Christ University Law Journal
2017, Vol. 6, No. 2, 61-75
ISSN 2278-4332X | https://doi.org/10.12728/culj.11.4

Comparative Analysis of Cyber Stalking Legislations in UK, US and India

Arunbaby Stephen*

Abstract

The Internet, with its vast connectivity and ample resources, provides an easy platform for committing crimes. Cyber stalking is one such offence, which has grown in the last two decades with the advent of cheap and fast internet connectivity. The Internet provides various means by which cyber stalking can occur. The lack of boundaries on the internet creates more risk for the users and as more and more people start using internet, the scope and complexity of this problem will only increase. More and more states are passing exclusive statutes for tackling Cyber Stalking, believing that their offline stalking statutes are not enough to handle different aspects of this issue. This paper analyses the different legislations passed across the world to tackle cyber stalking. With stalking itself being a comparatively fresh offence in India, it has been a late entry into the field of cyber stalking, with the first provision being made in 2013, in the form of Section 354 D of the Indian Penal Code. The article examines the shortfalls of this provision and the ways in which they can be tackled.

Keywords: Criminal Law Amendment, Cyber Stalking, Internet, Privacy, Section 354D of Indian Penal Code

* NALSAR University of Law, Hyderabad, India; babynuals@gmail.com

I. Introduction

Internet is the most efficient new age tool for communication and sharing of information. It has reduced the distance between people, and has made any information accessible with a few mouse clicks. While new technology makes our lives easier and helps in better sharing of ideas, it has also resulted in some negative consequences. As it is with every innovation, human ingenuity has identified ways to misuse the internet for one's own selfish needs and for achieving ulterior motives. Cyber stalking is one such abuse of the internet's immense potential which is the primary concern of this paper. Cyber stalking may occur when a person consistently tries to contact another person with the intention of controlling the victim's life or instilling fear in them. It is true that even males can be the victims of this, but studies show that majority of the victims are female. Women are the minority in the cyber world and hence, there is fierce competition among men for their attention.[1] It is different from stalking in the physical world, due to the increased potential of abuse because of the added dimension of virtual world. Even the act of physical stalking is comparatively a fresh entry into legislations with the first anti-stalking legislation being passed in California after a TV star Rebecca Schaeffer was murdered by her stalker.[2]

The Internet provides various means by which cyber stalking can occur. It can be in the form of a persistent online communication, posting messages on online platforms or chat groups which violate the victim's privacy, or by monitoring the online activities of the victim. As the use of technology increases it would result in more incidents of cyber stalking happening and hence, legal systems across the world have codified laws exclusively to handle cyber stalking. The lack of norms, the privilege of anonymity, and relatively low risk of facing consequences emboldens the stalker to go about his business in the cyberspace. The lack of boundaries on

---

[1] NANDAN KAMATH, *Cyber stalking a web of obsession, in* LAW RELATING TO COMPUTERS INTERNET & E-COMMERCE249 (Universal Publishing Co., 5thed).

[2] Naomi Harlin Goodno, *Cyberstalkinga New Crime: Evaluating Effectiveness of Current State and Federal Laws*, 72 MISSOURI L. R. 125(2007).

the internet creates more risk for the users and as more and more people start using internet, the scope and complexity of this problem would only increase.

II. Definition and Nature of Cyber Stalking

Cyber Stalking can be defined as a behavior by which an individual or group of individuals use internet and communication technology to harass another individual or group. It involves engaging in a course of conduct, to communicate or causes to be communicated words, images, or language through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose.[3] It is promoted by a delusional and narcissistic perception of a relationship and intended to empower the 'predator' to feel omnipotent and in control, while reducing the prey's emotional state to vulnerability and fear.[4] It includes online harassment by sending unwanted, abusive, or obscene emails or communications or jeopardizing the system by sending computer viruses or even by impersonating the victim in cyber space. Cyber stalking essentially violates the privacy of an individual. Providing personal information about the victim on public online platforms, or publishing altered or offensive pictures in online platforms also falls under cyber stalking. The stalker acts in a way that undermines the ability of the victim to take a decision in his/her own life.

Generally, cyber stalking is a course of conduct that takes place over a period of time and involves deliberate repeated attempts to cause distress to the victim. It consists of repetitious conduct which would cause fear in a reasonable person. A mere unsolicited communication does not amount to cyber stalking, but it involves methodical, deliberate and persistent efforts on the part of the stalker and would continue even after the victim has asked the stalker to stop communicating with him/her. Victims may be totally unaware of the physical location of the stalker which makes it more fearful for the victim. It totally disrupts the normal life of

[3]Florida Statute § 784.048(1)(d).
[4]*Supra* note 1, at 248.

the victim and affects the peace of mind. With the advent of social media, stalkers have the ability to post comments about the victim for the whole world to see which can harass the victim in front of a larger audience. It might also affect the professional life of the victim as she has to keep away from online activities for a while to stop this unwanted communication. The stalker might also assume the personality of the victim on online discussion forums or social media and might post hateful messages the backlash of which would be faced by the victim. There are high chances that online stalking might lead to violence in the real world. Online harassment might also include sexual harassment and might be indicative of obsessive nature of the stalker. In the infamous incident of Amy Boyer, her stalker had been running a website fully dedicated to her without her knowledge for two years. He published information about what she wore, what she did, what she said, etc., and ultimately committed suicide after killing her. Some stalkers go to the extent of installing key loggers in the system of the victim (especially when victim shared an intimate relationship with the stalker at one point of time) which supplies them with endless source of information. Nandan Kamath has classified Cyber Stalkers generally into three categories:[5]

- Simple obsessional
- Erotomanic
- Love obsessional

In 'simple obsessional' stalker behavior, a prior relationship exists between the stalker and the victim. The victim could be an acquaintance, colleague, or co-worker. The stalking begins when the relationship has deteriorated or terminated or when the stalker feels he has been mistreated. He attempts to restore the same level of intimacy or tries to harass the victim as retribution. This type of stalking can turn out to be the most dangerous type. In case of an 'erotomanic' the subject believes that the victim loves him passionately when they have not even met. This type of behavior does not result in any harm because the stalker will have the best interest of the victim in mind. In case of 'love obsessionals' they

[5]*Supra* note 1, at 250 – 52.

may not know the subject of obsession personally, usually they become aware through media and their goal is to get their subjects to respond to their expressions of love. [6]

III. Difference between Offline and Cyber Stalking

The objective of the stalker in both cyber as well as physical stalking is the same; it is the desire to exert control over the victim.[7] Even then cyber stalking and offline stalking differ in many ways. Anonymity is one condition which empowers human beings to do acts which otherwise they would not dare to do because they feel they have protection of the 'veil of anonymity'.[8] This condition is easily satisfied by cyber world where a distinct identity can be created in a matter of minutes. Anonymity helps to overcome inhibitions and inabilities of the stalker which would also prompt stalker to indulge in harassing behavior which he otherwise would not have indulged in real life. With the spread of internet and web enabled devices any person can abuse another within the veil of anonymity, and within a matter of seconds the entire world can view the offensive information. Anonymity can be easily achieved by using remailer technology. It removes all identification features from a mail and uses a random header. The trail created would be so complex that unprecedented anonymity would be granted. Unlike in physical stalking the time and effort required by the stalker is minimal and the cost is also negligent. For example, an offline stalker may harass by making repeated phone calls but each of such phone call requires his time and effort while in cyber stalking he can program his system to send an offensive message to a particular person at regular intervals without any further effort from his part. While in physical stalking, the victim and the stalker need to be in the same geographical location, in case of cyber stalking the act can be done from thousands of miles away. The easy and cheap access to internet due to technological development improves the ability of the stalker to commit his activities behind a veil of anonymity from a far off place without ever being in the

[6] *Id*.

[7] *Supra* note 2.

[8] Merrit Baer, *Cyberscapingand the landscape you have created* 15 Va. J.L. & Tech. 153, Fall, 2010, 156

presence of the victim. Cyber stalking from another country also makes investigation, collection of evidence, and prosecution more difficult.

Unlike in the offline world, in the cyber world the stalker can easily impersonate the victim. The stalker can easily post inflammatory or obscene messages in an online bulletin board under victim's name which would result in victim being at the receiving end of hate mails or lewd messages. Another fundamental difference between offline and cyber stalking is that in cyber stalking, innocent third party can be incited to commit harassment. For instance, a cyber stalker after being repeatedly rejected by the victim posed as the victim and posted in an online discussion forum that she fantasized of being raped. He published the name and address of the victim along with her phone number which resulted in men arriving at her house on numerous occasions to fulfill her wish.[9] So in a way cyber stalking is more frightening than offline stalking because it requires only minimum effort, minimum cost, provides instantaneous connectivity and anonymity, and also ample opportunities to pose as a third person.

IV. Legal Framework around the World

IV. 1 United Kingdom

There is no specific legislation in UK which deals with cyber stalking as such. Instead there are three major laws used to counter harassment which are also used in case of stalking. Telecommunications Act 1984, Malicious Communications Act, 1988 and Protection from Harassment Act 1997, are the three major statutes used to tackle the issue of stalking as well as cyber stalking. The Telecommunications Act 1984, makes it an offence to send a message which is inappropriate, threatening, or indecent. The 1988 Act, which is wider in its ambit is an Act for punishing those who send letters or deliver articles for the purpose of causing anxiety or distress. Section 1 of the Protection from Harassment Act 1997, states that, a person must not pursue a course of conduct which

[9]Bill Wallace, Stalkers Find a New Tool--The Internet, S.F. CHRON., (Jul. 10, 2000), http://www.sfgate.com/cgi-bin/article.cgi?file=/ chronicle/ archive/2000/07/10/MN39633.DTL

amounts to harassment of another or which he knows or ought to know amounts to harassment of other. Section 2A of the Act states that in order to constitute stalking three conditions have to be satisfied:

1) Course of conduct
2) Course of conduct in breach of Section1 under the Act
3) Course of conduct which amounts to stalking.

The Harassment Act does not try to define stalking, instead in Section 2A (3) certain activities which would amount to stalking are listed:

- Following a person
- Attempting to contact or contacting a person
- Publishing any statement or other material relating or purporting to relate to a person
- Monitoring the use of internet or electronic communication of any person
- Watching or spying on a person
- Interfering with property in possession of a person.

The list provided is not an exhaustive list, and whether the course of conduct would amount to stalking has to be determined by checking whether the conduct would cause harassment to a reasonable person. The offence under Section 2A is a summary offence and if found guilty, the stalker would be punished with imprisonment for a period not exceeding six month or with fine.

The more serious offence is under Section 4A which involves the following elements:

- Course of conduct
- Which amounts to stalking
- This causes another to fear on at least two occasions that violence will be used against him or her or causes serious alarm or distress which has a substantial adverse effect on his or her day to day activities.

Substantial adverse effect would involve the victim changing his way to work, pattern of work or employment itself, or deterioration of victim's physical and mental health, etc. Such activities are punishable by imprisonment for a maximum period of five years and Court is also enabled to pass a restraining order under Section 5 to prevent further contact of offender. The Act also enables a victim to file for injunction in civil court to prevent future harassment and to obtain damages. But recently the Act has been criticized for becoming a tool for curbing free speech as a result of misuse of the Act by corporations. Peaceful protesters are at the receiving end of civil injunctions which violate their right to express and protest.[10]

Before the enactment of 1997 there have been few interesting decisions from UK Courts where stalking has been brought under the ambit of offences like 'assault' 'grievous body harm' and 'public nuisance'. In *Burstow*[11] the Crown Court convicted the accused for causing serious body harm to the victim by a campaign of silent phone calls. The depression suffered by victim was held as inflicted upon her by the accused. The Court of Appeals affirmed the ruling. In *R v. Ireland*,[12] the Court of Appeals stretched the meaning of Assault to hold a series of calls followed by silence would constitute assault. Usually assault is constituted when force can be applied immediately but the Court in Ireland gave rise to prospect of long distance assaults. In *R v. Johnson* [13] Court of Appeal confirmed the conviction of an appellant of public nuisance based on his numerous obscene telephone calls over a period of five and a half years. These curious judgments seems to be stemming from the fact that there was no special law for tackling stalking which in turn seems to have triggered the 1997 Act.

[10] *Protection of Harrassment Act, 1997,* THE GUARDIAN (Jun. 9, 2009),https://www.theguardian.com/commentisfree/libertycentral/2009/jun/01/liberty-central-protection-harassment.

[11] R v. Burstow, (1996) Crim LR 331.

[12] R v. Ireland, (1997) 1 All ER 112.

[13] R v. Johnson, (1997) 1 WLR 367.

IV. 2 United States of America

In the United States due to its federal nature there exist state laws as well as federal laws which deal with problem of stalking. State legislations can be broadly divided into three categories:

- Statutes that do not address cyber stalking
- Statutes that cover some aspects of cyber stalking
- Statutes that specifically deal with issue of cyber stalking

State statutes that do not address cyber stalking are the ones which require physical pursuit requirements or which do not recognize stalking through electronic communication methods. An example would be anti-stalking legislation of Maryland which insists on physical pursuit requirements.[14] Some states might have telephone harassment statute which is wholly adequate to tackle cyber stalking. Some states have tried to solve this problem by amending the existing state laws to bring within its ambit electronic communication.

The second set of laws is the one with legislations which covers some aspects of cyber stalking. Electronic communication might be included in stalking laws but they fail to address issues like third party harassment and messages sent not directly to the victim. The New York state law addresses the issue of stalking over electronic devices but fails to address two different situations:

- Where the stalker publishes information in some blog post or website and not directly to the victim(as happened in Amy Boyer's case)
- Where the stalker incites third party to harass the victim.

Also, some statutes require fulfilling the 'credible threat' requirement to constitute the act of stalking.[15] State legislations of Louisiana and North Carolina require harassing electronic communication to be sent to victim. Florida and Mississippi statues also have the same issue, since they require the communication to

[14] AilyShimzu, *Towards creation of cyber stalking statute*, 28 BERKELEY J. GENDER L. & JUST.(2013).

[15] *Id*, at 135

be directed to a specific person.[16]These statutes fail to address third party harassment through stalking.

The third category of state statutes contains legislations that address all aspects of cyber stalking. Washington, Ohio, and Rhode Island are the only three states with legislation that address the aspect of third party harassment as a result of cyber stalking. These three states have passed laws exclusively dealing with cyber stalking despite the existence of separate statutes for offline stalking.

Civil protection orders are also available against cyber stalkers depending on the nature of state statutes governing civil protection orders. Protection orders prohibits the stalker from making further contact, possessing firearm, prohibits harassment and abuse, and any other order the Court may find suitable. If violated, the Court can initiate contempt of court proceedings against the violator. Florida and New York allows for issuance of civil protection orders on the basis of cyber stalkers acts.[17]

There are also three major Federal legislations which deal with harassing behavior. They are:

- Interstate Communications Act
- Federal Telephone Harassment Statute
- Federal Interstate Stalking Punishment and Prevention Act

The Interstate Communications Act prohibits interstate threats to harm another person. But the condition is that threat must be to injure or kidnap a person. The communication should be of such a nature that a reasonable person would take it of a serious nature. But the statute fails to address cyber stalking which causes harassment without any threat of injury. In *United States v.Alkhabaz,*[18] the defendant posted violent sexual fantasies about one of his classmate's son, wherein the internet. Court held he has

[16]*Supra* note 2, at 146.
[17]*Supra* note 13, at 121.
[18]United States v. Alkhabaz, 1997 U.S.App.1353.

not violated the statute since there was no element of threat in the communication.[19]

The Federal Telephone Harassment Statute passed in 1934 was amended in 2006 to address the problem of cyber stalking. The definition of Telecommunication devices was expanded to include any device or software which communicates using internet. The statute imposes imprisonment of two years for using a telecommunication device to annoy abuse or threaten any person. However, the Act has some serious drawbacks the major one being the requirement that communication must be anonymous. Secondly, the statute comes into play only on a direct communication and fails to address the concept of third party harassment incited by the Cyber Stalker. Some critics have also argued that the word 'annoy' in the Act is overboard.[20]

The Federal Interstate Stalking Punishment and Prevention Act, 1996 specifically accounts for cyber stalking. It prohibits any individual with the intent to injure, kill, harass, or cause substantial emotional distress from using any interactive computer device to cause these. Initially one condition was that the defendant should have travelled across state line which was removed by 2006 amendment. The statute is comparatively better than other federal statues because it does not insist on credible threat requirement and nor does it apply only in case of anonymous messages.[21] However, the statute is ineffective in handling third party harassment.

IV. 3 India

Before 2013 there was no legal definition for stalking or cyber-stalking in India. Stalking was recognized as an offence in India after the 2013 Criminal Law Amendment Act, which introduced S. 354D to the Indian Penal Code (IPC). Section 354D of IPC defines stalking as follows:

> '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

[19] *Supra* note 2, at 148.
[20] *Id*, at 149.
[21] *Id.*

> 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:
>
> Provided that such conduct shall not amount to stalking if the man who pursued it proves that i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the state ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law iii) in the particular circumstances such conduct was reasonable and justified.'

This definition of Cyber Stalking in comparison with the UK or US laws is very limited in its ambit. The wordings of Section 354D make it clear that offline and online stalking may happen together or as separate acts. The section as such does not try to define cyber stalking but the meaning has to be read from the text of the Section especially Section 354D (2).[22] Subsection (2) does not indicate how the victim can be 'monitored' or 'watched' or what constitutes these acts. It is clear that the section contains the concept of breaching privacy but it has been left to the Courts to expand the meaning of these words. Section 354D is also silent about how the personal information should not be used in online platforms so as to create fear or anxiety to the victim. Another provision which the law should have considered was power to give restraining order like the 1997 UK statute.

Section 354D (2) makes the offence punishable with imprisonment for a period not exceeding three years with fine in case of first conviction. It is cognizable and bailable at this stage but, in case of second conviction, the punishment would be for a period of maximum five years with fine. The offence would be non-bailable in the second chance. The provision is also silent about removing

[22] Debarthi Halder, *Cyber stalking victimization of women: Evaluating effectiveness of current laws in India from restorative justice and therapeutic Jurisprudential perspectives,* http://ssrn.com/abstract=2745352.

an offensive post or message in cyber space and fails to address the mental and psychological harm done to the victim. Proviso to Section 354D has excluded certain conduct from definition of stalking. These exceptions are inspired from Section 1(3) of Protection from Harassment Act 1997, which is UK legislation dealing with harassment. But, it remains to be seen the broad terms of the exception would stand the test of constitutionality especially the last provision which indirectly allows for breach of privacy and confidentiality on grounds that, such conduct was reasonable and justified in the circumstances. This Section suffers from the defect of vagueness and provides law enforcing authority with arbitrary powers to interfere in a person's privacy. There seems to be a direct conflict with this provision and the ration given in landmark case of *PUCL v. Union of India,*[23] where the Court laid down guidelines to regulate the power vested in State under Section 5 of Telegraph Act. The Court held that the tapping of telephone calls infringes the right to privacy and powers under Section 5 can only be used in case of public emergency or where public safety demands it. Even then the guidelines have to be followed.

There is no reason why these procedural safeguards should not be extended to online communications and then, the very exception carved out goes against the standard set by the judgment. Also, the first proviso goes to the extent of saying that a man entrusted with the duty of prevention of crime by the State can commit cyber stalking for the purpose of preventing or detecting a crime. The Supreme Court, in *Kharak Singh v. State of Uttar Pradesh,*[24] struck down as unconstitutional the part of Regulation 236 of U.P. Police Regulations, which allowed for domiciliary visit, because it violated Article 21 of the Constitution. Court quoted extensively from 4th amendment of the US Constitution and held police interference into the sanctity and security of a person's home violates personal liberty mentioned under Article 21 citing Frankfurt.J, from *Wolf v. Colorado*[25]holding, security of one's privacy against arbitrary intrusion by police is basic to a free society and implied in ordered liberty. It will be interesting to see how this

[23] PUCL v. Union of India, AIR 1997 SC 568.
[24] Kharak Singh v. State of Uttar Pradesh, 1964 SCR (1) 332.
[25] Wolf v. Colorado, 338 U.S 25 (1949).

notion of privacy is reconciled with the exceptions provided under Section 354D.

Another criticism which is raised against the provision is that its benefits are available only to female members of society. Even though majority of victims of cyber stalking and offline stalking are female, male victims are not something unheard of and in unfortunate incidents like Megan Meier[26] another woman was responsible for her suicide. Also, the range of actions which fall under cyber stalking is more than the ones mentioned under Section 354D. This Section covers only a part of cyber stalking and to address the entire issue of cyber stalking depending on the facts and circumstances of the case, we might have to use Section 67A of Information Technology Act 2000, or Section 503 of IPC.

V. Conclusion

The 2013 amendment which resulted in Section 354 D of IPC, does not address all aspects of cyber stalking. There is no attempt on the part of the legislation to define the term cyber stalking or to explain what amounts to monitoring the use of any electronic communication. The legislation only addresses the aspect of breach of privacy but does not address other aspects like communicating threats or posting harassing messages in social media. It also does not address the issue of third party harassment due to actions of the Stalker. The constitutional validity of the exceptions provided under the act is yet to be tested and it would be interesting to see how the exceptions would be reconciled with the idea of right to privacy under Article 21. The Indian provisions unlike the UK legislation does not grant a remedy of restraining orders which would have ensured better provisions to the victim especially considering what happened to Swathi.[27] In short the 2013

[26] Megan meier was an american teenager who committed suicide due to cyber bullying through *MySpace.* It was later found the fake account was created by her friends mother. *See also,* http:// www.meganmeierfoundation.org/megans-story.html.

[27] Swathi was an Infosys techie who got hacked to death on June 24 2016 at Nungambakkam railway station for refusing to be friends with her killer. The attacker Ramkumar was infatuated with her and stalked her for months and finally killed her after she rejected him. He committed

amendment is a step in right direction to tackle the issue of cyber stalking, but it is wholly inadequate. It leaves too much burden on the Judiciary to interpret and reinterpret the law to suit the circumstances of each case and Section 354D alone cannot ensure effective justice to the victim. It has to be used along with Section 69A of Information Technology Act or other relevant sections of IPC like 499 and 503 to ensure complete justice to the victim. So in my opinion, cyber stalking law in India has a lot of drawbacks to overcome, to become an efficient piece of legislation.

suicide in Police custody; *See also,* http://www.deccanchronicle.com/nation/crime/150716/saw-swathi-fell-in-love-stalked-her-says-ramkumar.html.