mouse click.

Technology ethics professor Lambèr Royakkers defines cyberstalking as perpetrated by someone without a current relationship with the victim. About the abusive effects of cyberstalking, he writes that:

"[Stalking] is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together (cumulative effect)."

7.2. DISTINGUISHING CYBERSTALKING FROM OTHER ACTS

Distinction between cyber-stalking & other acts becomes necessary so as to understand the phenomenon better. According to Wikipedia, the following is the difference between cyber-stalking & cyber-bullying. Harmless actions can be

perceived as cyber bullying but cyber-stalking is repetitive and persistent.

TM	Motive	Mode	Gravity	Description
1	Playtime	Cyber-bantering	Cyber-trolling	In the moment and quickly regret
2	Tactical	Cyber-trickery	Cyber-trolling	In the moment but don't regret and continue
3	Strategic	Cyber-bullying	**Cyber-stalking**	Go out of way to cause problems, but without a sustained and planned long-term campaig
4	Domination	Cyber-trickery	**Cyber-stalking**	Goes out of the way to create rich media to target one or more specific individuals

7.3. IDENTIFICATION

CyberAngels has written about how to identify cyberstalking:

When identifying cyberstalking "in the field," and particularly when considering whether to report it to any kind of legal authority, the following features or combination of features can be considered to characterize a true stalking situation: malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, personally directed, disregarded warnings to stop, Bharassment and threats.

7.4. STATISTICS

Cumulative Statistics for the year 2000-2013 by WHOA (Working to Halt Online Abuse)

Cumulative statistics for the years 2000-2013	
353 for calendar year 2000	256 for calendar year 2001
218 for calendar year 2002	198 for calendar year 2003
196 for calendar year 2004	443 for calendar year 2005
372 for calendar year 2006	249 for calendar year 2007
234 for calendar year 2008	220 for calendar year 2009
349 for calendar year 2010	305 for calendar year 2011
394 for calendar year 2012	256 for calendar year 2013

8. TYPES OF STALKERS

8.1 CATEGORIES OF STALKERS

Cyber stalkers can be categorized into three types.

a) The common obsessional cyber stalker: He/She refuses to believe that their relationship is over. They mislead by portraying that they are harmlessly in love.

b) The delusional cyber stalker: They may suffer from mental illness like schizophrenia etc. Having a false belief that they are tied to their victims, they commit the offence. They assume that their victim loves them . A delusional stalker is usually a loner/ Those in the noble and helping professions like

doctors, teachers etc are often at risk for attracting a delusional stalker. Delusional stalkers are very difficult to shake off. Celebrities are often the most common prey.

c) 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 and take revenge and believe that they have been victimized. Ex-spouses can turn into this type of stalker.

2. PSYCHOLOGY OF CYBER STALKERS

1. The Rejected Stalker: This type of stalking is generally connected with a relationship with the victim. Either it is due to the break up of a relationship and the partner who ends the relationship is generally the victim. Personality traits of such stalker can include Egotism, Jealousy, Humiliation, Over-dependence & bad social skills. Stalking behaviors can be intrusive as well as persistent. The victim may face extortion and assault. Violence is generally involved in the relationship. The stalking type is generally the sturdiest when it comes to studying the criminality.
2. The Resentful Stalker: The stalkers personality may be irrationally paranoid. This kind of stalking is mainly done to seek revenge from the victim and thus scare and harm them. The victim may have humiliated the stalker in the past. Verbal threats, Obsessive Stalking & physical assault.
3. The Predatory Stalker: This form generally involves the stalker seeking sexual advantage over the victim. Sexual assaults are most likely to occur. Generally people with lower than normal intelligence, poor social skills, poor self esteem & those who are sexually deviant indulge in this type of stalking. Behavior can include monitoring the victims activities, obscene phone calls & messages, fethism, etc
4. The Intimacy Seeker: The stalker who indulges in such behavior is usually shy, isolated & wishes to establish a romantic relationship with the victim. He/She believes they can be the "only one" for thr victim who can satisfy their desires. If rejected, they may resort to violence & deviant behavior. Most cases of one sided love result into this type of stalking. They send the victims messages, letter & make phone calls expressing their love. Such stalkers do not bother about the legal implications of their acts because they think they are just challenges to overcome & a test to their love.
5. Incompetent Suitor: Similar to the intimacy seeker but they feel that any woman should be attracted to them.

VOLUME 5 ISSN: 2456-9704

They constantly pursue the victim & ask for dates or a romantic or intimate relationship. The stalker may have stalked several others. They may have lower than normal intelligence but may stop stalking if counselled or informed about legal implications of their acts.

8.3. STATISTICS

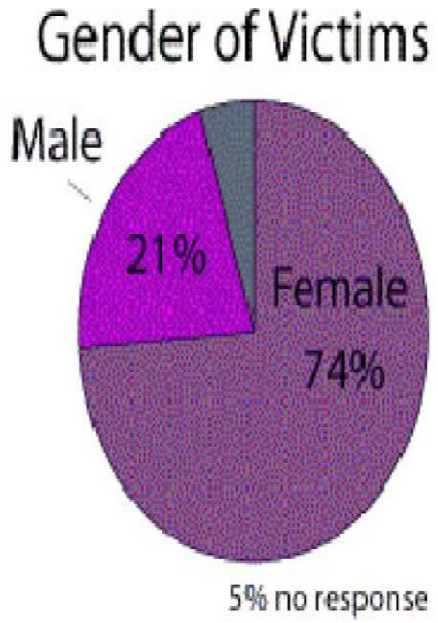

Figure 1: Cyber stalking statistics (source: Working to Halt Abuse Online)

9. TYPES OF CYBER STALKING

Easy availability of internet at low costs facilitates stalkers to it as a means to stalk people. Cyber stalkers use three different ways for stalking their target.(Ogilvie, 2000)

a. Email Stalking: Direct Communication through E-mail

b. Internet Stalking: Global communication through the Internet

c. Computer Stalking: Unauthorized control another person's computer

a. EMAIL STALKING: Email or electronic mail is the most commonly used network based application. Today, it has become the most common way to harass, threat or stalk a person. Stalkers send spontaneous mails in which lead to nuisance, hatred, obscenity or threats. Such stalkers repeatedly send mails to their victims for and try to iniatiate or fix a relationship or threaten and hurt a person.

This form also includes harassment by sending viruses or high volume of electronic junk mail to the victim. However, just sending viruses or telemarketing solicitations alone does not constitute stalking. But, if such communications are repetitive & in a manner which intimidates, then it may constitute concerning behaviors which can be categorized as stalking.

b. INTERNET STALKING: Stalkers comprehensively use the Internet to slander and endanger their victims. Cyber stalking takes on a public dimension. What makes it disturbing is that it appears

to be the most likely to spill over into physical space. Generally, cyber stalking is accompanied by traditional stalking behaviors such as threatening phone calls, vandalism of property, threatening mail, and physical attacks. There are important differences between the situation of someone who is regularly within shooting range of her/his stalker and someone who is being stalked from two thousand miles away.

c. COMPUTER STALKING: In this type, the stalker, by unauthorized access, controls victims computer. The stalker can thus communicate directly with his victim when the target computer connects to the Internet. Stalker assumes control of the victims computer and the only defense left for the victim is to renounce their current Internet "address"

More recent versions of this technology claim to enable real-time keystroke logging (keylogger) and viewing the computers desktop real time. It is not difficult to hypothesize that such mechanisms would appear as highly desirable tools of control and surveillance for those engaging in cyber stalking.

10. MODUS OPERANDI

According to Van Wilsem (2011, p.124) and Wykes (2007, p.167) stalkers often take advantage of the personal information stored on network sites, hard drives of personal computers, laptops, and smart phones to learn more about their victims. Some of the more industrious cyberstalkers also collect personal information about their victims through the use of hardware devices installed on the victim's computer to monitor key strokes, which enable the collection of passwords, PIN numbers, email accounts, and other personal information. Cyberstalkers may also use spyware software, which is available free over the internet or for purchase. Spyware allows a person anonymously to monitor the internet activity and habits of a target (Cox & Speziale 2009; Southworth, Finn, Dawson, Fraser, & Tucker, 2007, p.848; Reyns, et al., 2011; Wykes, 2007). Stalkers have also been known to use college campus computers and their internal networks to commit their cybercrimes (Peak, Barthe, & Garcia, 2008, p.257)

11. INCIDENTS OF CYBER STALKING

- **Manish Kathuria v. Ritu Kohli (2001)**
-

This is the first reported case of cyber-stalking in India and the reason behind the 2008 amendment to the IT Act, it involved the stalking of a woman named

VOLUME 5 ISSN: 2456-9704

Ritu Kohli. Manish Kathuria followed Kohli on a chat website, abused her by using obscene language and then disseminated her telephone number to various people. Later, he began using Kohli's identity to chat on the website "www.mirc.com". As a result she started receiving almost forty obscene telephone calls at odd hours of the night for over three consecutive days. This situation forced her to report the matter to the Delhi Police. As soon as the complaint was made, Delhi Police traced the IP addresses and arrested Kathuria under Section 509 of the Indian Penal Code. The IT Act was not invoked in the case, since it had not come into force at the time when the complaint was filed.

While there is no record of any subsequent proceeding, this case made Indian legislators wake up to the need for a legislation to address cyber-stalking. Even then, it was only in 2008 that Section 66-A was introduced. As a result, cases started being reported under this section as opposed to Section 509 of the Indian Penal Code, as was the case where a Delhi University student was arrested for stalking a woman from Goa by creating fake profiles on social networking websites, uploading pictures on them and declared herto be his wife. It is hoped that the decision in this would favour the victim.

However, in 2015, Section 66A was struck down as unconstitutional by the Supreme Court for being violative of Section 19(1)(a) of the Indian Constitution.

- **Karan Girotra v. State**
- The facts of the case are that Shivani Saxena, daughter of Sudhir Saxena, had lodged a complaint with the Police that she had married Ishan on 25.9.2009, however, the marriage between them failed within a few days as her husband, Ishan could not consummate the marriage. Both of them started living separately w.e.f. 1.10.2009 and it was amicably settled between them that after the expiry of one year of their marriage, both of them will file a joint petition, on mutual consent, for the grant of divorce, after which both the parties will be free to marry afresh.
-

It is further alleged by her that in the course of chatting on the internet, she had come in contact with Karan Girotra, about six years back from the date of the lodging of the complaint. On 3.4.2010, the petitioner is alleged to have told her that he had fallen in love with her and wants to marry her. On this, she allegedly told him that she is already married, whereupon the petitioner said that he would marry her after her divorce. On 15.5.2010, it is alleged that on the pretext of introducing the complainant to his

family members, the petitioner called her to his house, where she found that there was nobody except his old bed-ridden maternal grandmother. It is alleged by her that, at about 8:00 P.M., the petitioner gave her soft drink, which was perhaps laced with some intoxicant and on consuming the same, she became unconscious. It is stated that when she regained her consciousness at about 10:00 P.M., she found herself completely nude and she also noticed that she had been sexually assaulted. On noticing this, she started crying and she was consoled by the petitioner that she need not worry, as he would fulfill the commitment of marrying her. On 16.5.2010, she was shocked when she received her obscene pictures of the previous night. She confronted the petitioner with the said pictures, whereupon the petitioner represented to her that she need not worry about this and he is going to marry her. It has also been alleged that the petitioner threatened to circulate the objectionable pictures everywhere if she did not keep on maintaining physical relations with him. On the basis of this blackmail, she alleged that she was raped again on 18.5.2010. Subsequent thereto, on 9.7.2010, it is stated that a roka ceremony was held between the petitioner and the complainant at the restaurant i Delhi, where the mother of the complainant gifted the petitioner a santro car, jewellery, clothes and various other gift items. It has been alleged that the petitioner kept on sexually assaulting the complainant without her consent and on 12.9.2010, the petitioner informed the complainant's mother that he is breaking the engagement and he returned the car and the other articles, whereupon the complainant lodged a complaint in the month of June and the aforesaid FIR under Sections 328/376 of IPC read with Section 66A of the I.T. Act was registered by PS: Prashant Vihar, Delhi against the petitioner. As a result, Saxena filed a complaint under Section 66-A of the IT Act. Though the Court rejected the plea of anticipatory bail on the ground that nude and obscene pictures of Saxena were circulated by Girotra, an act which requires serious custodial interrogation, nonetheless it made some scathing remarks. According to the Court Saxena had failed to disclose her previous marriage to Girotra merely because she agreed to perform the engagement ceremony, even though such mention was made when Girotra had first professed his love to Saxena. The Court also took noted that there was a delay in lodging the FIR by Saxena. What is more shocking is that the Court held that Saxena had consented to the sexual intercourse and had decided to file the complaint only when Girotra refused to marry her.

This case highlights the attitude of the Indian judiciary towards cases involving cyber-stalking. It is appalling that factors as redundant as a delay in filing the FIR

have a huge bearing on the outcome of the case. It is for this reason that more stringent legislations are the need of the hour

12. RELATED LAWS AND ANALYSIS

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. In 2013, Indian Parliament made amendments to the Indian Penal Code, introducing cyberstalking as a criminal offence.

1. 12.1. The Information Technology Amendment Act, 2008

The Information Technology Act of 2000 was enacted with an aim to recognize electronic records and facilitation of e-commerce. To this extent, hardly ten sections were incorporated that actually dealt with cybercrime. One of these was Section 67, which dealt with the publishing or transmitting of pornographic material through a computer resource. It did not consider the need for specialized provisions regarding child pornography. However, it is pertinent to note that this Act was a significant step forward from the existing law.

The IT Act, 2008, however, does not directly address stalking. The problem is dealt as an "intrusion on to the privacy of an individual" than as regular cyber offences.

The most used provision for regulating cyberstalking in India is Section 72 of the IT Act, 2008.

Penalty for breach of confidentiality and privacy: Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, 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.

Section 72A: Punishment for disclosure of information in breach of lawful contract: Save as otherwise provided in

VOLUME 5 ISSN: 2456-9704

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 fine which may extend to five lakh rupees, or with both.

Cyber stalking is generally a bailable offense unless it causes severe defamation, sexual crimes, identity theft or terrorism.

Under the Indian Penal Code, 1860, the Indian Post Office Act, 1898 and the Indecent Representation of Women (Prohibition) Act, 1986, only obscene visual representations were the focus of the legislation. It left out audio materials and simulated images—both of which are recognized internationally.

As far as Indian constitutional jurisprudence is concerned, obscenity is not a protected expression under Article 19(1) (a), and thus can be validly restricted under Article 19(2) on the ground of decency or morality. When obscenity is judged as per the proper tests, and is deemed to be obscene by the court, there can be no allegation of a violation of Article 19(1) (a). It is in this pursuance of removing the obscene material from the website that the site is blocked under the IT Act. Prohibition is merely a form of restriction of a fundamental right. As such, the object of the block is to prevent users Internet from accessing that material.

12.2. The Criminal Law (Amendment) Act, 2013

The act added Section 354D in the Indian Penal Code, 1860 which defines "Stalking" and provides punishment for the same.

(1) Any man who—

1. 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
2. monitors the use by a woman of the internet, email or any other form of electronic communication,
3. commits the offence of stalking;
4.
5. 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.

6. **12.3. Following sections of IPC deal with the various cyber crimes:**

- Sending threatening messages by e-mail (Sec .503 IPC)
- Word, gesture or act intended to insult the modesty of a woman (Sec.509 IPC)
- Punishment for criminal intimidation (Sec.506 IPC)
- Criminal intimidation by an anonymous communication (Sec.507 IPC)
- Obscenity (Sec. 292 IPC)
- Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail
- (Sec.292A IPC)
- Obscene acts and songs (Sec.294 IPC)
-

12.4. Problems in Enforcement

"Even with the most carefully crafted legislation, enforcing a law in a virtual community creates unique problems never before faced by law enforcement agencies."(Ellison 1988)

"These pertain mainly to the international aspects of the Internet. It is a medium that can be accessed by anyone throughout the globe with a computer and modem. This means that a potential offender may not be within the jurisdiction where an offence is committed. Anonymous use of the Internet also promises to create challenges for law enforcement authorities."

Thus, anyone can fall prey to cyberstalking.

13. POSSIBLE REMEDIES (PREVENTIVE MEASURES THAT CAN BE TAKEN)

1. The Need for New Legislation

Effective legislations need to be enforced which provide stringent provisions for the offence of cyberstalking. The problem of jurisdiction should also be addressed by laws as Internet Crimes are not limited to a single territory.

2. Awareness

2. Apart from the judiciary taking action, people need to be aware about the problem. They should know what can cause a possible threat to them, and their code of conduct while in the global village.

3. **3. Following the "Prevention is better than Cure" Rule**

4. Users need to be cautious while interacting online. They should not share their personal information online, reveal the same to strangers. They should also make it a rule to save messages that are harassing or threatening in nature.

5.

VOLUME 5 ISSN: 2456-9704

6. 14. CONCLUSION

In 17 years since the Information Technology Act of 2000 was passed, dozens of cyberstalking incidents have been reported, but many more go unreported. The main reason behind this, is that the authorities who are concerned with registering such complaints or taking action in such matters are more comfortable with the traditional laws for the physical world.. Section 354D of the Indian Penal Code, covers stalking & not cyber-stalking except for the monitoring of a woman's communications by a man.

It is the need of the hour that the IT Act be amended to take into account cyber-stalking and cyber-bullying, which are the two most under-reported offences in the Indian society. The cases we looked into in our research also indicate that no serious consequences are faced by cyber stalkers and they easily get away with the offence.

90% of the victims of cyber-stalking are women. The IT Act's section 66A gave some protection against the same but it was challenged as unconstitutional, and was struck down by the Supreme Court in March 2015.

We've already seen that under Section 72 & 72A of the IT Act, 2008, the maximum imprisonment is 2 years and 3 years respectively. Likewise Section 354D of IPC provides a maximum imprisonment of 5 years. The level of punishment thus provided under these sections are therefore not enough to further stop these crimes.

Cyber stalking often leads the victim to suffer from extreme mental agony, financial crisis, depression and often leads the victim to commit suicide. Victims report a number of serious consequences of victimization such as increased suicidal ideation, fear, anger, depression, and post traumatic stress disorder (PTSD) symptomology.

Creating such circumstances for a person should be strictly punished. Till date, there is no legislation in the Indian Judicial System that is efficient enough to deal with, and prevent, the incidents of cyberstalking.

We thus conclude that our hypothesis is proved to be correct that the Indian Judiciary is not efficient enough to provide stringent punishment for the offence of cyber stalking.