CYBER STALKING: A CRITICAL STUDY

Ms. Heena Keswani*

Abstract

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 the mind of such other person. This emerging crime is popularly known as "cyber stalking". The author has made an attempt to deal with the issue of cyberstalking which is a newly coined phenomenon. In *first* chapter, there is discussion on cyberstalking and then, the differences between physical and cyberstalking are mentioned. In *second* chapter, the author shall focus on the legislative provisions as are mentioned in the Information Technology Act, 2000; and Indian Penal Code, 1860. There shall be an explanation as to how these provisions are related to cyberstalking and the shortcoming in these provisions is highlighted. In *third* chapter, the author shall focus on connecting link between cyberstalking and Constitution of India. The enforcement and jurisdictional issues associated with cyberstalking will also be dealt under this chapter. In *fourth* chapter, the author will give the concluding remarks followed by some suggestions and preventive action that one could take as "Prevention is better than cure".

Keywords: cyber space, harassment, anonymity, identity theft, emotional distress.

Introduction

"Cyber stalking" is defined as a crime where the stalkers use internet or any other electronic device to stalk someone. Online harassment and online abuse are synonymously used for cyber stalking. It involves a conduct of harassing or threatening repeatedly to an individual. Stalking can be done in the following ways such as: to follow a person till his home or where he does his business, to cause destruction to a person's property, leaving written messages or objects, or making harassing phone calls. The Cyber stalkers always think that they're anonymous and can hide. In other words, the cyber stalker's biggest strength is that they

* Student, BBALLB, Final Year, University of Petroleum & Energy Studies, Dehradun.

can rely upon the anonymity which internet provides to them that allows them to keep a check on the activities of their victim without their identity being detected. Thus, there is a need of efficient cyber tools to investigate cyber-crimes and to be prepared to defend against them and to bring victims to justice.

There are various psychological reasons behind stalking like severe narcissism, hatred, rage, retribution, envy, obsession, psychiatric dysfunction, power and control, sadomasochistic fantasies, sexual deviance, internet addiction or religious fanaticism. Some of them are discussed below:

- Jealousy: Jealousy can be a strong motive behind stalking especially when it is towards ex-partners and their current partners.
- Obsession and attraction: Another motive behind stalking could be obsession and attraction. The stalker could be attracted to victim sexually or mentally. There's a fine line between admiration and stalking.
- Erotomania: It is a kind of belief in which the stalker assumes that the victim, usually a stranger or famous person, is in love with him. It always involves sexual inclination towards someone.
- Sexual harassment: It is said to be the main motive behind cyber stalking. This is so because the internet reflects the real life.
- Revenge and hate: Sometimes the victim is not reason for the feeling of hatred and revenge in the mind of the stalker yet he/he becomes the target of the stalker. Internet appears to be the most convenient platform for the stalker to express his feeling of hatred and revenge.[1]

Based on the above mentioned motivations behind stalking, a stalker could be an obsessed one or enraged or psychopathic or deranged. More specifically, there are three categories of stalkers: Obsessional stalkers are those stalkers whose motivation are their obsession for sexual harassment and sometimes love; the delusional stalkers are those stalkers who feel the need to prove their power and the vengeful stalkers are those stalkers who want to take revenge.[2]

---

[1] *Id.* at 1.

[2] Leroy McFarlane & Paul Bocij, *Cyberstalking: The Technology of Hate*, 76 POLICE JOURNAL 204 (2003).

- Cyber space:Before studying the topic in detail, there is a brief description of the basic terminology which will be used frequently i.e., cyberspace.The term "cyber space" means the environment where the communication takes place using internet. In other words, it is a world created by internet. Cyber space can be defined as follows: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3] Another definition is "the virtual space in which the electronic data of worldwide PCs circulate."[4]This is a vague description of cyber space.

  The main characteristic of cyberspace is that it is composed of various computer networks, switches, routers, servers, etc. It is a cluster of various infrastructures such as transportation, banking, finance, telecommunication, energy and public health.

- Physical Stalking v. Cyber Stalking:
  In order to discuss the difference between cyberstalking and physical stalking, there is a need to understand what does physical stalking mean. Physical stalking meansand includes acts which are intended towards harassing the victim.[5]The difference between these two is as follows:

Basis of Distinction	Physical Stalking	Cyber Stalking
Geographical proximity	The stalker and the victim are geographically close to each other. It is not easy for the stalker to instigate third party to harass or threaten the victim. Physicalconfrontation is necessary.	As compared to physical stalking, there is a chance that the victim and the stalker may not be in the same geographical boundaries. It is comparatively an easy task for the stalker to instigate the third party to harass or

[3] Defined by U.S. Dept. of Defense.
[4] Defined by European Commision.
[5] SubhajitBasu, *Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis*, 3(2) EUR. J. L. & TECH. 1 (2012).

		threaten the victim. Physical confrontation is not necessary to achieve the intended purpose.
Predictability	It is fairly predictable as the stalker follows the victim to his/her house, workplace, etc. It becomes easy for the investigators to track down the offender.	It is not easily predictable as the stalker uses cyber platform and there is no physical confrontation. The stalker hides his/her identity making it difficult for the investigators to trace down the offender.
Familiarity with the victim	It occurs in interpersonal relationships. Generally the victim is known to the stalker such as the victim may be a celebrity, or a relative or those residing nearby to stalker.	In this case, the stalker chooses the victim randomly. E.g., where the stalker follows victim on social networking sites, the knowledge is restricted to the information available on the site.
Anonymity	It becomes difficult for the stalker to hide his/her identity in case of physical stalking.	The cyber stalkers, comparatively, enjoys high level of anonymity. Anyone with immense knowledge of technology can hide his/her identity in virtual world.
Nature	There is personal interaction between the stalker and the victim. Thus, it prevents shy people	The stalker does not need to confront his victim as the internet provides anonymity to him/her. In cyber

	from committing any criminal acts because they may not feel comfortable to talk to people over the phone or cause a sense of threat in their minds by using words in a letter.	stalking, it is easy for the stalker to choose how to behave.
Risk	The stalker can monitor the activities of his/her victim in the real world as well but it involves a high degree of risk that could make the stalker vulnerable to criminal action.	The internet provides an opportunity for the stalkers to keep a check on the activities of his/her victims such that the stalker may get into a discussion with the victim on some discussion forum or chat rooms, or access his/her personal information by tracking their virtual movement or even get direct access to details stored in the victim's computer.[6] The risk is comparatively less as the identity of the stalker is hidden.
Intimacy	It becomes easy for the victim to understand the intentions of the stalker in case of physical stalking as there is no false sense of intimacy.	Internet provides a feature of ensuring a false sense of closeness between the stalker and the victim. This results in a misunderstanding of the stalker's intention.[7]

[6] J. Joseph, *Cyberstalking: An International Perspective* 105 Y. JEWKES ED. (2002).

[7] KYA McKenna, AS Green and MEJ Gleason, *Relationship formation on the Internet: What"s the big attraction?*, 58 (1) J.OF SOCIAL ISSUES 9 (2002).

Based on the above mentioned differences, a number of criminologists have advised that a solution to cyber stalking is not to take recourse to regulations to identify the guilt and eventually pronounce punishment for physical stalking but a new system must be created for protection against cyber-stalkers. This new regime should encompass the two basic feature of crime i.e, *actus reus* and *mens rea*. This new system must deal in addressing the issues of identification of crime, gathering evidence and the issues regarding jurisdiction.[8]

Legislative framework and its shortcomings

In this section, the author shall focus on the legislative provisions as are mentioned in the Indian laws more specifically with respect to Information Technology Act, 2000 and Indian Penal Code, 1860. There shall be explanation as to how these provisions are related to cyberstalking and under what all sections can the perpetrator be booked. In India, the laws are gender biased as the law-makers considered women as the weaker section of the society hence; every statute revolves around protecting women. There are no direct provisions that deal with the issue of cyber stalking. However, the author has tried to explain few sections of Information Technology Act and Indian Penal Code that have some link with this offence and the explanation has been given regarding the relation between the provisions and the crime.

Let's discuss the Indian laws with respect to cyberstalking in detail:

Firstly, Section 354D of IPC defines "stalking". It reads as follows:

"(1) Any man who—

i. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; ormonitors the use by a woman of the internet, email or any other form of electronic communication commits the offence of stalking;.."[9]

The section was added by Criminal Amendment Act 2013 post *Delhi gang-rape* case. This section takes into account both, the physical stalking and cyberstalking. The section defines its scope in terms of activities that forms the offence of "stalking." The

[8] KW Seto, *How Should Legislation Deal With Children as the Victims and Perpetrators of Cyberstalking?*, 9 CARDOZO WOMEN"S L. J. 67, 73-74 (2002).

[9] Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.

Section clearly mentions that if anyone tries to monitor the activities of a woman on internet, it will amount to stalking. Thus, if the stalker indulges in any of the activities defined in the section, he shall be guilty of the offence under Section 354D of Indian Penal Code.

This section has many loopholes such as firstly; the section only considers "women" to be the victim and ignores the fact that even men can be the victim. The Section states that whoever tries to monitor the usage by a woman of internet, e-mail or any other mode of electronic communication shall be liable for committing the offence of cyber stalking. We can see that it focuses only on women. Thus, it is gender biased legislation. Secondly, the legislators have not mentioned the "method of monitoring." It might happen that the person might lack the intention but his actions amount to stalking.

Secondly, Section 292 of IPC defines "obscenity". The offence of cyberstalking takes within its purview the act of sending obscene materials to the victim on a social networking site or through e-mails or messages etc. Where the stalker attempts to deprave the other person by sending any obscene material on internet with the intention that the other person would read, see or hear the content of such material then he shall be guilty of the offense under Section 292 of Indian Penal Code.

Thirdly, Section 507 of IPC relates to "criminal intimidation by anonymous communication." This section states that where the stalker tries to hide his identity so that the victim remains unaware of the source from where the threat comes, it amounts to an offence. Thus, it ensures the very characteristic of cyberstalking i.e., anonymous identity. The stalker shall be guilty under this section if he attempts to conceal his/her identity.

Fourthly, Section 509 of IPC relates to modesty of women reads as follows:

> "Word, gesture or act intended to insult the modesty of a woman.—Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished..."[10]

[10] Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.

A stalker can be booked under this section if the conduct of the stalker hinders the privacy of such woman by making any gesture or through words sent by e-mails, messages or posted on social media. If he does any such activities, he shall be guilty of offence under Section 509 of Indian Penal Code.

Section 509 suffers from many shortcomings. Some of them are: it is a gender biased provision as it focuses only on modesty of a woman and therefore, ignores the fact that this crime of cyberstalking is gender neutral in nature and even males can also be the victim in such crimes. This section requires that the words, sound or gesture should be spoken, heard and seen respectively. Thus, cyber-stalkers can easily escape the penalty under this section as word cannot be spoken, gesture cannot be seen and sound cannot be heard on internet.[11]Lastly, the intention of insulting the modesty of the woman cannot be assumed from communications on internet.

Fifthly, Section 67 of Information Technology Act, 2000 is replica of Section 292 of Indian Penal Code. This section relates to publishing obscene material in "electronic form". Thus, this section covers the online stalking. If the stalker tries to publish any obscene material about the victim on social media i.e., in electronic form so as to bully the victim, he shall be guilty of offence under Section 67 of IT Act.

Sixthly, Section 67A of Information Technology Act, 2000 relates to a part of cyberstalking crime. This section was added after the amendment in 2008. It states that if stalker attempts to publish any "sexually explicit" material in electronic form i.e., through e-mails, messages or on social media then he shall be guilty of an offence under Section 67A of IT Act and shall be punished accordingly.

Seventhly, Section 67B of Information Technology Act, 2000 is a newly inserted section. This section is newly inserted by Amendment Act 2008. The section focuses on when stalker targets children below the age of 18 years and publishes material in which children are engaged in sexual activities in order to terrorize the children.

Eighthly, Section 66E of Information Technology Act, 2000 and Section 354C of Indian Penal Code deals with "voyeurism." Section 66E reads as follows:

---

[11] P. Duggal, *India's first Cyberstalking Case- Some Cyberlaw Perspectives*, http://cyberlaws.net/cyberindia/2CYBER27.htm (May 13, 2017, 8:55PM).

> "Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished."[12]

Ninthly, Section 354C reads as follows:

> "Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished..."[13]

The stalker might hack the account of the victim and post private pictures of the victim on social networking sites in order to cause depression and a sense of threat in the mind of the victim. Both the above mentioned sections aims at publishing or capturing pictures of private act of a person without the consent of such person shall be guilty of an offence under these sections. However, Section 66E is more generic as it addresses the victim as "any person" whereas Section 345C is kind of gender biased. As per section 354C, the victim should be a "woman".

"What is noteworthy here is that despite the fact that all offline laws apply to digital media, the punishments under the IT Act are much stronger."[14] "Indeed, it is worth noting the emphasis placed even by the IT Act on women's bodiesor sexualities: within the Act, while Section 66A deals with a generic category of 'offensive messages'."[15]

Section 354C of Indian Penal Code takes within its purview the act of voyeurism. It is comparatively narrow in scope because to attract this section, the victim should a "woman". On the other hand, Section 66E of Information Technology Act also covers voyeurism but the scope is broader as compared to Section 354C of Indian Penal Code. Section 66E addresses the victim as "any person". Thus, the victim need not be only "woman" in order to fetch justice under this section. Where the victim is a man, he may take recourse to Section 66E of Information Technology Act, 2000.

---

12 Information Technology Act, 2000, No. 21, Act of Parliament, 2000.
13 Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.
14 RichaKaulPadte, *Keeping woman safe?Gender, Online Harassment and Indian Law, (2013).*
15 *Id*. at 15.

The Information Technology Act, 2000 and the Indian Penal Code, 1860 does not explicitly provide provisions for dealing with the issue of Cyber Stalking and the defamatory or threatening messages sent by the stalker during stalking the victim through messages, phone calls, e-mails or by publishing blogs under the name of the victim. It is possible to punish the offender under some of the provisions of the above mentioned Acts as mentioned in above chapters but there is no express provision that solely deals with this crime. The commission of this crime is very easy whereas its effects are very long-lasting. It can badly affect the victim's mental and physical health. The penalty provided under existing provisions must be increased keeping in mind the well-being of the victim.[16]

Constitutional framework and enforcement problem

The main issue of territorial jurisdiction has not been effectively addressed in Information Technology Act, 2000 or Information Technology Amendment Act, 2008. The various sections in which the matter of jurisdiction has been mentioned are Sections 46, 48, 57 and 61 where adjudication process and the appellate procedure is mentioned. Another section is section 80 that explains the power of the police officers to enter and conduct search of a public place in relation of a cyber-crime etc. The cyber-crimes are the crimes that are committed with the help of computers and if someone hacks the mail account of a person sitting in another state or country, it will be difficult to determine P.S. of which shall take the cognizance of the offence. Many Police officers try to avoid admitting complaints of the victim in such cases due to the problem of Jurisdiction. Since the cybercrimes are not bound by the geographical limits, there is a need to clear the issue of jurisdiction as what all are the relevant considerations to be seen in such situations. Proper elaborations to be made as to which State shall have the authority to deal with the cases of cybercrime.

The solution to the problem can be the extradition arrangement between the two respective countries. An extradition arrangement is an arrangement where the criminal is deported to the country where he has committed the crime in case where such arrangement exists between the two concerned countries. Thus, in case of cyber stalking also, if there is an arrangement between the country to which the victim belongs and the country to which the

[16] Vijay Mukhi and Karan Gokani, *Observations on the Proposed Amendments to the IT Act 2000,* AIAI.

stalker belongs then there will be no such problem of enforcement.

The main problem arises when laws of one country are in conflict with laws of another country. A situation may arise where the conduct of stalker may be penalized in one country but may not be regarded as a crime in another country. This is known as Jurisdictional Issue. In such cases, the problem of enforcement also arises. In such a situation, there is a need of cooperation between both the countries. This is where extradition policies come into picture.

In India, the Information Technology Act confers the "extraterritorial jurisdiction" by virtue of Section 75. This section makes it clear that whether an offence is committed outside or in India, the offender shall be governed by the provisions of Information Technology Act irrespective of the fact whether he is a citizen of India or not. Provided such an offence relates to the computer systems, or network that is situated in India. Thus, the solution provided by Indian laws to the problem of enforcement is limited.

One of the features of cyber stalking is anonymous identity of the stalker. There has been a suggestion to put restrictions on keeping the identity anonymous. This, however, appeared to be a debatable topic as almost the laws of every country ensures Freedom of Speech and putting restrictions on anonymous identity would be violative of this freedom. In the cases of *In Re RamlilaMaidan Incident* v. *Home Secretary*[17] and*Sahara India Real Estate Corp. Ltd.* v. *Securities & Exchange Board of India*[18]the court held that the freedom of speech and expression as provided under Article 19(1)(a) is not an absolute right.

Article 14 of the Constitution of India provides for 'equality before law'. We can see that our Constitution provides Equality but when we read the legislative provisions, we can see that there is too much gender inequality. The provisions are more inclined towards protection of women considering them to be the weaker section of the society. However, such gender inequality doesn't hold good when it comes to present scenario.

Section 354D of Indian Penal Code is at present that only provision that has some proximate relation to the crime of cyber stalking. It is evident from the provision that it solely protects

---

17 SuoMotu Writ Petition (Crl.) No. 122 of 2011, decided on Feb. 23, 2012.
18 Media Guidelines Case, C.A. No. 9813 of 2011, decided on Sept. 11, 2012.

women. The legislators have considered that the females are the "victim" every time.

> "(1) Any man who—
>
> i. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
> ii. monitors the use by a woman of the internet, email or any other form of electronic communication commits the offence of stalking."[19]

From the reading the section it appears that the legislators have assumed "man" to be always the offender/stalker and "woman" to be the victim in every case. This violates Art. 14 of the Indian Constitution. However, it is true that this Section was added recently through Criminal Amendment Act 2013 after the very famous Delhi gang rape case took place. So, the legislators might have, at the time of framing this section, kept this case in their mind. But this provision needs amendment. The terms "man" and "woman" should not be explicitly used. The section should be reframed using the term "anyone" or "any person" to make it non-violative of Article 14.

Section 509 of Indian Penal Code addresses the issue to offending the modesty of a woman. This section should also be reframed by the term "any person" instead of "woman". A female stalker can also offend the modesty of a man through sending obscene materials on internet or e-mails or messages, the stalker. Thus the legislators should make an attempt to protect man and woman and not just the woman both from the ill-effects of cyber stalking.

Section 354C of Indian Penal Code deals with voyeurism which also a part of cyber stalking as the offender/stalker might indulge in hacking the computer of the victim so as to have a look on to the private pictures of the victim without his/her consent. This section is also gender biased. It reads as:

> "Any man who watches, or captures the image of a woman ..."[20]

In this section too, the legislators have assumed that only man will indulge in voyeurism the woman being the victim. There can be a situation where the woman hacks the computer system of a

---

19 Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.
20 Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.

man so as to capture the image of man in such a situation what is the resort for a man? There is no such provision like this section that solely protects a man. Hence, this section should be reframed in order to be neutral ensuring protection to both a man and a woman.

Article 21 of Indian Constitution "No person shall be deprived of his life or personal liberty except according to procedure established by law."[21]This section condemns any person from depriving another such person the right to personal liberty. The stalker aims at entering into the private space of the victim thereby ruining his/her right to privacy and right to personal liberty. Following the victim on social networking sites, e-mails, messages or through telephone calls or through any other mode the stalker always tries to monitor each and every move of the victim. This causes distress and a sense of threat in the mind of the victim. The victim cannot enjoy his personal space. Thus, the offender/stalker must be charged under Article 21 as well because his actions are violative of this article. Every citizen has the right to life and personal liberty and no one can deprive him of his right "except according to procedure established by law".

Conclusion and suggestions

It is very correctly said that if you want to bring change in the current scenario, you need to overcome the obsolete model of dealing with the situation and build a new model that is effective and efficient. Cyberstalking is a newly coined term. It has gain attention of the legislature and judiciary recently. There have been many instances where the need for effective legislation was felt as it becomes very difficult for the enforcement agencies to deal with such cases. Cyberstalking is proved to be a grave offence. It has very far-reaching impact on the mental and physical health of the victim. Through this article, the author has made an attempt to discuss the term "cyberstalking" in detail along with its nature and scope.

Some people argue that it is an extended version of cyber stalking or a new form of stalking but it appears to be more than that. It is a new form of crime itself. We have seen that the intention of the stalker is to harass and threaten his/her victim. Thus, it involves criminal activity. Many countries have legislations on this subject. None of the existing provisions are capable of dealing with the cases efficiently. India does not have any direct legislation on the subject. Information Technology Act and Indian Penal Code have

[21] INDIA CONST. Art. 21.

few provisions that could be related to this cybercrime and hence the stalker can be booked under those provisions. These are the lacuna in the legislative approach followed by the countries to address this crime. There are hardly any reported cases because the police authorities do not take up the case because of the enforcement issues as the stalker and the victim may belong to different countries thus, it becomes difficult to decide as to law of which country is to be followed. We should not solely depend upon the legislative provisions but should proactively make an attempt to do not give rise to such situations. As is correctly said, "Prevention is better than cure". We should take some precautions for our safety and if after then such situation arises, we should take recourse to legislative provisions. Our step should be taking precaution on our end.

Some suggested reforms are as follows:

1. Amendment to Information Technology Act
   Information Technology Amendment Act, 2008 added a new section i.e., Section 66A. This section addressed the issue of cyber stalking but was eventually struck down by the Supreme Court of India in the case *Shreya Singhal v. Union of India*. The reason behind putting down this section was the vagueness in the wording of the section. Thus, there is a need for a new amendment to this Act. A new section should be added that would solely deal with cyberstalking.

   This new section should be worded in such a manner so as to include the following:
   a) It is a punishable offence to harass torture, embarrass, intimidate or annoy any person through communications on internet by using any computer resource or any other electronic device.
   b) It is a punishable offence to use any obscene or indecent words, or taking any obscene images of such other person or instigating anyone to commit any such indecent act.
   c) It is a punishable offence to repeatedly communicating with such other person by concealing the identity.
   d) There should be rigorous imprisonment for the offender of the crimes mentioned above.
   e) There should be explanation regarding use of computer resource and any other electronic device to include communication using all electronic modes such as radio, optical cable, etc.

The author believes that if such a section is incorporated in the Information Technology Act, 2000 it would be an effective provision to deal with the issue of cyberstalking. It would control the actions of the stalker as it imposes rigorous punishment if found guilty. It makes it an offence to keep anonymous identity and covers almost every mode of electronic communication or computer resource using which the stalker tries to communicate with the victim.

2. Self-Regulation

Self-Regulation is the best method to control such crime but is often the least followed method. Following are the few instructions:

a) Everyone should choose a username that is gender neutral or the e-mail ids should be a combination of characters and phrases that are meaningless. The passwords should contain some digits or letters.[22]
b) There should be minimum personal information available on social networking sites.
c) While communicating with strangers, the personal information should not be shared easily.
d) Children are the most vulnerable class. The must be educated about what should or should not be done over internet.[23]
e) Protection agencies such as WHOA and Cyber Angels[24] that provides education to the public regarding self-protection. They also guide in drafting policies of online communities.
f) Government has also made an attempt to educate people on how to use internet and what precautions need to be taken while surfing on Internet. An example of Government initiative is the collaboration between the U.S. Department of Justice in collaboration and the Information Technology Association of America declared their Cybercitizen Partnership in 1999. This collaboration was intended to spread awareness about crimes related to computers.

---

[22] Working to Halt Online Abuse, http://www.haltabuse.org/resources/online.shtml (May 13, 2017, 7:15AM).
[23] Cyberangels, http://www.cyberangels.org/parents/childIDtheft.php (May 13, 2017, 09:50AM).
[24] *Id.* at 23.

3. Use of software programs
   Another method of restricting the scope of computer related crime is to make use of certain software programs that will ensure control with respect to the contents received. Such programs also helps in blocking the emails received from anonymous senders or from unauthorized senders. For example, Facebook also has a policy wherein we can choose to receive messages from unknown people or we can simply keep this option off. There is certain software such as *Netnanny*which helps parents to restrict certain websites from access.

4. Role of Internet Service Providers
   In order to restrict the harassing behaviour of the stalker, few steps have been taken by Internet Service Provider. Few providers provide the opportunity to report abuses for example, Facebook as discussed above, Facebook has certain privacy policies whereby we can restrict strangers from sending messages containing obscene content and abusive behaviour.[25] Internet Service Providers take control measures by sending unwanted emails to spam folder.

   There is a requirement of cooperation between Internet Service Providers and the enforcement agencies when it comes to tracking down the stalker.

With time only we can judge how effective these measures can be if the crime of cyberstalking increases at a fast pace. However, the need for legislative provisions cannot be ignored in the light of taking precautions. There is a requirement of effective legislative provisions to deal with such cybercrimes.

References

Articles referred

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).

[25] https://newsroom.fb.com(May. 13, 2017, 11:42PM).

V. D. Halder and K. Jaishankar, *Cyber Crimes against Women in India: Problems, Perspectives and Solutions*, 3(1) TMC ACAD. J. 48, 55 (2008).

VI. D. Lamplugh& P. Infield, *Harmonising Anti-Stalking Laws,* 34 Geo. Wash. Int'l L. Rev. 853 2002-2003.

VII. David C. Potter, *The Jake Baker Case: True Threats and New Technology,* 79 B.U. L. Rev. 779 1999.

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

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

X. Dr. DebartiHalder, *Creating Awareness of Online Victimization using Social Media: A Therapeutic Jurisprudential Approach,* June 9, 2015.

XI. Dr. DebratiHalder, *Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and Therapeutic Jurisprudential Perspectives,* SSRN 103, 103-130 (2015).

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

XIII. Eric A. Fischer, *Cybersecurity Issues and Challenges: In Brief,* CRS, (2016).

XIV. F. Mishnaet. Al, *Real-World Dangers in an Online Reality: A Qualitative Study Examining Online Relationships and Cyber Abuse,* 33 SOCIAL WORK RESEARCH 107, 107-118 (2009).

XV. J. Joseph, *Cyberstalking: An International Perspective* 105 Y. JEWKES ED. (2002).

XVI. John M. Deirmenjian, *Stalking in CyberSpace*, (1998).

XVII. John Marshal, *Cyber-Space, or Cyber-Topos: The Creation of Online Space,* 45 IJSCP 81, 81-102 (2001).

XVIII. Justice Surya Rao, *Cyber Laws- Challenges for the 21st Century,* (2004).

XIX. Jaishankar and V. Uma Sankary, *Cyber Stalking: A Global Menace in the Information Super Highway*, 2 ERCES (2005).

XX. K. W. Seto, *How Should Legislation Deal With Children as the Victims and Perpetrators of Cyberstalking?*, 9 CARDOZO WOMEN'S L. J. 67, 73-74 (2002).

XXI. K. Y. A. McKenna, A. S. Green and M. E. J. Gleason, *Relationship formation on the Internet: What"s the big attraction?*, 58 (1) J.OF SOCIAL ISSUES 9 (2002).

XXII. L. Ellison & Y. Akdeniz, *Cyber-stalking: the Regulation of Harassment on the Internet,* CLR 29, 29-48 (1998).

XXIII. Leroy McFarlane & Paul Bocij, *Online Harassment: Towards a Definition of Cyber Stalking*, 139 PRISON SERVICE .I 31, 31-38 (2002).

XXIV. Leroy McFarlane& Paul Bocij, *Cyberstalking: The Technology of Hate*, 76 POLICE JOURNAL 204 (2003).

XXV. Noora Al Mutawaet. Al, *Forensic Investigation of cyberstalking cases using Behavioral Evidence Analysis,* 96 ELSEVIER, 96-103 (2016).

XXVI. OlgutaDogaru, *Challenges in Cyber Space- Threats to Public Order and Safety,* Pub. Sec. Stud. 91 2015.

XXVII. P. Bocij, *Corporate Cyberstalking: An Invitation to Build Theory*, 7 PEER-REVIEWED J. (2002).

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

XXIX. Pittaro, M.L, *Cyber Stalking: An Analysis of Online Harassment and Intimidation*, 1(2) IJCC 180, 181 (2007).

XXX. Portland State University, Criminology and Criminal Justice Senior Capstone, *Prevention of Cyberstalking: A Review of the Literature,* (2012).

XXXI. R. Ottis& P. Lorents, *CyberSpace: Definition & Implications,* Cooperative Cyber Defence Centre of Excellence.

XXXII. RichaKaulPadte, *Keeping woman safe? Gender, Online Harassment and Indian Law,* (2013).

XXXIII. RidhiKabra, *Cyberstalking: one problem control-alt-delete can't solve, (*2013).

XXXIV. Robert KurmanKelner, *United States v. Jake Baker: Revisiting Threats And The First Amendment,* Virginia Law Review, Vol. 84, No. 2 (Mar., 1998), pp. 287-313.

XXXV. Samarth Agrawal, *Cyber Forensics & Electronic Evidences: Challenges in Enforcement & Their Admissibility,* Jan 12, 2012.

XXXVI. *Sticks and Stones May Break My Bones, But Your Words Are Sure To Kill Me,* 50 DePaul L. Rev. 993 2000-2001.

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

XXXVIII. SW Brenner, *Fantasy Crime: The Role of Criminal Law in Virtual Worlds*, 11(1) VANDERBILT J. ENT. & TECH. L. 1, 53 (2008).

XXXIX. The Harvard Law Review Association, *First Amendment — True Threats — Sixth Circuit Holds that Subjective Intent Is Not Required by the First Amendment When Prosecuting Criminal threats*, 126 HLR 1138, 1138-1145 (2013).

XL. VenkatBalsubramani, *Conviction for Cyberstalking & Revenge Porn Survives First Amendment Challenge,* (May 8, 2014).

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