CYBERSTALKING AND ONLINE HARASSMENT: A NEW CHALLENGE FOR LAW ENFORCEMENT

Dr. Sapna Sukrut Deo*

Introduction

The Internet has become a medium for people to communicate globally in the course of business, education and their social lives. The Internet has made it easy for people to communicate, meet a companion, or compete with people on the other side of the world with click of a mouse.

In 2013, according to the *Internet World Stats Report*, 137,000,000 people used Internet, and 56,698,300 people used *Facebook* in India, as a result there arises a concern for Internet safety. The increased use of the Internet has created an impact on the number of online harassing/cyberstalking cases.

Cyberstalking is a new form of computer related crime, occurring in our society. Cyberstalking means when a person is followed and pursued online, invading his/her privacy as his/her every move watched. It is a form of harassment that can disrupt the life of the victim and leave him/her feeling very afraid and threatened. Cyberstalking usually occurs with women, who are stalked or harassed by men, or with children who are stalked by adult predators or pedophiles. Cyberstalkers need not have to leave their home to find, or harass their targets, and has no fear of physical violence since they believe that they cannot be physically touched in cyberspace. They use Internet, e-mail, and other electronic communication devices to stalk persons.

This paper addresses the issue of cyberstalking and online harassment, and what legal remedies an Internet user may have when confronted with this form of behavior. Firstly, the paper will examine what constitutes cyberstalking and harassment, and will discuss the way in which the Internet may facilitate such behavior.

The nature of the behavior is effects-based one upon the victim wherein the stalker is anonymous, although the harasser may not be

* Assistant Professor, New Law College, Pune.

so. Online harassment is similar to real world stalking in the way that it can be disturbing to the victim. At the same time the unique environment of the Internet creates "remoteness" on the part of the stalker, and provides a false sense of security arising from the apparent anonymity that is present on the Internet.

Secondly, this paper will review the current harassment legislation in India, and examine how this legislation has been applied by the Indian courts. In addition it will provide remedies for an Internet user confronted with this behavior.

Finally, the paper will consider "self prevention/protection" measures that individuals may adopt in dealing with online harassment and cyberstalking.

Definitions of Online Harassment and Cyberstalking

Cyberstalking involves using the Internet, cell phone, and/or any other electronic communication device to stalk another person. It may involve threats, identity theft and damage to data or equipment, solicitation of minors for sexual purposes, and any other form of repeated offensive behavior.

Online harassment can involve sexual harassment which is unwanted contact of a personal nature, or other conduct based on sex affecting the dignity of men and women at work.[1] This may include unwelcome physical, verbal or non-verbal conduct. It is unwanted if such conduct is unacceptable, unreasonable and offensive to the recipient. Sexual attention becomes sexual harassment if it is persistent and once rejected by the recipient. However, a single act, if sufficiently serious, can also constitute harassment.[2]

Online harassment can be divided into direct and indirect harassment. "Direct" harassment includes the use of pagers, cell phones and the email to send messages of hate, obscenities and threats, to intimidate a victim. E.g., the majority of offline stalkers will attempt to contact their victim, and most contact is restricted to mail and/or telephone communications. On the other hand "indirect" harassment includes the use of the Internet to display messages of hate, threats or used to spread false rumours about a victim. Messages can be posted on web pages, within chat groups or bulletin boards. This form of harassment is the electronic equivalent of

---

1 http:www.mindspring.com\~techomom\harassed\ (last visited May 1, 2013).
2 British Telecommunications PLC v. Williams, (1997) IRLR 668.

placing pinups on a factory wall, and if the display of such material from the victim's perspective causes offence it will amount to harassment.[3]

Thus generally speaking, online harassment becomes cyberstalking when repeated unwanted communications, whether direct or indirect, takes place over a period of time, via one or more mediums of Internet or electronic communications. The messages themselves must be unwanted, and the content can be-but is not limited to-threatening, sexually harassing, emotionally harassing or bullying, or general misinformation. Provided the messages create reasonable fear in the victim, they fit the definition for cyberstalking.[4]

There are a number of definitions of stalking that exist, each differing slightly. Stalking as "a course of conduct directed at a specific person that involves repeated (two or more occasions) visual or physical proximity, nonconsensual communication, or verbal, written, or implied threats, or a combination thereof, that would cause a reasonable person fear". It is interesting that the definition excludes most electronic forms of stalking as there is often a lack of visual or physical proximity in such cases.[5]

The definition used in the *British Crime Survey*[6] is that stalking is "two or more incidents causing distress, fear or alarm of obscene/threatening unwanted letters or phone calls, waiting or loitering around home or workplace, following or watching, or interfering with, or damaging personal property carried out by any person". In parallel, the psychiatric literature has defined stalking as a course of conduct by which one person repeatedly inflicts on another unwanted intrusions to such an extent that the recipient fears for his or her safety.[7] Whilst each source offers its own interpretation, repetition leading to fear is a recurring theme in any definition.[8]

Stalking and harassment are distinctive in law since the offending behavior is said to occur only when the victim reports him/her self to be distressed as a result of the behavior of another to whom they

---

3 J. ANGEL, COMPUTER LAW 17 (4th ed. Blackstone Press Ltd, London, U.K. 2000).

4 Randy McCall, *Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada-Concepts and Recommendations*, www.vaonline.org (last visited May 15, 2013).

5 Patricia Tjaden & Nancy Thoennes, *Stalking in America: Findings from the National Violence against Women Survey* (1998), http://www.ncjrs.gov/pdffiles/169592.pdf.

6 K. Smith, K. Coleman, S. Eder & H. Hall, *Homicides, Firearm Offences and Intimate Violence*, 2 CRIME IN ENGLAND AND WALES 1-97 (2009/10.)

7 *Id.*

8 http://www.beds.ac.uk/research/irac/nccr (last visited May 6, 2013).

believe to be threatening. The victim's perception of the offending behavior and its effects are therefore pivotal in providing criteria on which to make a charge.

Online Harassment and Cyberstalking in India: Legislative Remedies

Since the 1990s, stalking and harassing has become a common occurrence due to Internet.

In 2001, India's first cyberstalking case was reported. Manish Kathuria was stalking an Indian lady, Ms. Ritu Kohli by illegally chatting on the web site, *www.mirc.com* using her name; and used obscene and obnoxious language, and distributed her residence telephone number, invited people to chat with her on the phone. As a result, Ms. Ritu Kohli was getting obscene calls from various states of India and abroad, and people were talking dirty with her. In a state of shock, she called the Delhi police and reported the matter. The police registered her case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 refers only to a word, a gesture or an act intended to insult modesty of a woman. But when same things are done on Internet, then there is no mention about it in the said section. This case caused alarm to the Indian government, for the need to amend laws regarding the aforesaid crime and regarding protection of victims under the same.

1. The Information Technology (Amendment) Act, 2008

As a result, **Section 66A** of the Information Technology (Amendment) Act, 2008 (hereinafter the IT Act, 2008) states:

> **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 makes 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 3 years and with fine.

The IT Act, 2008 does not directly address stalking. But the problem is dealt more as an 'intrusion on to the privacy of individual' than as regular cyber offences which are discussed in the IT Act, 2008. Hence the most used provision for regulating cyberstalking in India is Section 72 of the IT Act, 2008 which runs as follows:

Section 72: Breach of confidentiality and privacy.- Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made 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 2 years, or with fine which may extend to 1 Lakh rupees, or with both.

Section 72A: Punishment for disclosure of information in breach of lawful contract.- Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to 3 years, or with a fine which may extend to 5 lakh rupees, or with both.

In practice, these provisions can be read with **Section 441 of the Indian Penal Code, 1860** which deals with offences related to criminal trespass and runs as follows:

Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any

such person, or with an intent to commit an offence, is said to commit criminal trespass.

2. The Criminal Law (Amendment) Act, 2013

Prior to February 2013, there were no laws that directly regulate cyberstalking in India. In 2013, Indian parliament made amendments to the Indian Penal Code, 1860 introducing cyberstalking as a criminal offence.[9]

After 'the December 2012 Delhi gang rape incidence', the Indian government has taken several initiatives to review the existing criminal laws. A special committee under Justice Verma was formed for this purpose and basing upon the report of the committee, several new laws were introduced. In this course, anti-stalking law was also introduced. The Criminal Law (Amendment) Act, 2013 added **Section 354D** in **the Indian Penal Code, 1860** to define and punish the act of stalking. This section is as follows:

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

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

(i) that it was pursued for the purpose of preventing or detecting crime, and the person accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the state; or

(ii) that it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or

(iii) that in the particular circumstances the pursuit of the course of conduct was reasonable.

(2) Whoever commits the offence of stalking shall be punished with imprisonment of either description for a term which shall not be less than 1 year but which may extend to 3 years, and shall also be liable to fine.

---

9 The Criminal Law (Amendment) Act, No. 13 of 2013, INDIA CODE (2013).

Stalking has been defined as a man who follows or contacts a woman, despite clear indication of disinterest to such contact by the woman, or monitoring of use of Internet or electronic communication of a woman. A man committing the offence of stalking would be liable for imprisonment up to 3 years for the first offence, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to 5 years and with fine.[10]

The term "cyberstalking" can be used interchangeably with online harassment. Cyberstalker does not present a direct threat to a victim, but follows the victim's online activity to collect information and make threats or other forms of verbal intimidation. A potential stalker may not want to confront and threaten a person offline, but may have no problem threatening or harassing a victim through the Internet or other forms of electronic communications.

Enforcement Problems

"Even with the most carefully crafted legislation, enforcing a law in a virtual community creates unique problems never before faced by law enforcement agencies."[11]

These problems pertain mainly to 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, as explained below, that a potential offender may not be within the jurisdiction where an offence is committed. Anonymous use of the Internet, though beneficial in many instances, also promises to create challenges for law enforcement authorities.[12]

The Internet is a global medium regardless of frontiers, and this creates new possibilities for the so-called cyberstalker. Cheap and easy access to the Internet means that distance is no obstacle to the cyberstalker.[13] Anyone can become a target for a cyberstalker through the use of the Internet in many forms. The victim can be

---

10 http://en.wikipedia.org/wiki/Criminal_Law_%28Amendment%29_Act,_2013(last visited May 1, 2013).

11 B. Jensen, *Cyberstalking: Crime, Enforcement and Personal Responsibility in the Online World*, http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm (last visited May 1, 2013).

12 L. Ellison & Y. Akdeniz, *Cyberstalking: The Regulation of Harassment on the Internet*, CRIMINAL LAW REVIEW-*CRIME, CRIMINAL JUSTICE AND THE INTERNET* 7 (Special ed. Dec. 1998).

13 *Id.*

contacted by e-mail, instant messaging (IM) programs, via chat rooms, social network sites, or the stalker attempting to take over the victim's computer by monitoring what he is doing while online. The Internet is not a "lawless place"[14], and there are difficulties in applying laws that are made for specific nation states and this would be also true of applying national harassment and stalking laws to the Internet.

Self-help Approaches

After researching on various aspects of cyber talking, the problem came to know is that the limitations of legal regulation of online harassment in cases which involve anonymous cyberstalkers. These limitations in legal regulation are, to some extent, compensated for by the availability of non-legal solutions to online harassment. A number of more suitable ways in which users can protect themselves from online harassment are discussed below.

- Do not share personal information in public spaces anywhere online, nor give it to strangers, including e-mail or chat rooms.
- Do not ever reply to offensive, defamatory, provocative e-mails if you get them.
- Do not respond to flaming, or get provoked online.
- You can use online segregating tools such as blocking of the email ID, reporting of spams, and are also advised to use strong encryption programmes such as the Pretty Good Privacy (PGP) which ensure complete private communications.
- If you are being stalked, you don't have to be a victim. Report the incident to your Internet Service Provider, police station in your city, or an online help agency and also take advice from your techno-savvy friends.
- Keep evidence of possible harassment by saving messages, or copying and pasting them to self e-mails. Prevention is always better than cure.

[14] *See* J.R. Reidenberg, *Governing Networks and Cyberspace Rule-Making*, 45 EMORY LAW JOURNAL 911 (1996).