"CYBERSTALKING: AN EMERGING CRIMINAL OFFENCE"

MILIND RAJRATNAM

INTRODUCTION

Increased dependence of humans on Information Technology has brought with it, some boons as well as curses. We find new technologies and innovations every day. Over the past few decades, our lives have become increasingly digitized. We do more things online than ever before: date, bank, shop, work, socialize and entertain ourselves. We are living in the Age of Convenience, which is both a cause of celebration and a recipe for increased vulnerability. The shift to living virtually has happened so quickly and so pervasively that we have hardly had time to adjust to all the implications. Just like every other sphere of life, crime too has gone online. And we are very poorly prepared. Some of the most prevalent online crimes include cyberstalking, identity theft, or online harassment.

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. Many cyber stalkers are obsessed, unstable, or otherwise mentally ill. Still, others are simply angry or hurt and have crossed the line into criminal activity when expressing these emotions. While they can exhibit charm and eloquence, they are generally isolated and desperate, have very low self-esteem, and are especially sensitive to rejection. The financial ruin of the victim can also be part of their goal. Where some of us may poke our nose into Facebook a little too often or fanatically follow a celebrity online, a cyber-stalker will go further by repeatedly sending unwanted anonymous messages, threats, or comments, and he or she will continue doing these things despite repeated requests and warnings to stop. Internet has thus become an easy medium for frauds, sexual exploitation, exploiting or harassing. It most commonly happens 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.

CYBERSTALKING AND ITS PREVALENCE

What Is Cyber Stalking?

Cyberstalking is a compulsion. It aims to humiliate, control, frighten, manipulate, embarrass, get revenge at, or otherwise harm the victim. Many cyber-stalkers are obsessed, unstable, or otherwise mentally ill. Still, others are simply angry or hurt and have crossed the line into criminal activity when expressing these emotions. While they can exhibit charm and eloquence, they are generally isolated and desperate, have very low self-esteem, and are especially sensitive to rejection. The financial ruin of the victim can also be part of their goal. Where some of us may poke our nose into Facebook a little too often or fanatically follow a celebrity online, a cyber-stalker will go further by repeatedly sending unwanted anonymous messages, threats, or comments, and he or she will continue doing these things despite repeated requests and warnings to stop. Although in previous years' stalkers tended to be ex-lovers, spouses, acquaintances, or other known individuals to the victim, today, cyber stalkers can be either known or unknown. They can target their victims via social media, dating websites, blogs, or by hacking into phones or personal computers where most of us store highly personal information without any security in place. Worst of all, cyberstalking can lead to escalation and does so in over 70 percent of cases. This can result in physical attacks and abductions, especially as perpetrators of domestic violence are more easily able to locate victims online who may be in hiding.

Elements of cyberstalking

1. 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 of Internet or other electronic means 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.

ACTS OTHER THAN CYBERSTALKING

Cyber Harassment

The terms cyberstalking and cyber harassment are often used interchangeably to refer to crimes committed against victims through electronic communications devices. Although the crimes are similar, they differ in the elements and mental state. The National Conference of State Legislatures defines cyber harassment as "threatening or harassing email messages, instant messages, blog entries or websites dedicated solely to torment an individual." Cyber harassment is similar to cyberstalking, but victims of cyber harassment generally are not subjected to behavior that would instill fear in a reasonable person. The concept of cyber harassment is often included in general harassment or telephone harassment laws by merely adding the phrase "electronic communication. "Cyberbullying is also an important and related issue, but is beyond the scope of this project.

Online Impersonation

Online impersonation consists of creating a fake social media page, an Internet site, or an e-mail address without someone's consent and with the intent to harm or threaten that person. Online impersonation can be committed in many ways. For example, perpetrators have created fake web pages of celebrities and candidates running for public office, and then made statements to the public on behalf of those celebrities and candidates. Perpetrators have also impersonated victims through e-mail or social media, and subsequently contacted the victims'

friends and family with a fabricated story that the victim is in danger and in dire need of money. Some states include the crime in general cyberstalking and cyber harassment laws, while others draft separate statutes to criminalize the distinct offense.

TYPES OF CYBERSTALKERS

Cyber stalkers can be categorized into three types:

a. Common obsessional cyberstalker: He/ She refuses to believe that their relationship is over. They mislead by portraying that they are harmlessly in love.

b. Delusional cyberstalker: 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. Vengeful cyberstalker: 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.

TYPES OF CYBERSTALKING

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) E-Mail 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 initiate 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 victim's 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 (key logger) and viewing the computer's 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.

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 breakup of a relationship or 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 the 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.

RELATED LAWS IN INDIA 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 behaviors such as cyberstalking. In 2013, Indian Parliament made amendments to the Indian Penal Code, introducing cyberstalking as a criminal offence.

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 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 boilable 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.

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;

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.

Sections of IPC dealing with various cybercrimes:

· 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).

INCIDENTS OF CYBERSTALKING IN INDIA

- ***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 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 her to be his wife. It is hoped that the decision in this would favor the victim.

- ***Karan Girotra vs State & Anr.***

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 i.e. 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 in Delhi, where the mother of the complainant gifted the petitioner a santro car, jewelry, 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.

PREVENTIVE MEASURES

Here are a few important pointers to help you thwart cyberstalking, whether it's directed at you, your PC, or your family:

1. Be careful what personal information you share online.

2. Create a different email account for registering in social networking sites and other online spaces.

3. Do not feel obligated to fill out all fields when registering online or provide identifying information such as birth dates and place in required fields.

4. In your online user profile, use a photo that doesn't identify you or your location, so you can't be recognized.

5. In your online user profile, use a photo that doesn't identify you or your location, so you can't be recognized.

6. In your online user profile, use a photo that doesn't identify you or your location, so you can't be recognized.

7. In your online user profile, use a photo that doesn't identify you or your location, so you can't be recognized.

8. Consider using a name that is not your real name or a nickname as your email name, screen name or user ID.

9. If you are breaking up with an intimate partner – especially if they are abusive, troubled, angry or difficult – reset every single password on all of your accounts, from email and social networking accounts to bank accounts, to something they cannot guess.

10. Services such as Facebook change their privacy policy all the time, so it is a good idea to check your privacy settings to make sure you are sharing the information you want to share with people you trust and not the general internet public

11. Ask your family and friends to take prior permission before posting and information about you.

12. Do an internet search of your name regularly and monitor whether you appear online.

13. Make sure that your internet service provider (ISP), cell phone service, instant messenger (called internet relay chat, or IRC in some terms of service) network and other services you use has an acceptable privacy policy that prohibits cyberstalking.

14. If you have a blog or personal website you maintain, please read the information on the next page.

CONCLUSION

In 19 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 cyberstalking 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. Cyberstalking 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.