Cyber stalking: New Age Terror

Diksha Bhasin
Bharati Vidyapeeth Deemed to be University, New Law College,
Pune, India

Aryan Mehta
Bharati Vidyapeeth Deemed to be University, New Law College,
Pune, India

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 authors have made an attempt to deal with the issue of cyber stalking which is a newly coined phenomenon. In first chapter, there is discussion on cyber stalking and then, the types of cyber stalking are mentioned. It is followed by differences between physical and cyber stalking. The authors have focused on the legislative provisions as are mentioned in the Information Technology Act, 2000; and Indian Penal Code, 1860. Lastly, the authors will give a few prevention measures to be followed on everyday basis against cyber stalking and the concluding remarks.

I. WHAT IS CYBERSTALKING?

"With a click of the 'Post Comment' button, Netizens can quickly bring down the level of dialogue. Bloggers lob zingers, commenters trade barbs, and bullies target kids in the cyber schoolyard. Mudslinging - a time-honoured political tradition - thrives on the Web."[1]

-Willow Bay

Cyberstalking is a criminal practice that involves using the Internet, cell phone, and/or any other electronic communication device to stalk another person. The perpetrators are involved in the destruction of data or equipment, solicitation of minors for sexual purposes, threats, or any other form of repeated offensive behaviour. The offenders use social media platforms, email, chat rooms, instant messaging, or any other online media to harass the victim.

The British Crime Survey defines stalking as "two or more incidents causing distress, fear, or alarm, of obscene or threatening unwanted letters or phone calls, waiting or loitering around home or workplace, or following or watching, or interfering with, or damaging personal property carried out by any person".[2]Bocij, Griffiths and McFarlane think of cyber stalking as "a group of behaviour in which an individual, group of individuals or organization, uses information and communications technology to harass one or more individuals. Such behaviour may include, but are not limited to, the transmission of threats and false accusations, identity theft,

[1] Available on (https://www.brainyquote.com/quotes/willow_bay_531432)
[2] Available on (https://blog.ipleaders.in/cyber-stalking/)

data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes and confrontation".[3]

Cyberstalking is a type of online harassment or computer oriented harassment. The term is interchangeably used as online harassment or online abuse. Forbes defines online harassment or cyber harassment as repeated online expression amounting to a "course of conduct" targeted at a particular person that causes the targeted individual substantial emotional distress and/or the fear of bodily harm[4].

Thus, online harassment takes the form of cyberstalking when repeated unwanted communications, whether direct or indirect, takes place over a period of time, through one or more mediums of Internet or electronic communications.

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.

II. TYPES OF CYBERSTALKING

There are three usual types of cyber stalking: online abuse, trolling and sexting.

1) Online abuse – Online abuse incorporates actions that use information and communication technologies to support intentional, repeated, and hostile behaviour by an individual or group that is intended to harm another person. Victims are frequently known personally by the perpetrator.
2) Trolling - Trolling is deliberately sowing hatred, bigotry, racism, misogyny, or just simple bickering between others. Trolls are users who thrive in any environment where they are allowed to make public comments, like blog sites, news sites, discussion forums, and game chat starting arguments or making people unhappy, by posting inflammatory, extraneous, or off-topic messages in an online community.
3) Sexting – Sexting involves the use of a mobile phone or other similar electronic device to distribute sexually explicit images or videos.

Cyber stalking takes many forms such as:

- Making and posting fake or real sexual images of the victim or their loved ones
- Tracking the victims' every movement by placing a GPS device on their car
- Threatening the victim or their friends and family via emails

[3] Available on (http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html)
[4] Available on (https://blog.ipleaders.in/cyber-stalking/)

- Uploading personal information such as name, address or phone number on the Internet
- Hacking and saving emails, text messages and social media posts and using them to harass or blackmail a victim
- Hacking into the victim's social media account to post offensive material and comments
- Releasing personal or fake information to discredit a victim at his/her office
- Using the victim's social media account or email to stalk and contact others
- Creating malicious websites, fake social media profiles and blogs about a victim

III. PHYSICAL STALKING VS CYBERSTALKING

People often tend to get confused between the two terms, Physical Stalking and Cyber stalking. Physical Stalking includes the acts which are intended towards harassing the victim. The main difference between the two terms being as under:

Firstly, the two terms can be distinguished on the basis of geographical proximity between the stalker and the victim. While, the stalker & the victim are geographically close to each other in physical stalking, there is a chance in cyber stalking that the victim and stalker may not be in same geographical boundaries.

Secondly, the relationship between the stalker and the victim differentiates the two. Physical stalking occurs in interpersonal relationships. The victim is known to the stalker. Cyber stalking does not require an interpersonal relationship between the stalker and the victim. The stalker may choose a victim randomly.

Thirdly, it becomes difficult for the stalker to hide his identity in Physical stalking, making it easy for the investigators to track him. His pattern is predictable, as he follows the victim usually to the place of work, home, etc. The cyber stalkers, comparatively, enjoys high level of anonymity. Anyone with immense knowledge of technology can hide his/her identity in virtual world. 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.

The low level of anonymity in case of physical stalking makes it easier for the stalker to monitor the activities of his/her victim in the real world, making him vulnerable to criminal action. The risk of criminal action is comparatively less in cyber stalking as the identity of the stalker is hidden and not easily traceable.

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.[5]

IV. CYBERSTALKING: STATISTICS

A survey by a global security firm Norton among 1,035 adults last year found that online harassment is on the rise in India. Some of its key findings were that 8 out of 10 people had encountered some form of online harassment, cyber bullying and cyber stalking.

A study also revealed that social media platforms like Facebook, Twitter and even Instagram are potential hunting grounds for cyber-stalkers. Victims usually pick up or run into an offender at such platforms. This could be because 39% of children fail to enable their privacy settings on social media. However, 95% of teens that witnessed bullying on social media report that others, like them, have ignored the behaviour. Moreover, 25% of teens on social media reported that online incidents have resulted in face-to-face confrontation. So, one must be careful about what they post and who they interact with on social media sites.

The study also proved the basic notion of the mass, that women are more often victims of cyber-stalking compared to men. According to the research report by WHOA (Working to Halt Online Abuse) in 2013, the ratio stood at 60% women to 40% men. In 2013, most reported victims of cyber-stalking lived in California and most cases were reported in the US.[6]

V. LEGISLATIVE FRAMEWORK OF CYBERSTALKING IN INDIA

In 2001, India's first cyberstalking case was reported. Ms. Ritu Kohli was working with an embassy in New Delhi when her perfectly normal life turned upside down. She started receiving a series of emails from an unknown source.

The person, through the mails, threatened her to either pose nude for him or cough up Rs.1 Lakh. Initially, she ignored the mails. But when she started receiving similar threatening letters through post, she got alarmed.

In the mails and letters, the accused, Manish Kathuria, threatened Kohli that he would put up her morphed pictures on adult sites along with her telephone and home address. He also alleged to put up the same pictures in her neighbourhood. She also received numerous unsolicited phone calls from strangers at odd hours, asking her for sexual favours. Distraught, Kohli lodged a police complaint.

The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 had no mention of acts done to outrage the modesty of a woman online. This acted

[5]KW Seto, How Should Legislation Deal With Children as the Victims and Perpetrators of Cyber stalking?, 9 CARDOZO WOMEN˝S L. J. 67, 73-74 (2002)
[6] Available on (https://www.globalsign.com/en-in/blog/what-is-cyberstalking-and-how-to-prevent-it/)

as an alarm for the Indian Government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same.

As a result to this, The Information Technology Act, 2000 was amended in the year 2008 and it contained Section 66A which stated:

Punishment for sending offensive messages through communication service, etc.:

"Any person who sends, by means of a computer resource or a communication device,-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,shall be punishable with imprisonment for a term which may extend to three years and with fine."[7]

The Section was later struck down in a landmark judgment upholding freedom of expression. According to the apex court, the said section lays outside the ambit of Article 19(2) of the Indian Constitution, which relates to freedom of speech. It took a series of petitions, but the case in the question which lead to this radical judgment, was Shreya Singhal v. Union of India[8].

Section 67A of the Act which is another provision dealing with cyber stalking and as a replica of Section 292 of Indian Penal Code states that:

Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:

"Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees."[9]

As this section relates to publishing obscene material in electronic form, it can be related to online stalking. In cases where the stalker publishes any obscene material about the victim in electronic form, he shall be guilty of offence under Section 67A of the IT Act.

[7]The Information Technology (Amendment) Act, 2008, No.10, Act of Parliament, 2009
[8] AIR 2015 SC 1523
[9]The Information Technology (Amendment) Act, 2008, No.10, Act of Parliament, 2009

Section 66E of the Act deals with voyeurism and reads as follows:

"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 with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both."[10]

Section 67B of the IT Act deals with the publishing of obscene material targeting children below 18 years of age, and states that:

Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: "Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees"[11]

Apart from the Information Technology Act, 2008, The Indian Penal Code, 1860 also lays down some provisions relating to the offence of Cyber stalking. Section 354D of IPC defines stalking. It reads as follows:

"(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,commits the offence of stalking.*

[10]The Information Technology (Amendment) Act, 2008, No.10, Act of Parliament, 2009

[11]The Information Technology (Amendment) Act, 2008, No.10, Act of Parliament, 2009

(2) 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."[12]

Section 354C of IPC criminalises the offence of Voyeurism. It states that:

"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 on first conviction with imprisonment of either description for a term which shall not be less than one year, but 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 shall not be less than three years, but which may extend to seven years, and shall also be liable to fine."[13]

The victim can also additionally file a complaint against the perpetrator under Section 499 of IPC which deals with defamation. The section has bailed out those acts of stalking which are performed for the purpose of preventing and detecting crime by a person who has been entrusted with such responsibility by the state. Additionally, instances where pursuing such conduct was reasonable or where the person was authorised under any act cannot insinuate the offence of stalking.

Section 503 punishes criminal intimidation as threats made to any person with injury to her reputation, either in order to cause alarm to her, or to make her change her course of action regarding anything she would otherwise do/not do. The offences under S. 499 and S. 503 are punishable with imprisonment which may extend to two years, and/or fine.

Section 509 of IPC comes to the rescue of a victim when the perpetrator is constantly bugging you with derogatory verbal abuse because of your gender. The section provides that any person who utters any word or makes any sound or gesture, intending that such word, sound or gesture be heard or seen by a woman and insult her modesty, shall be punished with one-year imprisonment and/or fine.

Section 507 punishes criminal intimidation by an anonymous communication with a term which may extend to two years of imprisonment. Vengeful posting of images or videos of rape victims is punishable with imprisonment which may extend to two years and fine under section 228a of IPC.[14]

[12] Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.
[13]Indian Penal Code, 1860, No.45, Acts of Parliament, 1860
[14]Available on (https://blog.ipleaders.in/cyber-stalking/)

The Indian Legislation lack provisions explicitly dealing with the offence of Cyber stalking. It is possible to punish the offender under the abovementioned provisions, but there is no expression provision dealing with solely this crime.It makes the commission of the crime easier, while the effects on the mental and physical well-being of the victims are major and long lasting. The penalty provided under existing provisions must be increased keeping in mind the effect on the victim.

VI. PREVENTION OF CYBERSTALKING

In the virtual universe, cyber-stalkers are hidden at every corner waiting to attack their potential prey. People may never know when they're being projected as a target until it's too late. There are many ways in which a cyber-criminal can target you. Fortunately, there are many ways to protect ourselves from this chaos. The following are some simple ways to protect yourself online:

- Don't send or receive private emails or messages when connected to a public Wi-Fi as they are highly unsafe. With modern technology, there's always a chance that someone could be keeping an eye on your internet traffic.
- In order to protect your personal data and to keep yourself anonymous online use of a VPN should be done.
- Install a safe, secured and latest version of top-notch antivirus software on your PC, laptops and other devices.
- Keep your uploads on social media in check. One should not provide excessive personal information which would help a cyber-stalker to commit crimes easily.
- One should use strong and unique passwords and also put multi-factor authentication in order to prevent easy access to your personal information.
- One should not enable the location or display the location to public excessively while uploading the pictures; it may help the cyber stalker to stalk you easily.
- Avoid phishing mails, which are a major threat online.
- Keep your privacy settings in check; one should only know that much information which is necessary.

In today's time, it's eminent to educate our kids and even adults about cyber-stalking and its remorse consequences and this can be done by raising awareness and implementing the strategies suggested above in order to protect yourself and your loved ones from these types of threats.

VII. CONCLUSION: CHOICE BETWEEN "NO SOLUTION" & "COMPROMISE"

"You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete"[15]

-- R. Buckminster Fuller

In recent years, a succession of legal articles proposing regulation of cyber stalking have either attempted to justify cyber stalking as an extension/continuation of stalking or have overemphasized the importance of formal black letter law. They have rarely looked into cyberspace with any real social insight, instead focusing on the question of how to adapt laws of the real world for application in cyberspace. Cyber stalking, however, does not always conform to the reason and logic of the real world.

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 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.

[15]Available on (https://www.goodreads.com/quotes/13119-you-never-change-things-by-fighting-the-existing-reality-to)