International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Increasing Vulnerability of the user Data at Cyberspace

N Parmesh

Student, Sastra Deemed University, Thanjavur, Tamil Nadu, India

ABSTRACT

Cyber Stalking is a burgeoning concept where a person is vigiled by another using electronic media without consent. Using the pragmatic stealthiness of networking tactics, a stalker intrudes into the privacy of the victim causing him harm either coming in physical contact or by inflicting mental agony my the means of misusing the information collected online via stalking. The stalker may demand for money in exchange of sparing his/her dignity or put across unreasonable demands such as to have intimate relationship with him. It can be noticed very often that a victim is left with no option other than to cater to the unreasonable demands. Such attacks have to be handled through either efficient enforcement agencies with adequate technical backing or through extremely stringent laws which would create fear in the minds of the offenders. Unfortunately the India is still in the phase of growth in the terms of its technical advancement which makes it pracitcally impossible to bring the offender before the Court of Justice. This research article deals with the concept of cyber stalking in detail. It also explains about the self regulatory user guidelines and the legal structure required to secure user data from illegal intrusions and embezzlements.

KEYWORDS: *cyber, stalking, attack, technique, virus*

How to cite this paper: N Parmesh "Increasing Vulnerability of the user Data at Cyberspace" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.1104-1106, URL: www.ijtsrd.com/papers/ijtsrd30251.pdf

IJTSRD30251

INTRODUCTION

With the prodigious growth in Online Media Platforms, it is very much impossible for a person to confine his data to himself. The ease at which it allows others to have access to personal information has constructed an insurmountable threat to privacy. Stalking has been in limelight for some time now and it has started guising in different contours. Cyberstalking is one of the kinds, the successor of the traditional methods of physical surveillance and intimidation of stalking victims. Most commonly used methods include stalking through chat messengers, emails and other interactive portals.

The concept of cyberstalking is assuming a substantial advancement in the terms of its misuse because it is extremely difficult to trace the ones involved behind it. The stalkers take undue advantage of the information posted by the victims in different social networking websites and other networking platforms. One of such incidents which happened in California is worth noting. A girl posted an image catering to discussions of her sexual fantasies saying 'She wanted to play rape games' mentioning her real-time mobile number and address of residence. Soon after that, she was threatened by few men at her doorstep for fulfilling her sex fantasies.

CYBERSTALKING TECHNIQUES

Cyber Stalking can be effectuated through various techniques such as hacking, SQL injections, Virus Dissemination, Denial-of-Service Attack, Email Spamming & Bombing, Web jacking, Data diddling, identity theft and credit card fraud, salami fraud attacks etc. Hacking is the essence of all the internet related crimes committed across the globe. By hacking, the intruder would get complete access to the computer or to any electronic device without the permission of the victim. Viruses may harm the computer acutely by attaching itself to the system files. These viruses can be disseminated through junk electronic mails and through corrupted file engines. This would eat up the entire memory in the system rendering it paralyzed for-ever.

Web high jacking is one such tool at the hands of the stalker to jeopardize the victim. Through this, the hacker might fraudulently change the content of an original website or can even redirect the user to a similar website keeping him in the realm of ignorance. Social Media accounts are high jacked to vary the content of the information with a detrimental effect to the real user. Salami slicing attack is an internet fraud which involves stealing of money (small amount) from the victim's account repeatedly. The victim may come to notice about it only after a long period when the bank statement would reveal a hefty sum being stolen.

Cyber Stalking is construed broadly as it includes various feats in itself. It includes and is not limited to identity theft, solicitation of minors for illegal activities, computer monitoring, false accusations, data theft and damage to data or to equipment. These acts are linear descendants of stalking through telephone calls a few decades before. Surveillance through telephonic calls included hate messages and obscene comments. Technology has opened up new dimensions to vigil the virtual activities of the victims over the social web. In research conducted in the United States, it revealed that the number of active stalkers was more than 2, 00, 000. It also meant that one is every 1250 was a stalker.

EFFECTS OF CYBERSTALKING

Cyber Stalking involves implied and threatened violence rather than actual violence at the initial stage of harassment. Nonetheless, the harm which it produces is nothing less than one produced through actual violence. The issue might look insincere and trivial but it had dire repercussions impelling the victims to commit suicide. Cyberstalkers can target multiple users at the same time to intimidate and threaten either for fulfilling their monetary demands or for tarnishing the reputation of the victim involved. Physical stalking might not have such harrowing effects. It is appalling to see that 90% of the people victimized by stalking are women. In this technological era, people constrain themselves to the virtual world via their devices making them vulnerable to data misuse. Women especially have got to be extremely cautious and discreet before uploading any sensible information which might give a leeway to the stalker to harm them. At the same time, it is disheartening to see that a woman cannot express herself completely in this world of virtual dynamics. It is also very pertinent to note that 95% of the stalkers involved are men. This categorically indicates that the element of **"Mutual Respect"** necessary between men and women in the society is dwindling. Educating men regarding the responsibility they owe towards women can only reduce such devious behaviors. Sex education to the people, especially men, at the earlier stages of their life would also curtail such stridulous behavior towards women.

THE FLIP SIDE OF THE TECHNOLOGICAL ERA

By use of different soft-wares, a stalker can assume complete control over the computer of the targeted victim. This would imply that the stalker can access all the data on the computer of the victim. The stalker can send emails, messages as if it were to be sent by the original user himself. Thus in the days to come, the concept of Privacy might only be present in textbooks. The only way the victim can come out of this trap is by abnegating the internet address. It can also happen with mobile phone chat applications too. Real-time keystroke logging is one of such techniques which are great tools for the stalkers allowing real-time monitoring and surveillance. Other stalking tactics involves following the women from a distance, or spying the victim using the visual camera or audio transmitters or through global positioning system.

STATISTICS RELATING TO CYBER STALKING ACROSS THE GLOBE

There are several occurrences where the stalkers have morphed the images to make it look revealing and sexually attractive. Using such images, the stalkers have forced the victims to have an intimate relationship with them. Stalking was often committed by those who had a relationship with the victims before. National Intimate Partner and Sexual Violence Survey conducted a research which revealed that 1 in 6 women are stalked. It also affirmed that 2/3rd of such stalkers were current or former intimate partners of the aggrieved. 1/4th of the stalkers were identified to be the acquaintance of the victim and only 1 in 8 females victims were stalked by the strangers.[1] Nearly 50% of the victims who were stalked in the United States were less than 25 years.

A. INTIMATE PARTNER FEMICIDE

The repercussions of stalking don't wind up with virtual threatening and intimidations, there are several cases where the stalking has resulted in further severe altercations leading to acid attacks and murders. Most of such murders were committed by the intimate partners itself. It was found in one of the surveys that 76% of intimate partner femicide have been stalked before their murder and also 89% of the victims were assaulted and harassed frequently for one whole year before their murder.[2] The cyberstalkers by assuming the identity of the victim can reveal personal victim's sensitive information to the online interactive platforms which in turn would also attract responses from the cyber community. While the victims were stalked, their day to day activity and routine was found to be adversely affected. The research concluded that 46% of the victims never knew what would happen next or how the problem had to be dealt. Among others, 29% of such victims felt that such stalking might never end. It is also very significant to note that the victims who went through stalking harassment faced social dysfunction, anxiety, insomnia, and severe depressions. These characteristics were more prevalent when the stalker had come into physical contact with the victim.[3]

PHYSIOLOGICAL BACKLASH

Stalking research Centre in the United States is organized to provide effective control over stalking and to increase awareness among the general public regarding cyber safety and control. It also works for ensuring proper rehabilitation facilities to the ones who have undergone serious agony and harassment through stalking. The research center also analyzed the reason as to why do the victims shield their malaise without taking initiative for legal redressal. The victims were afraid of the stalker and the harm which the stalker may inflict. The victims were always scared that they have contributed to their own agony and had no sufficient evidence. It is also evident from the research that most of the victims never believed that the police would not be able to trace the real culprits.[4] Prosecution and conviction of the stalking offenders are comparatively very less compared to the number of stalking cases registered because of the paucity of evidence on behalf of the complainant to prove the case.[5]

The first case relating to Cyber Stalking in India was Manish Katuria's case (2008). The accused abused the victim over the telephone and dissipated her telephone numbers to

[1]Matthew J. Breiding et al., "Prevalence and Characteristics of Sexual Violence, Stalking, and Intimate Partner Violence Victimization - National Intimate Partner and Sexual Violence Survey, United States, 2011", Centers for Disease Control and Prevention Morbidity and Morality Weekly Report , Vol. 63, No. 8 (2014)

[2]Judith McFarlane et al., "Stalking and Intimate Partner Femicide", Homicide studies 3, no. 4 (1999)

[3]Eric Blauuw et al., "The Toll of Stalking," Journal of Interpersonal Violence, 17, no. 1 (2002):50-63

[4]Brewster, M. (2001). Legal help-seeking experiences of former intimate-stalking victims. Criminal Justice Policy Review, 12, 2, 91-112.

[5]Baum, K., Catalano, S., Rand, M., & Rose, C. (2009). Stalking victimization in the United States (NCJ 224527). Bureau of Justice Statistics Special Report. Washington, D.C.: U.S. Department of Justice.

several others. She started getting calls at odd hours and was harassed severely. She filed a complaint against the stalker and was soon arrested by tracing their IP addresses. The case was filed under section 509 of the Indian Penal Code as the Information Technology act was not in force when the complaint was filed. Only in 2008, section 66A was introduced to curb down the crimes committed via online platforms. The above-mentioned provision of law was struck down being called a draconian law infringing the fundamental right to speak and express as per Article 19(1) (a) of the Indian Constitution in the case of Shreya Singhal v. Union of India[6].

LAWS GOVERNING CYBER STALKING IN INDIA

The cases relating to cyberstalking are increasing steadily for a decade but most of them have ended in the acquittal of the accused. Stalking is an offence explicitly specified in Indian Penal Code under section **354D** of **IPC**. Stalking was brought through amendment into the Indian Penal Code after the infamous Delhi Gang Rape case. It is significant to note that this law protects the rights of women against stalking and various other similar offences. The fact that even the men are equally vulnerable to stalking and other such offences cannot be overlooked. The legislators through this section might have assumed that the offenders are always men and the victims are always women. This suffers from the vires of arbitrariness infringing Article 14 of the Indian Constitution. So the legislation brought should be amended to substitute the word "Woman" by "any person" to pull out the arbitrariness prevailing in this section.

The section 354D of IPC says that when a woman is contacted repeatedly to foster personal information even after her clear disapproval and disinterest, the act would amount to stalking. The maximum punishment prescribed in this section is five years. The act clearly purports that the offence would also include stalking through online interactive portals and networking. Prior to this provision coming into existence, the offence of stalking was governed under **section 509 of the code** which states that any person who uses word, gesture or act intended to embarrass and insult the modesty of a woman would be an offence punishable with a maximum imprisonment of 1 year or fine or both. It is pertinent to refer to the **Sec. 67** of the Information Technology Act, 2000, though it does not explicitly deal with the offence of stalking. It deals with the offences committed through the electronic medium which states that if a person publishes or transmits obscene material in electronic form to either intimidate or to harass the victim would be punishable under this section with a maximum punishment of 5 years.

Despite Stringent laws in force, the situation prevalent in India is disquieting and alarming. India doesn't have a specific law to deal with cyberstalking, unlike America. A specific legislation has to be meticulously drafted to effectively make the offenders accountable. This is not practically feasible until the country is technologically sound in combatting the ever growing technical debacle. Research centers should be organized to train the professionals to effectively respond to the stalking. **Sec 354 of IPC** does not entitle a redressal mechanism for a man. Both men and women are equally vulnerable to stalking. The police officials are not competent enough to respond quickly to such cases which in turn give the stalker sufficient time to makeshift, thus fleeing away from the justice. Most of the times, the authorities never took such cases being fearful of the enforcement as the offenders belonged to a foreign nation.[7]

TERRITORIAL JURISDICTION OF THE COURTS TO TRY STALKING OFFENDERS

The main issue of territorial jurisdiction in reference to the offence of stalking is in the realm of a blind spot as the offender can belong to any part of the world. To effectively deal with this issue, India should have active extradition agreements with all the countries, so as to implement the laws enforceable in India. An extradition agreement is an arrangement through which a criminal is brought back to the country where the offence was committed. Here, it is worth noting that the scope of extraterritorial Jurisdiction as per section 75 of the Information Technology Act which states that irrespective of the place of commission of the offence, the offender shall be governed by Indian Legislation. The actual problem arises when the criminal laws relating to the offence and the territorial jurisdiction differs between the countries involved.

CONCLUSION

Apart from the Legislature and Judiciary of the country playing a curative role, the people should take an active part in playing a precautionary role by regulating themselves. The government should take effective steps to create awareness among the people regarding the information they reveal to others either in person or through online interactive portals. Though it is practically impossible to shun away from the virtual world, it is recommended that the users should conscientiously reveal sensitive information such as their contact numbers, residence details, passwords or financial information such as credit and debit card details, medical records, biometric information etc. It is also recommended that the passwords should be different for different Web portals and interactive social media sites. The stalkers may take advantage of the vulnerability of the children. So it is very important to educate them on how to use the internet properly. Cyber Protection Agencies such as Cyber Angels & WHOA[8] provides education to the general public pertaining to self-regulation and awareness. Various soft wares are available on the online platforms which gives a reasonable security against intrusion over personal data. These would reduce the threat of online felonies. Internet Service Providers (ISP) does play a major role in governing the activities of users across the globe. Improvised Firewall protection over websites offered by the ISP can reduce the crime rate online. It is greatly safe to upload fake numbers and addresses concealing one's identity ensuring safety. Women have got to be more careful on this regard as India is still on the gridlock failing to provide adequate safety.

[6]AIR 2015 SC 1523

[7]Cyber Stalking: A Critical Study; Bharathi Law Review-June, 2017

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