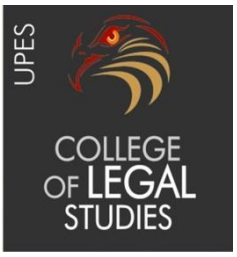
CYBERSTALKING: CRITICAL ANALYSIS OF LEGAL PROVISIONS & STUDY OF ENFORCEMENT

Devika Dua

Submitted under the guidance of: Ms. Preetika Sharma, Assistant Professor at College of Legal Studies, UPES.

This dissertation is submitted in partial fulfillment of the degree of B.A., LL.B. (Hons.)



College of Legal Studies

University of Petroleum and Energy Studies

Dehradun

2017

CERTIFICATE

This is to certify that the research work entitled **"CYBERSTALKING: CRITICAL ANALYSIS OF LEGAL PROVISIONS & EMPIRICAL STUDY OF ENFORCEMENT"** is the work done by Devika Dua under my guidance and supervision for the partial fulfillment of the requirement of B.A., LL.B. (Hons.) degree at College of Legal Studies, University of Petroleum and Energy Studies, Dehradun.

Ms. Preetika Sharma
Assistant Professor
March 15, 2017.

DECLARATION

I declare that the dissertation entitled **"CYBERSTALKING: CRITICAL ANALYSIS OF LEGAL PROVISIONS & EMPIRICAL STUDY OF ENFORCEMENT"** is the outcome of my own work conducted under the supervision of Ms. Preetika Sharma, Assistant Professor at College of Legal Studies, UPES, at College of Legal Studies, University of Petroleum and Energy Studies, Dehradun.

I declare that the dissertation comprises only of my original work and due acknowledgement has been made in the text to all other material used.

Devika Dua
March 15, 2017.

TABLE OF CONTENTS

ABBREVIATIONS

1. App-Application
2. Art.-Article
3. CBI-Crime Branch Investigation
4. C.P.C.-California Penal Code
5. C.P.C., 1908-Code of Civil Procedure
6. CPS-Crown Prosecution Service
7. Corp.-corporation
8. Crl.-criminal
9. Dept.-Department
10. Distt.-District
11. Edn.-Edition
12. E-mail-Electronic mail
13. Etc.-etcetera
14. FBI-Federal Bureau of Investigation
15. FIR-First Information Report
16. GSCASH- Gender Sensitisation Committee Against Sexual Harassment
17. Govt.-Government
18. i.e.-that is
19. IEA-Indian Evidence Act, 1872
20. IJCC-International Journal of Cyber Criminology
21. IP-Internet Protocol
22. IPC-Indian Penal Code, 1860
23. IT-Information Technology
24. ISP-Internet Service Provider
25. LLR-Land Law Reporter
26. L. Rev.- Law Review
27. Ltd.-limited
28. MCC-Michigan Criminal Code
29. N.Y.-New York
30. PC-Personal Computer
31. P.-page
32. PHA-Protection Against Harassment Act

33. r/w-read with
34. s.-Section
35. Ss.-Sections
36. u/A-Under Article
37. UK-United Kingdom
38. u/s-under section
39. US- United States
40. U.S.C.-United States Code
41. Vol.-volume

TABLE OF CASES

ACKNOWLEDGMENT

Completion of this dissertation was possible with the support of several people. There are no proper words to convey my deep gratitude and respect for my thesis and research advisor, Ms. Preetika Sharma, Assistant Professor at College of Legal Studies, UPES. She has inspired me to become an independent researcher and helped me realize the power of critical reasoning. This feat was possible only because of the unconditional support provided by Ma'am. A person with an amicable and positive disposition, she has always made herself available to clarify my doubts despite her busy schedules. Thank you ma'am, for all your help and support.

Some faculty members of the University have been very kind enough to extend their help at various phases of this research, whenever I approached them, and I do hereby acknowledge all of them. I thank them for their valuable suggestions and concise comments on some of the research papers of the thesis. They have extended their support constantly and I thank them for their contributions.

No research is possible without the Library, the centre of learning resources. I take this time to express my gratitude to all the library staff for their services. Last but not the least, My colleagues have all extended their support in a very special way, and I gained a lot from them, through their personal and scholarly interactions and their suggestions at various points of my research programme. Therefore, I thank all of them for their support and constant motivation. This dissertation would not have been possible without each one of the people mentioned above.

1. INTRODUCTION/PREFACE

The offence of cyberstalking is a recent issue which has gathered much attention of the lawmakers as well as the media. All over the globe, the instances of this crime is increasing at a fast pace. However, this crime is one of the most different forms of crime committed over the internet because it targets individuals ranging right from children up to adults.

The reason for the cybercrimes' rate increasing continuously is attributed to the advancements and growth of technology. As the technology is improving day by day, so is the use of the internet as a means to communicate, is increasing. People from all walks of life are making use of the Internet because it is faster, efficient and also cheaper as compared to the other modes of communication. With the invention of the internet, various social platforms have come up wherein one can easily share their personal information[1] and meet new people, thereby increasing their social circle[2]. This is one of the pros of the fast-growing technology. But there are a few negatives as well.

People have started using this same technology for the purpose of satisfying the thirst of their criminal mind. They are using the internet as a means to harass and threaten the people by sending them offensive and harassing pictures, messages etc. on the various social networking sites. These social platforms have in a way, activated the criminal side of an individual, thereby giving rise to crimes such as cyber stalking.[3]

Let us proceed further and discuss about the origin of offline stalking and how with the technological progress, people started taking recourse to stalking over the internet for it is a more suitable and convenient form of stalking. We will see as to how cyber stalking proves to be a safer form of stalking from the point of view of the perpetrator of the offence.

---

[1] M. HAND, MAKING DIGITAL CULTURE: ACCESS, INTERACTIVITY AND AUTHENTICITY (2008).
[2] A. Wittel, *Towards a Network Sociality*, 18(6) THEORY, CULTURE & SOCIETY 51, 72 (2001).
[3] MG Mcgrath and E Casey, *Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace*, 30(1) J. AM. ACADEMY PSCYCHIATRY & L. 81 (2002); ML Ybarra and K Mitchell, *How Risky are Social Networking Sites? A Comparison of Places Online where Youth Secual Solicitation and Harassment Occurs*, 121(2) PEDIATRICS 350 (2008).

Cyberstalking is an issue which requires awareness, universally. The basic objective of this project is to throw light upon Cyberstalking and its related areas.

Firstly, in the Introduction Of Cyberstalking, the very first part discusses about the history of stalking as well as cyberstalking, the second part talks about the various definitions of cyberstalking that have been given by different scholars and the last part ,about how is online stalking different from offline stalking.

Secondly, "cyberspace and challenges it faces", which is a significant matter, has been discussed about, in the second chapter. The chapter outlines the various definitions of the term "Cyberspace" and the various kinds of threats that have invaded this space.

Further, the third chapter explains the legal framework that further involves Laws of India, Laws of US & Laws of UK. The chapter gives a deep insight into the various statutes that can be resorted for the purpose of regulating cyber stalking.

Fourthly, since it is essential to have an understanding of all other legal aspects, the same have been talked about in the fourth chapter, categorized as – Jurisdictional Constitutional, & Evidentiary. The chapter talks about the different loopholes in the laws of India to successfully deal with the instances of online stalking.

The fifth chapter involves an elucidation of the judicial approach that unfolds the Critical analysis of various case laws from the three countries i.e. India, US & UK.

Lastly, the conclusion along with some suggestions has been presented in a lucid manner so as to give a better understanding and analysis of the main topic, to the reader.

STATEMENT OF THE PROBLEM

There does not exist any concrete legislation in India which directly addresses the offence of Cyber Stalking. Firstly, In the Information Technology Act, 2000 certain provisions such as Sections 66E, 67 & 67A maybe resorted to for the purpose of regulating cyber stalking. Sections 67 & 67A are attracted as they talk about punishments for publishing or transmitting obscene material and material containing sexually explicit act, etc. in the electronic form respectively. The stalker, for the purpose of terrorising his victim, might publish or transmit the above for which he may be booked under Sections 67 & 67A of the Act. Section 66E deals with punishment for violation of privacy, therefore it will also be attracted as the stalker intrudes into the privacy of the victim. Previously, Section 66A of the aforementioned Act dealt with the instances of cyber stalking, but now the provision has being declared unconstitutional by the Supreme Court of India in the case of *Shreya Singhal v Union of India*[4] on the ground that it is vaguely worded. Presently, there is no provision in the Act which solely deals with cyber stalking.

As far as the Indian Penal Code, 1860 is concerned, Sections 292A, 354D, 503, 507 & 509 maybe attracted for the purpose of dealing with instances of cyber stalking. Section 292A deals with "Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail". Section 354D, which was inserted post the Delhi gang rape case in 2012 by the Criminal law (Amendment) Act, 2013 deals with the instances of physical stalking. However, sub-clause (2) of clause (1) of section 354D deals with an aspect of cyber stalking. Sections 503 & 507 can also be attracted as they deal with "criminal intimidation" & "criminal intimidation by an anonymous communication" respectively. Section 509 talks about "word, gesture or act intended to insult the modesty of a woman", can be resorted to for regulating instances wherein a woman is being cyber stalked by man.

Most of the provisions contained in the IPC, as abovementioned, are gender biased as they cater only to instances where a woman gets stalked by a man. There is absolutely no mention of situations wherein a man is stalked by a woman. There is also no provision for regulation same sex stalking. What will be the position of law under above circumstances is unknown and not thought of by the legislature.

[4] AIR 2015 SC 1523

Secondly, there is no law for the purpose of regulating evidence in the case of cyber stalking. How will one prove in the court of law that one is being stalked and has fallen prey to online harassment by another individual.

Thirdly, the public at large is highly unaware about Cyber Stalking being a punishable offence. The need of the hour is to spread awareness amongst the people and to formulate stricter laws for regulating it.

Fourthly, Articles 14, 19 & 21 of the Indian Constitution are being violated by the aforementioned provisions. Section 354D for instance is gender biased as it deals with only female victims of stalking and there is no provision in cases wherein a male is victimised which is clearly violative of Article 14. The perpetrators of the offence usually argue that their right to freedom of speech and expression is being infringed whenever a case is brought against them for cyber stalking. Therefore, the above provisions can lead to violation of Article 19 in the sense that the offender may commit an offence under the guise of his fundamental right. The legislators shall explicitly provide for situations where the offender might take the defence of his right guaranteed under Article 19. The victim on the other hand undergoes mental trauma on being cyber stalked which is again violative of Article 21 as it invades an individual's Right to Privacy guaranteed under Article 21.

Concrete legislation is required to deal with the offence of Cyber Stalking because it may lead to heinous crimes such as rape or physical assault under those circumstances where the stalking is accompanied with rape threats and other threats of violence. The stalker may be stalking the victim not only online but also offline which is immensely traumatising for the victim.

IDENTIFICATION OF THE ISSUES

The following research questions will be answered through this thesis:

1. Whether the laws prevalent in India sufficient to deal with the offence of Cyber Stalking?
2. What are the various jurisdictional issues which may arise pertaining to the offence of Cyber Stalking?
3. What are the various measures which may be adopted so as to prevent instances of cyber stalking?
4. What is the status of the actual reporting, prosecution and enforcement of the existing provisions pertaining cyberstalking?

SCOPE OF THE RESEARCH

Cyber Stalking is a relatively newer phenomenon in the Indian context. There is no concrete legislation in India which directly deals with cyber stalking due to which limited literature is available on the subject. India has failed to keep pace with the developed nations like US & UK who have effective laws to deal with the instances of cyber stalking. India on the other hand is facing challenges to enforce a concrete law concerning the offence. The current study shall be limited to the analysis of law relating to the offence of cyber stalking in US, UK and India. The study shall also incorporate case laws revolving around the issue.

RESEARCH METHODOLOGY ADOPTED

This study utilises the doctrinal method of research. As widely accepted, doctrinal research is the type of research which asks what is the law prevalent concerning a particular issue. It involves analysing the legal doctrines and observing as to how the law has evolved over the years.

HYPOTHESIS

The present study shall test the following hypothesis:

The instances of online as well as offline stalking are equally grave offences and cause the same amount of emotional agony to the victim.

PROBABLE OUTCOME

The present study shall seek to propose a special legislation to deal with the cases of cyber stalking in India. Further the study will critically evaluate the existing provisions pertaining to cyber stalking. The paper in the end shall suggest the amendments in order to fill up the gaps and grey areas in the existing provisions. The paper shall also propose ways by which a victim of cyber stalking can prevent from being stalked in the future. Also, it will suggest ways by which a victim can collect evidence for the purpose of proving the guilt of the victim.

1.1 HISTORY OF CYBERSTALKING

"Stalking is the crime that involves following a person against his or her own will that is more or less equivalent to harassment. It was only in the 20th century that, the term, as an offense, came into wide use.

During the past, stalking was described using various other words. For instance, the term erotomonia was used to talk of a person (usually a woman) who was deluded into believing that he or she was loved by a person who was often famed or renowned. Moreover, tendencies such as obsession were regarded as mere relationship issues rather than as crimes or grounds for mental illness[5].

Publicized incidents spoke of celebrity stalking in the early 1990 which involved serious heinous crimes. The myriads of such star stalking cases included the murder of television actress Rebecca Schaeffer by a fan in 1989 and also, in 1993, the stabbing of famous tennis player Monica Seles by her rival player's (Steffi Graf) supporter grabbed much attention.

One deranged John Hickley was also talked about in the early 1980s. He, only for Jodie Foster's attention, attempted shooting President Ronald Reagan. This ultimately led him to be considered as nothing but a maniac and psychopath. He also tried impressing her with love poems and letters. Such incidents involving obsession and maniac like behaviour have been happening in such great numbers that they pose serious threats and potential dangers to lives of various people.

Thereafter, it was only by the early 21st century, that the Distt. of Columbia and fifty US states began considering stalking as a criminal offense. Soon after they criminalized stalking, many countries around the world started adopting such policies.

On one hand , there were countries offering shelter under the then existing harassment laws whereas , on the other hand , there were other countries safeguarding the victims under newly charted out laws against stalking.

After comprehending the instances of stalking in the past, another question that strikes the mind is the psychology of a stalker. What actually is the psychology of a stalker remains a big, rather, significant question residing in the minds of most of the people.

[5] Joel Best, *Stalking*, (Mar, 3, 2017, 7:02PM), https://www.britannica.com/topic/stalking-crime.

How actually is the state of mind of a stalker has been deeply explained by various psychologists. It has been observed that such people suffer from personality disorders and depression in most cases. One of the most noticeable features of stalkers is that they have a tendency of ignoring signals that evidently prove the disinterest of the other person. The basic norms of behaving are mostly violated by stalkers.

The sudden and tempestuous growth of social media has simplified life to a great extent. The ease with which people are able to communicate and share data , crossing all geographical borders and hindrances , not actually , but virtually , has made life easier and simpler.

However there is always another side of a coin which cannot be disregarded. The pros and cons of everything exist and have to be comprehended. Social media has caused a sudden and significant rise in the instances of stalking and the inappropriate and troubling behaviour associated with it.

Through social media, stalkers have found an easier way of reaching the victim in absolutely no time. Social media is a boon when looked from the perspective of communicating with the near and dear ones. Services such as emails, voice messages, media sharing, instant messaging etc. when used to approach, follow, harass, taunt, comment or persecute someone, against his or her will due to obsession for that particular person, it ultimately amounts to stalking through social media, for which the term "Cyber Stalking" has come into use.

Cyber stalking has one very important factor, upon which a stalker mostly relies - It is the condition of being anonymous, so that the identity of the stalker remains unrevealed. Also with the inception of Internet and development of various applications, it has become easy to track locations of a person"[6].

[6] *Id*. at 5.

1.2 DEFINITIONS OF CYBERSTALKING

For the past twenty years the use of technology, as a medium to not only communicate but also to work, study and interact with one another, has increased at an alarming rate. It has become one of the most essential components of businesses as well as our own lives[7]. The use of technology has simplified both our personal as well as our professional lives. With the advent of technology, one can now communicate with people not only from the same city or the same country, but also with people residing in various other areas of the world.

As the world is advancing, the use of technology is continually being improved. People from all sections of the society are being able to use it in the form of mobile phones, computers etc. The process of communication has changed through the time. Anonymous letters always existed, but Internet, with the handy technology, has made everything easier and faster. Internet has become the most attractive form of technology in today's world. It is being used by one and all. In the past, when there was no technology, there existed famous people like artists, wordsmiths, sport personalities, etc. as well as non-famous people. Nowadays, we all are a little famous exposing ourselves to the public eye through the social networking platforms provided as an outcome of technological advancements. Even our way to make friends and open up to strangers has changed and the credit for it goes to social networking. The young people have been influenced the most as they are being provided with a range of platforms to socially connect and interact with each other. This has both positive and negative implications, positive in the sense that they are exposed to a wide variety of opportunities by connecting with people from various parts of the world whereas negative in the sense that people might engage in criminal activities and misconduct by taking undue advantage of the internet, thereby resulting in commission of what are called cybercrimes. The Internet is thus, becoming nothing but a reflection of the real-life. Undoubtedly it is one of the most wonderful tools which has led to the emergence of a new era of the information-age. But at the same time, if misused, it can prove to be terrifying and sometimes even deadly.

[7] Steven D. Hazelwood & Sarah Koon-Magnin, *Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis,*7 IJCC 155, 155-156 (2013).

Criminal offences are increasing as the technology is improving and advancing. The perpetration of crimes in the cyber world has become easier with development in the technology as it has provided new opportunities and possibilities. Advancements made in the computer technology has opened up various opportunities for commission of cybercrimes. These crimes pose a serious threat to the personal as well as the public well-being of an individual. Communications through the internet are now being used for the purpose of harassing, intimidating and instilling feelings of terror etc. to others thereby causing harm to them[8]. This is known as Cyberstalking. Let us first define stalking before we proceed into the various academic and legal definitions of the term cyberstalking. Generally speaking, "*stalking involves repeated harassing or threatening behaviour*"[9]. Today the technological advancements has led to the creation of a new crime known as Cyberstalking.[10] So far, there has not been any universally accepted definition for the offence, "cyberstalking involves the use of the Internet, e-mail, or other means of electronic communication to stalk or harass another individual.[11]" The term is being defined by Bocij, Griffiths and McFarlane as "*a group of behaviours in which an individual, group of individuals or organization, uses information and communications technology to harass one or more individuals. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes and confrontation*". Baer defines the term as "*Cyberstalking in particular is composed of words alone and therefore stands more distinctly as apart as a crime of accumulation*". Brenner has

[8] *Id*. at 7.

[9] U.S. DEPARTMENT OF JUSTICE, STALKING AND DOMESTIC VIOLENCE: REPORT TO CONGRESS 1 (May 2001), available at http://www.ncjrs.org/pdffilesl/ojp/186157.pdf [hereinafter REPORT TO CONGRESS]. Stalking behavior includes, but is not limited to following a person, appearing at a person's home or business, harassing communications and/or messages (e.g., phone calls, letters), or vandalizing property. Id.

[10] Renee L. Servance, Cyberbullying, Cyber-Harassment, and the Conflict Between Schools and the First Amendment, 2003 Wis. L. REV. 1213, 1215 (2003).

[11] PATRICIA TIADEN & NANCY THOENNES, STALKING IN AMERICA: FINDINGS FROM THE NATIONAL VIOLENCE AGAINST WOMEN SURVEY 1 (1998), available at http://www.ncjrs.gov/pdffiles/169592.pdf. "Stalking generally refers to harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. These actions may or may not be accompanied by a credible threat of serious harm, and they may or may not be precursors to an assault or murder. Id. With cyber-harassment, the purpose remains the same: to cause distress to the targeted individual and to derive power from that distress".

construed the term as "*in a sense, cyber stalking and cyber harassment are lineal descendants of the obscene or annoying telephone call offenses that were created roughly a century ago, to address harms resulting from the misuse of a nineteenth century technology*". Ellison and Akdeniz have defined the term as "*online harassment, which may include various digitally harassing behaviours, including sending junk mails, computer viruses, impersonating the victim, etc.*"

It is noteworthy that the term 'Cyberstalking' was being identified as an offence in the early 1990s. Michigan criminalised online stalking in the year 1993 through the MCC.[12] In the UK, there is still no provision that legally defines the term 'cyberstalking'.[13] Presently, for the purpose of regulating instances of both offline and online stalking, provisions of the Protection from Harassment Act, 1987[14] (PHA) such as Ss. 2-7 are being resorted to. An exhaustive definition for the term has been formulated by the Crown Prosecution Service (CPS) keeping in mind S2A (3) of the Act.

It is clearly implied from the aforementioned definitions that Cyberstalking is an offence wherein an individual is being harassed 'digitally' thereby curtailing his 'privacy'. Most of the legal definitions of the term have been derived from provisions revolving around the concept of offline stalking. In India the term was recognised in 2010 when Halder and Jaishankar defined it as "*In one word, when 'following' is added by mens rea to commit harm and it is successfully digitally carried out, we can say cyber stalking has happened*."

Therefore, in common parlance the term cyber stalking maybe understood as stalking of an individual by another individual over the internet. It is just like the instances of stalking in the real world with the only difference that cyber stalking occurs over the internet. With the advent of electronic media, instances of stalking in the cyberspace have arisen on an alarming rate. Although anybody may fall prey to the

---

[12] Michigan Criminal Code, Stalking: Section 28.643(8), definitions. 1993 section 411h, (Mar, 4, 2017, 11:00 AM), www.haltabuse.org/resources/laws/michigan.shtm.

" Later, the Federal law also developed anti-cyber stalking law through "Violence Against Women and Department of Justice Reauthorization Act, 2005", which amended Section 2261A (2) of Title 18, USC through Section 114, which specifically deals with stalking including cyber stalking".

[13] Crown Prosecution Service, (Mar, 4, 2017, 12:30 PM), www.cps.gov.uk/ legal/s_to_u/stalking_and_harassment/.

[14] Protection from Harassment Act, 1987, (Mar, 4, 2017, 12:30 PM), www. legislation.gov.uk/ukpga/1997/40/contents.

abovementioned crime, statistics reveal that females are more susceptible to it as compared to males. Even children are not spared and are being victimised by adults or paedophiles. Those individuals who are not well versed with the usages of the internet are mostly attacked. These attackers, or more appropriately these stalkers, stalk the victims on account of several reasons which is why these stalkers maybe classified into several heads, although this does not necessarily imply that every stalker would neatly fit into these heads. They are people who come from all walks of life. Therefore, virtually, everyone and anyone has the ability of becoming a stalker. But there still is some degree of commonalty in their characteristics. "Thus, they may be categorised as under:

1. **Rejected Stalker**

   These are those kinds of stalkers who begin to stalk when their romantic relationship or a very close friendship comes to an end or is on the verge of coming to an end. The stalker either wants to get back with the victim or he seeks revenge on him/her. They have a personality which is being characterised by narcissism and jealousy. These stalkers are almost resistant to the activities launched against them so as to end their behaviour.

2. **Resentful Stalker**

   These are those kinds of stalkers who try to scare the victim and usually stalk him/her with the sole aim to seek revenge on a third person who has annoyed them. They are people who are often 'irrationally paranoid' and harass those people, whom they believe have wronged them or those, whom they think represent the group who had wronged them in the past. They may also stalk a complete stranger as well. They actually feel that it is they who are the victims and it is right for them to seek revenge by stalking the ones who have humiliated them. These are the most obsessive kind of stalkers who may verbally threaten their victim but would never physically assault him/her. These stalkers maybe prevented from continuing the stalking by confronting them as soon as possible thereby imposing legal sanctions.

3. **Predatory Stalker**

These are those kinds of stalkers who stalk the victim as a part of their plan to later on attack him/her sexually. They are often motivated by the idea of 'sexual gratification' and their control and authority over the victim. For the aforementioned purpose, these stalkers may either stalk someone they know or a total stranger. They do not usually harass their victim while they are stalking them, but engage in activities like fetishism, voyeurism, obscene phone calls to the victim, exhibitionism etc. These stalkers have the potential of becoming physically violent with their victim. Also, they stalk for a shorter span of time when compared with the other kinds of stalkers.

4. **Intimacy Seeker**

These are those kinds of stalkers who stalk the victim with the purpose of developing a romantic relationship with him/her. They usually feel that the victim is also in love with them and are equally willing to get involved in an intimate loving relationship with them. They are basically delusional and feel that the victim is the only ideal partner for them and that only he/she is capable of fulfilling all their desires. Any kind of responses from the victim be it negative or positive, are being interpreted as positive thereby encouraging them to continue with t stalking. They feel that since they have invested plenty of their time in stalking the victim, the victim now in turn owes them all the love and affection. These types of stalkers strongly believe what they want to and can never really mend their ways. They either stalk people whom they are acquainted with or at times even people who are complete strangers. These stalkers have the tendency of becoming violent and threatening if the victim does not reciprocate the way they expect them to. They may even turn jealous on seeing the victim getting involved in a romantic relationship with someone other than them. They are one of the most persistent type of stalkers who are not scared of legal sanctions for they feel them to be hurdles which need to be overcome so as to exhibit their love for the victim.

5. **Incompetent Suitor**

   These are those kinds of stalkers who have poor social skills and try to engage in a romantic relationship with the victim by stalking them. They engage in activities like calling the victim continuously over his/her phone or asking the victim to go out with them despite they have been rejected and turned down several times. These stalkers are likely to stop the stalking as soon as they are exposed to legal sanction only after being properly counselled.

6. **Erotomania and Morbidly Infatuated**

   These are those kinds of stalkers who believe that the victim loves them in spite of the fact that the victim has neither behaved nor stated anything that would suggest that they love the stalker. They keep interpreting the statements of the victim in such a way as would support their belief that the victim is genuinely in love with them. These stalkers give immense importance to their imagined romantic relationship with the victim. They suffer from what is known as acute paranoia and/or delusions. They usually stalk those people who belong to a socially higher class as compared to their own. These stalkers continuously try to communicate with the victim. These stalkers require psychological treatment. They are not scared of legal sanctions and also spent short periods behind the bars. Sometimes they are highly responsive to the treatment and their condition is improved"[15].

Above mentioned are the several categories of stalkers which are same for the cases of online as well as offline stalking. Let us now discuss the similarities and differences between the two types of stalking.

[15] *Sexual Assault Prevention And Awareness Center*, (Mar, 4, 2017, 11:00 AM), https://sapac.umich.edu/article/320.

1.3 SIMILARITIES AND DIFFERENCES: ONLINE AND OFFLINE STALKING

The internet is a very young technology which makes cyberstalking as the most recent form of offences. On the other hand instances of physical or offline stalking are also a relatively newer form of crime. The aim of the stalker is to exercise full control over the victim so as to inculcate feelings of fear, terror and intimidation in him/her. This behaviour of the stalker may sometime give rise to physical action being taken by him against his victim. Many believe that online stalking is synonymous with offline stalking as their content and intent is almost the same[16].

Undoubtedly, there are very many similar attributes of the two kinds of stalking like there is a desperate urge in the stalker to exercise power and control over the victim[17]. Another similarity lies in the fact that just like in cases of offline stalking, the stalker tries to terrorise, intimidate and scare the victim, the same approach is being adopted by the stalker in cases of online stalking where his main is to repeatedly harass and threaten the victim which may sometime result in a more serious behaviour[18]. Although there are similarities between the two offences, still the number of differences between the two outweighs these similarities so much so, that the existing statutes on offline stalking will prove to be insufficient in regulating the instances of online stalking. It is very important to carefully analyse the differences between them, and then steps shall be taken by the legislators to formulate a full-fledged statute purely dealing with the instances of online stalking outlining the punishments for the perpetrators and remedies available to the survivor of the stalking.

The various differences between the two forms of stalking are, *Firstly*, the cyberstalkers may instantly use the Internet with the intention of stalking , following or harassing their victim and disseminating information. They are at an advantage when stalking over the internet when compared to physical stalking because the internet has no geographical limitations. This enables the stalkers to maintain complete anonymity and instantly disseminate the message so as to terrorise the

[16] Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 Mo. L. Rev. 125 (2007).

[17] Harry Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, STAN. TECHNICAL L. Rev. 2, 54 (2004).

[18] *Id.* at 16.

victim. The stalkers have got a number of options and ways to harass their victim. In the cyber world, there are so many modes by which the stalkers may communicate the intimidating and threatening messages to their victim. The various modes include e-mails, instant messaging, anonymous electronic bulletin boards, chat rooms and various other online communication devices. The internet has made it possible to disseminate information to a large number of people at the same time so as to threaten and harass them which is obviously impossible in the case of physical stalking. The message can easily be distributed to a public forum in a faster and an efficient manner through the internet. Also, it is one of the most inexpensive ways to share information.

For instance, in case of offline stalking, the stalker, in order to repeatedly harass the victim, will engage in continuously contacting the victim on his telephone, which would consume a lot of his time and energy for every single time he is required to act for making the phone call, whereas in cases of online stalking the stalker saves on a lot of time and energy as he can successfully harass and terrorise the victim by sending him a threatening e-mail, and make his computer to systematically and continuously send the message to the victim over and over again. This may be termed as an "*e-mail bomb*[19]". All this has been made possible only because of advancements made in the technology and the people using this technology in the commission of crimes.

Furthermore, the cyberstalkers can create a website and use it for the sole purpose of posing threatening and harassing comments for the world at large. This again results in the breach of privacy of an individual which is another aspect of cyberstalking[20].

Secondly, in the cases of cyberstalking the perpetrator may not necessarily be physically present around the victim so as to threaten and harass him. In the cases of physical stalking, the crime can only be committed only if the stalker is physically close to the victim[21]. The internet is large and unending as the human psyche. Due to lack of geographical constraints, the stalker may harass the victim sitting miles away

[19] PAUL BOCIJ, CYBERSTALKING: HARASSMENT IN THE INTERNET AGE AND HOW TO PROTECT YOUR FAMILY 11 (2004).

[20] J.A. HITCHCOCK, NET CRIMES AND MISDEMEANORS: OUTMANEUVERING THE SPAMMERS, SWINDLERS, AND STALKERS WHO ARE TARGETING YOU ONLINE 11 (Loraine Page ed., 2002).

[21] VALETK, s*upra* note 16.

from him in an altogether different country. This unrestricted reach of the web makes offline stalking different from online stalking. This can further be expanded in three different ways. First, the stalker may harass the victim in the most inexpensive and efficient way in spite of being miles away from the victim. The stalker may continue stalking the victim sitting in some other city or another country as long as he has access to the internet. The internet is a cheaper as well as an instantaneous mode to communicate as compared to telephone or letter. Second, the stalker can maintain his anonymity which again intimidates the victim for he keeps wondering about the whereabouts of the stalker. The victim is scared for he is clueless whether his stalker is someone in close proximity of the victim or whether he is someone from a neighbouring state[22]. Finally, there may arise a lot of jurisdictional issues in the instances of cyberstalking as the victim and the stalker may belong to two different countries altogether making the enforcement of laws a tedious job especially from the side of the victim for he has to collect evidence from a different jurisdiction so as to prove the stalker guilty[23].

Thirdly, the stalkers in case of online stalking can maintain their anonymity and can still be able to harass their victim[24]. It is usually believed that online stalking is less

---

[22] Louise Ellison, *Cyberstalking: Tackling Harassment on the Internet,* (David S. Wall ed., 2001).

[23] "Some state and local law enforcement agencies also have been frustrated by jurisdictional limitations. In many instances, the cyberstalker may be located in a different city or state than the victim making it more difficult (and, in some cases, all but impossible) for the local authority to investigate the incident. Even if a law enforcement agency is willing to pursue a case across state lines, it may be difficult to obtain assistance from out-of state agencies when the conduct is limited to harassing e-mail messages and no actual violence has occurred. A number of matters have been referred to the FBI and/or U.S. Attorney's offices because the victim and suspect were located in different states and the local agency was not able to pursue the investigation".

U.S. Dept. of Justice, *A Report on Cyberstalking: A new challenge for law enforcement and industry (Aug. 1999),* Available at: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm; Accessed 3/3/17.

[24] "The issue of whether anonymity should be regulated on the Internet is a current debate". *See, e.g.,* George F. du Pont, *The Criminalization of True Anonymity in Cyberspace,* 7 MICH. TELECOMM. & TECH. L. REv. 191, 196-216 (2000-2001).
" Du Pont's analysis distinguishes between "true anonymity," which is untraceable, and"pseudo-anonymity," which, although indirectly, is inherently traceable. *Id.* at 196. He cites a historical precedent for pseudo-anonymity, and realizes its social good for anonymous public debate *(i.e.*, the American Revolutionary period, The Federalist Papers, modem political campaigns, etc.)". *Id.* Where the courts and history have recognized a free speech value to anonymity, it has almost always meant pseudo-anonymity. *Id.* But true anonymity is prone to abuse and danger. Cyberspace has greatly increased the ease with which true anonymity can be attained. Du Pont's proposal is to criminalize all

dangerous when compared with offline stalking because in the cases of online stalking, the victim does not have to physically face his stalker[25]. But this in fact, is not true. The cyberspace has enabled those people to commit the crime of cyberstalking who had always been potential stalkers, but were hesitant to face and harass their victim in person. Internet, in a way, has helped these stalkers to overcome their hesitation by giving them an opportunity of committing the offence online[26]. The environment of the cyberspace is such that it only persuades the stalker to keep doing what he has been doing without any fear of being caught[27].

According to one of the scholars, the stalker is "at an advantage" due to the "veil of anonymity" on the internet[28]. Due to this veil, it becomes almost impossible to track the location of the stalker. Consequently, he can neither be located nor can he be arrested. There are certain marks which can be used to trace and identify the apt location and identity of the stalker. But unfortunately, the stalkers have the technology to remove those marks, thus saving themselves from being exposed.

Fourthly, it is very easy for cyberstalkers to impersonate the victim and use his identity for the purpose of harassing and threatening people over the internet. This is achieved by posting threatening statements and comments on electronic bulletin boards and chat rooms. The stalker also sends inflammatory e-mails from the victim's mailbox to the mailbox of different people. The people get intimidated by the content posted by the stalker due to which the victim has to suffer as he is banned from the various social networking platforms for the stalker had been misusing his identity. This is not the case in offline stalking as the stalker does not impersonate the victim so as to intimidate or terrorise a third person.

---

non-privileged, truly anonymous communication in cyberspace and mandate that all anonymous communication in cyberspace be merely pseudo-anonymous".

[25] Neal Kumar Katyal, *Criminal Law in Cyberspace*, U. PA. L. Rev. 1003 (2001).

[26] Bocij, *supra* note 18.

[27] U.S. Dept. of Justice, *Stalking and Domestic Violence:Report to Congress* 1 (May 2001), Available at http://www.ncjrs.org/pdffilesl/ojp/186157.pdf.
"Stalking behavior includes, but is not limited to following a person, appearing at a person's home or business, harassing communications and/or messages *(e.g.*, phone calls, letters), or vandalizing property".

[28] Amy C. Radosevich, Note, *Thwarting the Stalker: Are Anti-Stalking Measures Keeping Pace with Today's Stalkers?*, U. ILL. L. Rev. 1371, 1387 (2000).

Fifthly, in the case of online stalking, the stalkers may persuade "innocent" people to stalk on their behalf. This is possibly one of the most frightening outcomes of this form of stalking. For example, the stalkers fulfil the above motive by sending hate e-mails in the name of the victim to the various "Satanists, drug users and pornographers"[29]. The e-mail sometimes also contains the telephone number as well as the house address of the victim. Consequently, the victim, unknowingly, starts to receive harassing phone calls and hate mails from these Satanists and drug users.

All these things are not possible in the case of offline stalking.

It can thus be concluded that, internet has made the frightening consequences of offline stalking even more serious and grave. It is the internet which has given so many advantages to a cyberstalker as compared to a stalker in the case of offline stalking. The cyberstalker can engage in identity theft, maintain complete anonymity, can stalk people or even the public at large for the purpose of harassing or terrorising them. Stalking online is very convenient in the sense that the cyberstalker can continue to harass and intimidate the victim for a continuous period of twenty four hours provided he has proper access to the internet. Also, it is one of the fastest, easiest, inexpensive and most efficient way to stalk a person online as compared to in person i.e. in cases of offline stalking, as a lot of time and energy is consumed for the stalker has to get into some real action for the purpose of harassing his/her victim. The need of the hour is that there shall be better and proper laws enacted so as the fill in the gaps and regulate the criminal activities in cyberspace which is increasing at an alarming pace. Therefore, there shall be better and effective laws so as to deal with instances of online stalking in a better fashion[30].

[29] N.Y. State Assembly. (N.Y. 2006), Available at http://assembly.state.ny.us/leg/?bn=A06016.

[30] Radosevich, *supra* note 27, at 1389. ("Until broader language is implemented to cover the use of new information technologies and methodologies in [cyber]stalking cases, victims may have to search for alternative solutions."). "Some of those solutions include: utilizing more computer specialists on law enforcement task forces; combating technology with technology by providing computerized response systems for victims; launching public awareness campaigns and educational Websites so that victims are informed of their options and rights; and getting Internet Service Providers involved in the regulation process".

2. CYBERSPACE AND ITS CHALLENGES

The term 'Cyberspace' neither has any universally accepted definition nor does it have any geographical restraints[31]. From the beginning of the human history and tracing back to about a hundred years, humans had only a few modes of communication available in the physical domain which required technology to function. Those physical domains comprised of the land, sea, aerospace and the outer space. All of these developed gradually through the years and each one comprised of different physical characteristics. For the purpose of successfully exploiting these four domains, technology played a major role. For instance, the land was used as a means of communication by the use of technology in the form of wheels, chariots etc. while the sea was used by man for the purpose of communicating through ships, submarines etc. which again was made possible by the use of technology. On the other hand, the aerospace was introduced "to the mix"[32] which had huge economic, social and political implications for the purpose of travelling through air and transportation of goods in the 21st century. Then the fourth domain, in the form of outer space, was introduced in the year 1957. A completely new domain has been added to the above described four domains which is the "Cyberspace".

Literally speaking the term "Cyberspace" is composed of two words: 'Cyber' which means "automation, artificial control, and computerisation"[33] whereas on the other hand 'Space' connotes "a multidimensional place, most often used in relation with electronic spaces created by computer-based media"[34]. The term was first being defined by the science fiction author, William Gibson as "*a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted*

---

[31] *Cyber Security and Related Issues: Comprehensive Coverage,* (Mar, 4, 2017, 20:08 PM), http://www.insightsonindia.com/2014/11/25/cyber-security-related-issues-comprehensive-coverage/

[32] "While some in the U.S. Air Force have argued that the aerospace is a seamless environment that extends from the Earth's surface to infinity, the fact is that the air and outer space are subject to not only differing legal regimes—overflying a nation's sovereign airspace could be a violation of international law, while orbiting the Earth in space is not—but physical ones as well. Movement in the air is governed by lift, while in space, the laws of orbital mechanics rule. Thus, air and space are two very different domains".

[33] 'Cyber-' has actually become the prefix of the 1990s: cyberspace, cyberdeck, cyberpunk, cybernaut, cyberart, cybergames, cybersex, cybertalk, cyberbody, cyberworld, …

[34] Other non-electronic 'spaces' are able to emerge when, for instance, people read books, listen to radio, etc.

from banks of every computer in the human system. Unthinkable complexity."[35] The definition given by Gibson is of great importance for it reveals the possibilities of having a huge cyberspace experience.[36] Author Winn Schwartau has defined the term as "*That intangible place between computers where information momentarily exists on its route from one end of the global network to the other. . . . the ethereal reality, an infinity of electrons speeding down copper or glass fibers at the speed of light. . . . Cyberspace is borderless . . . [but also] think of cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world."*[37] He again defined the term as "*[National] cyberspace are distinct entities, with clearly defined electronic borders. . . . Small-C cyberspaces consist of personal, corporate or organizational spaces. . . . Big-C cyberspace is the National Information Infrastructure. . . . add [both] and then tie it all up with threads of connectivity and you have all of cyberspace*"[38]. According to author Walter Gary Sharp, cyberspace maybe defined as *"The environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web"*[39].It has been defined in the early 2000s by the Department of Defense Dictionary of Military and Associated Terms as "*the notional environment in which digitized information is communicated over computer networks.*"[40] Unfortunately, the definition was considered to be incomplete for it lacked several key components. The term was being defined by Gregory Rattray as *"A physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place. . . . Cyberspace is a man-made environment for the creation, transmittal, and use of information in a variety of formats. . . . Cyberspace consists of electronically powered hardware, networks, operating systems and transmission standards"*[41]. The various other definitions for the term are "*The on-*

[35] William Gibson, Neuromancer (1984)
[36] Cyberspace: Definition and Implications, Rain Ottis, Peeter Lorents Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
[37] Information Warfare: Chaos on the Electronic Superhighway (1994)
[38] Information Warfare: Chaos on the Electronic Superhighway (2d ed., 1996)
[39] CyberSpace and the Use of Force (1999)
[40] Joint Publication 1–02, DOD Dictionary of Military and Related Terms (Washington, DC: The Joint Staff, dated April 12, 2001, and amended through November 9, 2006), www.dtic.mil/doctrine/jel/new_pubs/jpl_02.pdf.
[41] Gregory Rattray, *Strategic Warfare in Cyberspace*, (2001).

line world of computer networks"[42]. *"A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures.*[43]*"* *"The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries"*[44]*. "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*[45]*"* Over the years, several definitions for the term have been given by various authors, but so far, no universal consensus has reached on what shall be the most suitable definition. Since cyberspace does not have any physical existence, and is nothing but a mirror image of the real world, it may also be known as "virtual space".[46] Therefore, Gibson rightly states Cyberspace as *"the total interconnectedness of human beings through computers and telecommunication without regard to physical geography."*

The Cyberspace is a reflection of the real world, hence, it has both kinds of implications: positive as well as negative. The positive aspect is that individuals can communicate with each other in an easier and a faster manner while the negative aspect is that just like crimes are committed in the real world, the cyberspace also comprises of criminals who use it as a tool for criminal applications and misconduct. Therefore the cyberspace has several challenges that it needs to overcome so as to ensure cyber security. David Whittle has pointed out several disadvantages of using cyberspace for commercial purposes. The disadvantages maybe laid as follows:

1. **<u>DIFFICULT ACCESS</u>** - Sometimes users land up into user interfaces which are not only very complicated but also over designed. This is mostly characterised by links as well as texts in abundance that require quick attention. Although, the design that is exactly opposite cannot be considered user friendly.

[42] Merriam-Webster Third New International Dictionary (2002)
[43] National Military Strategy for Cyberspace Operations (2006)
[44] National Security Presidential Directive 54 (2008)
[45] • Deputy Secretary of Defense Gordon England (2008)
[46] Supra n.9

2. **BANDWIDTH CONSTRAINTS**- Bandwidth is the capacity or amount of data that can be transmitted by any medium. The ordinary users of modem still do not use the latest technologies such as fibre optic wires. They are still confined to coaxial cables and twisted pairs even in the coming years.

3. **WIDE GAP IN THE QUALITY AND APPLICABILITY OF INFORMATION**- The abundance in which the same kind of information is present is quite shocking. In order to meet the needs of the people, grave efforts are being made to make techniques such as searching, filtering etc., come into use. For example, some actions should be made possible such as analysing news service, searching, negotiating and ascertaining the cheapest as well as the most economical air travel, eliminating junk emails etc.

4. **LACK OF REAL SECURITY-** The lack of privacy or security issue has been resolved by a very technical and practical solution. The *"pretty good privacy"* is used for this issue. This is based on the concepts of encryption and decryption. Encryption refers to the translation of data/message, by the sender, into a code which can be decoded or decrypted by the receiver only. The encrypts the message with the public key (unique) which the receiver can only decrypt with the help of a private key (secret).

Data is being transferred from one computer to another as per the binary number system which utilises Zeros and Ones. The information transferred does not carry any other data for the purpose of authentication. In order to send authentication information along with the data transfer, an entirely new transaction needs to be made in the cyberspace. This transaction is executed so as to identify the source from where the data has been sent and make sure that the source is an authenticated one.

Whenever additional information regarding authentication of data sent is being sent along with the data to be transferred, the communication is one which is digitised. Therefore, this increases the chances of identity of the sender being stolen by the stalker. This is a very serious issue. There shall be a proper mechanism in place which

enables individuals to verify their identity to others in a safe manner without exhibiting their digital representation.

"As the cyberspace is unlimited, it is vulnerable to a large number of security threats. These threats eventually assist in giving rise to a large number of cybercrimes. Cybercrimes can be categorized into myriads of crimes involving hacking, phishing, child pornography, hate crimes, internet fraud etc. They have been discussed hereunder –

1. **HACKING:** The term hacking can be simply referred to illegally intruding into a network or a computer system. It can also be understood as gaining an unauthorized access over a computer system. Any expert who breaks into computer systems to gain such access is known as a hacker. Every hacker uses bugs , exploits and such other readymade programs to attack the data targeted.

2. **CHILD PORNOGRAPHY:** The atrocious acts of sexual abuse of children through the internet aren't uncommon. As more and more computers and internet connections have come within the reach of children, the graph of child pornography has gone way above our imagination. This has increased the chances of more and more children falling prey to the brutes sexually attracted to children (Paedophiles). These Paedophiles sometimes dupe the children into believing that they are of the same age group. This makes them successfully win their confidence and trust. All this mostly happens through chat rooms where the children are sexually exploited. Sometimes they also try toexploit children by sharing pornographic stuff with them in order to satisfy their own aggressive needs.
3. **CYBER STALKING:** The term suggests harassment though the internet by following, threatening, persecuting, annoying and going against the will of a person. The term has been derived from the word stalking only after the explosive growth of the internet in a few years.

4. **DENIAL OF SERVICE:** This is the term used to describe a situation where a user is prevented access to his or her network / internet and the services

provided therefrom, usually with a malicious intent. This is done by blocking or flooding the targeted users network with traffic in order to make the service inaccessible to the victim.

5. **DISSEMINATION OF MALICIOUS SOFTWARE (MALWARE):** The term Malware can be more appropriately understood by breaking it into two words – "Malicious" and "Software''. The software with a malicious intent is known as Malware. Malware can be classified as follows :

    a. **VIRUS**: A program in the computer that runs against our wish, modifies other programs. A computer virus is man-made. The basic characteristic of computer virus is that it replicates itself. It makes copies of itself repeatedly which in turn leads to much more usage of the memory. This causes the system to come to a halt. A virus can easily spread or transmit itself across a number of networks, completely destroying the data files in the system. However, nowadays many antivirus softwares have come into use that scan and check the system for any viruses For example Quick Heal, McAfee etc.
    b. **WORMS**: There is similarity between Worms and Viruses of replicating themselves. However there is difference between the two. Virus needs a human or a host program to propagate it whereas worms just need standalone software. The terms worms viruses and Trojans cannot be used interchangeably as some blurred boundaries exist between the three despite the fact that all three are malicious programs causing damage to the network or system.
    c. **TROJAN**: Trojan differs from viruses in the sense that is does not replicate itself but destroys the system by allowing the hacker to have access to the system through a back door. What it basically does is , disrupts the security of the system so that a hacker may gain unauthorized access to the system of the victim (Also known as Trojan Horse which is related to the wooden horse constructed by Greeks during the Trojan War)

d. **HOAX:** An email that acts as a warning signal against certain program on a computer, claiming it to be destructive, when it is actually not, is known as hoax. Thereafter the email instructs starting off a particular download procedure which only permanently deletes an important file in the system.

e. **SPYWARE:** Spyware can be understood as 'monitoring without consent'. As the name clearly suggests it spies into a system without any prior consent and monitors the activities. They are usually forwarded through emails.

6. **PHISHING:** Disguising as a real and authentic appearing user , phishing is used for satisfying the malicious intent of obtaining passwords , credit card information , usernames etc.

7. DATA RELATED: The three kinds of data related threats are as under:

a. **DATA INTERCEPTION**: With the intention of gathering sensitive information from data streams, hackers often monitor the data stream. The hackers may then hijack, alter or read the data packets by intercepting the network traffic session.

b. **DATA DIDDLING:** Data diddling usually takes place in tandem with data interception. It basically refers to the unauthorized altering of data before it reaches the intended recipient. Succinctly it refers to wrong data entry so that the erroneous data is entered into the system.

c. **DATA THEFT**: As a result of data interception, what commonly takes place is referred to as data theft. It means stealing information without prior permission or authorization. The most common intention lurking behind such data thefts is only to obtain confidential information.

8. **NETWORK RELATED:** The two kinds of network related threats are as under:

a. **NETWORK INTERFERENCE:** Temporary disruption or disturbance in a computer network is commonly referred to as Network Interference. This usually leads to delay in transmission of data. Common examples of network interference can be smurf attacks, Denial Of Service attacks etc.

b. **DATA SECURITY NETWORK SABOTAGE:** It simply means deletion of important files and records from the computer network, thus leaving it permanently damaged. The main intention is to disable computers deliberately"[47].

There are several other new types of crimes that have invaded the cyberspace today. For instance Cyber Terrorism. The word cyber terrorism comes from the two words 'Cyberspace' and 'terrorism'. The two words when converged form the term Cyber Terrorism. Threats of attacks/unlawful attacks with the intention of causing fear and disruption is known as Cyber Terrorism[48]. These attacks are mostly against computers, networks and the information stored within them in order to further social or political objectives. To sum up, terrorism through electronic media is what is termed as Cyber Terrorism that intends to spread fear among the people.

An important characteristic of Cyber Terrorism is that it results in damage to life and property, and if not actual damage, at least creates fear and trepidation. When critical infrastructures face serious attacks, when there are deaths, plane crashes, economic losses etc., such attacks come under the definition of Cyber Terrorism.

Intimidating or frightening the government and the general population of people also comes under Cyber Terrorism. This takes place through using computer network tools that in turn shut down the government operations.

---

[47] *Cyber Security and Related Issues: Comprehensive Coverage*, (Mar, 4, 2017, 20:08 PM), http://www.insightsonindia.com/2014/11/25/cyber-security-related-issues-comprehensive-coverage/

[48] *Id*, at 46.

Poor security networks are often vulnerable to such attacks by hostile groups who intend to disrupt critical functions.

3. LEGISLATIVE APPROACH

This chapter describes the legal framework of the three countries i.e. India, U.S. & U.K. with respect to the offence of cyber stalking.

3.1 POSITION IN INDIA

There does not exist any concrete legislation in India which directly addresses the offence of Cyber Stalking. Therefore, there do exist a few legislations which can be resorted to deal with offence indirectly. Let us deal with the various provisions that can be used for the purpose of dealing with the instances of online stalking.

Firstly, In the Information Technology Act, 2000 certain provisions such as Sections 43, 66, 66E, 67, 67A, 67B & 72 maybe resorted to for the purpose of regulating cyber stalking. These provisions may be reproduced as under:

1. S. 66E- *"Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both….*[49]*"*

This provision deals with punishment for violation of privacy of an individual; therefore it will be attracted as the stalker intrudes into the privacy of the victim so as to harass him or intimidate him which is one of the major aim of the stalker in the cases of (cyber)stalking.

2. S.67- "*Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and*

[49] Information Technology Act, 2000, Section 66E.

in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees[50]*".*

3. S. 67A- "*Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.*[51]*"*

The aforementioned provisions, i.e. 67 & 67A will be attracted for regulating instances of online stalking because they talk about punishments for publishing or transmitting obscene material and material containing sexually explicit act, etc. in the electronic form respectively. The stalker, for the purpose of terrorising his victim, might publish or transmit the above for which he may be booked under Sections 67 & 67A of the Act.

4. S.67B- *"Whoever,-*

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

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

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

[50] Information Technology Act, 2000, Section 67.
[51] Information Technology Act, 2000, Section 67A.

d) facilitates abusing children online or

e) *records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees…*[52]*"*

The above section is a newly inserted provision in the IT Act, 2000. It was inserted through the IT Amendment Act, 2008. It may be resorted to in cases where the privacy of children aged below 18 years of age is being targeted by stalkers. The section stipulates an enhanced form of punishment for those criminals who harass children.

Sections 43 and 66, which were amended by the IT Amendment Act, 2008, and deal with aspects of data protection and hacking respectively, will also act as regulatory provisions to deal with instances of online stalking.

Previously, Section 66A of the aforementioned Act dealt with the instances of cyber stalking, but now the provision has been declared unconstitutional by the Supreme Court of India in the case of "*Shreya Singhal v Union of India"*[53] on the ground that it is vaguely worded. Although the section was considered to be an effective provision for the purpose of regulating instances of online stalking for it dealt with "*punishment for sending offensive messages through communication service* etc."
The section was worded as under:

5. S.66A-"*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,

[52] Information Technology (Amendment) Act, 2008, Section 67B.
[53] Shreya Singhal v. Union of India, AIR 2015 SC 1523.

enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.[54] *"*

Presently, there is no provision in the Act which solely deals with cyber stalking.

Secondly, As far as the Indian Penal Code, 1860 is concerned, Sections 292, 354C, 354D, 503,507 & 509 maybe attracted for the purpose of dealing with instances of cyber stalking. The provisions may be stated as under:

1. S.292- *"...shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt person, who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it…..*[55] *"*

The above provision can be used for dealing with the offence of cyberstalking because it deals with one of its aspect i.e. hacking. The section defines the term "obscene" and will be resorted to under those circumstances where the stalker hacks into the online social networking accounts of the victim and uploads obscene material in the form of images etc. or repeatedly sends the victim obscene material so as to harass or intimidate him. This section r/w S.67 of IT Act, 2000 can be used for the purpose of regulating hacking.

2. S.354C deals with "Voyeurism". It is worded as under:

"Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or

[54] Information Technology Act 2000, Section 66A.
[55] Indian Penal Code, 1860 Section 292.

disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine….[56]*"*

3. S.354D deals with "Stalking". It is worded as under:

"(1) Any man who—

- *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*
- *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—

- *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; or*
- *it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or*
- *in the particular circumstances such conduct was reasonable and justified.*

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction,

[56] Indian Penal Code 1860, Section 354C.

with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.[57]*"*

The abovementioned provisions, i.e. 354C & 354D, were inserted post the Delhi gang rape case in 2012 by the Cr. law (Amendment) Act, 2013. They deal with the instances of voyeurism and stalking respectively and the corresponding punishments for the two offences have also been defined in the sections. Section 354C deals with those instances where a woman's sexual privacy is being invaded by a man whereas sub-clause (2) of clause (1) of section 354D deals with an aspect of cyber stalking. This section will be attracted because the content and intent of online and offline stalking is almost the same. Therefore, this section defines the punishment in the cases of physical stalking and also brings out those circumstances under which a person will not be liable for the offence of stalking. The section suffers from numerous shortcomings which will be discussed in the coming chapters in detail. Both, Section 354C and Section 66E of the IT Act, 2000 deal with 'Voyeurism' and are used as regulatory provisions to prevent the offence and punish the perpetrators with the only difference that s.354C is gender biased for it only provides protection to women whereas s.66E is generic in the sense that it is applicable to both men and women.

4. S.503- *"Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation…*[58]*"*

The above provision is attracted in cases of online stalking because intimidating the victim is one of the major aspects of cyberstalking. Therefore, this section defined the term 'criminal intimidation'.

[57] Indian Penal Code 1860, Section 354D.
[58] Indian Penal Code, 1860, Section 503.

5. S.507- "*Whoever commits the offence of criminal intimidation by an anonymous communication, or having taken precaution to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment provided for the offence by the last preceding section*[59]*."*

The above provision is attracted in cases of cyberstalking because it defines the punishment for those circumstances where a person uses an anonymous communication for the purpose of intimidating another person thereby committing an offence. Anonymity along with intimidation are major attributes of online stalking.

6. S.509- "*Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.*[60]*"*

The above provision deals with instances that outrage the modesty of a woman. Whenever a man cyber stalks a woman he may end up committing acts that may seriously hamper her modesty. Therefore, this section is a regulatory provision for checking online stalking.

Thirdly, as far as the Indian Evidence Act, 1872 is concerned; there are few sections that may be resorted for the purpose of regulating electronic evidence in the cases of cyberstalking. Those sections are S.39, S.65 (B) and S.88 (A) of the Act. Since the offence is committed over the internet, most of the evidence is available in the electronic form. Therefore, regulating evidence may be a tough task. There is no concrete law in the Act dealing solely with the regulation of the evidence in the cases of cyberstalking. The above sections that may be used for the purpose of dealing with the offence are as follows:

[59] Indian Penal Code, 1860, Section 507.
[60] Indian Penal Code, 1860, Section 509.

1. S.39- *"When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.*[61]*"*

The provision states that when any evidence is produced of a statement that is originally part of a longer statement, a conversation, letter etc. or is a part of an electronic record, then evidence shall only be produced of such longer statement, or conversation or letter or electronic record if it is demanded by the court and no more. Therefore, this provision is also important from the point of view of regulating evidence in the electronic form.

2. s. 65 (B)- *"....any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or any fact stated therein of which direct evidence would be admissible....*[62]*"*

The above is clause (1) of S. 65(B) which clearly reveals that electronic evidence will be admissible in the court of law just like the documentary evidence. Clause (2) of the section discusses the several conditions under which the information generated by the computer will be considered to be admissible.

3. S.88 (A) - "*The Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the*

[61] Indian Evidence Act, 1872.Section 39.
[62] Indian Evidence Act, 1872.Section 65 (B).

> *message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.3[88A. Presumption as to electronic messages.—The Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.*[63]"

The above section reveals how the information in the electronic form is admissible in the court of law. It also states that the court shall not decide that the person to whom the e-mail address belongs is the original sender of the message. It could be anyone.

Lastly, Protection of Children from Sexual Offences Act, 2012, which was recently enacted, can be resorted in those situations wherein a child below the age of 18 years is being harassed online or is being cyber stalked. The punishment defined in the act is 3 years along with fine. This act accords protection to both male and female children.

S. 70 of the Communications Convergence Bill, 2001 will prove to be an effective provision in checking crimes like online stalking. At present, the bill is under consideration and is yet to become a concrete legislation. The section can be stated as under:

"Any person who sends, by means of a communication service or a network infrastructure facility,—

(a) any content that is grossly offensive or of an indecent, obscene or menacing character; or

(b) for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will, any content that he knows to be false or persistently makes use for that purpose of a communication service or a network infrastructure facility, shall be punishable with imprisonment which may

[63] Indian Evidence Act, 1872Section 88 (A).

extend to three years, or with fine which may extend to two crore rupees, or with both"[64].

In case the offence of cyber stalking is being committed against an individual, there are certain provisions of the C.P.C., 1908 r/w the provisions of the Specific Relief Act, 1963 with respect to grant of injunction against the perpetrator that may be resorted to provide a civil remedy to the victim thereby preventing the accused from harassing the victim. For the purpose of obtaining order for injunction against the victim, he needs to establish the fact that he is being stalked or has a fear of being stalked in the near future. The fear should be so grave that the victim anticipates "imminent danger" or such degree of injury that cannot be repaired. "Specific instances when these may be got are when there is trespass, nuisance etc. on the part of stalker or apprehension of these[65]".

[64] Communications Convergence Bill, 2001Section 70.
[65] WINFIELD AND JOLOWICZ, TORT (12th ed.).

3.2 POSITION IN US

The instances of cyberstalking have been shown to be one of the major concerns in the US. This has been exhibited by a U.S. Department of Justice report. The problem is growing at an alarming rate. The statistics revealed in the report show that presently around 80 million adults and about 10 million children are using the internet in the US. In the report it has been predicted that the number of victims of cyber stalking will be round about tens of hundreds or thousands in the United States. The need of the hour is to have stringent legislations in place so as to prevent the instances of cyber stalking.

There are certain provisions in the United States Code, which is the central legislation in the U.S. in which all the federal statutes of the U.S. have been compiled together, deal with the instances of online stalking. The various may be stated as under:

1. Interstate Stalking Punishment and Prevention Act
   18 U.S.C. § 2261A(a)
   "Whoever—
   (2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that—
   (A) places that person in reasonable fear of the death of or serious bodily injury to a person described in clause (i), (ii), or (iii) of paragraph (1)(A); or
   (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A),
   shall be punished as provided in section 2261(b) of this title."[66].

The provisions of above statute will be attracted to deal with the instances of online stalking for they define punishments for those acts done with an intention to harass or intimidate another person by means of electronic communication such as e-mails etc.

[66] Interstate Stalking Punishment and Prevention Act, 18 U.S.C. 2261(a).

It also has a psychological aspect to it in the sense that it penalises those who by the above acts, cause emotional stress and trauma to the victim.

2. Interstate Communications Act

   18 U.S.C. § 875(c)

   "*it is a federal crime, punishable by up to five years in prison and a fine of up to $250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Section 875(c) applies to any communication actually transmitted in interstate or foreign commerce - thus it includes threats transmitted in interstate or foreign commerce via the telephone, e-mail, beepers, or the Internet*"[67].

The provisions of above statute can be resorted to deal with the instances of online stalking because it determines punishments for those crimes wherein a person threatens another person via e-mails or any other mode of online communication. Therefore, threatening another person on the internet is one of the major attributes of cyber stalking.

3. 18 U.S. Code § 2425

   "Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, knowingly initiates the transmission of the name, address, telephone number, social security number, or electronic mail address of another individual, knowing that such other individual has not attained the age of 16 years, with the intent to entice, encourage, offer, or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title, imprisoned not more than 5 years, or both"[68].

The provisions of above statute will be attracted in cases of online stalking as it states that it is a crime to communicate with another person over the internet, which the perpetrator knows to be of age less than 16 years, for the purpose of encouraging and

[67] Interstate Communication Act, 18 U.S.C. 875(c).
[68] "Use of interstate facilities to transmit information about a minor", 18 U.S. Code § 2425.

instigating him to indulge in illegal sexual acts. This statute accords protection for children.

4. Federal Telephone Harassment Statute
   47 U.S.C. 223
   "Whoever—
   (1)in interstate or foreign communications—
   (A)by means of a telecommunications device knowingly—
   (i) makes, creates, or solicits, and
   (ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, with intent to abuse, threaten, or harass another person;

(B) by means of a telecommunications device knowingly—
(i) makes, creates, or solicits, and
(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

(C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to abuse, threaten, or harass any specific person;

(D) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or

(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any specific person; or

(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18 or imprisoned not more than two years, or both"[69].

The provisions of above statute will be attracted to deal with the instances of cyber stalking for it makes it a crime to call a person via telephone or any other telecommunication device so as to threaten or harass the person. It talks about those circumstances wherein the perpetrator directly communicates with the victim. The statute defines the punishment for the above acts.

"*One could argue that one of the limitations of 18 U.S.C. § 875(c) is its inapplicability to a situation where an individual engages in a pattern of conduct intended to "harass" or "annoy" another (absent some threat). Also, it is unclear whether this statute would apply to a situation in which a person harasses another by posting messages on a "public" bulletin board or in a chat room, encouraging others to harass or annoy the individual. It would appear that in some of these situations, a defendant may be prosecuted under the federal telephone harassment statute, 47 U.S.C. § 223*"[70].

The anti-stalking laws in Michigan, U.S. as laid down under the Michigan Criminal Code are as under:

1. Section 750.411i

   "... (d) "Harassment" means conduct directed toward a victim that includes, but is not limited to, repeated or continuing unconsented contact that would cause a reasonable individual to suffer emotional distress and that actually causes the victim to suffer emotional distress. Harassment does not include constitutionally protected activity or conduct that serves a legitimate purpose.

   (e) "Stalking" means a wilful course of conduct involving repeated or continuing harassment of another individual that would cause a reasonable person to feel terrorized, frightened, intimidated, threatened, harassed, or

[69] Federal Telephone Harassment Statute, 47 U.S.C. 223.

[70] "47 U.S.C. § 223 was passed in 1934, when the telephone was at the cutting edge of communication technology. It was subsequently amended in January 2006 to cover e-mail communications via the Internet." Violence Against Women and Department of Justice Reauthorization Act of 2005, P.L. 109-162 Tit. I, § 113, 119 Stat. 2960 (2006).

> *molested and that actually causes the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested.*
> *(f) "Unconsented contact" means any contact with another individual that is initiated or continued without that individual's consent or in disregard of that individual's expressed desire that the contact be avoided or discontinued. Unconsented contact includes, but is not limited to, any of the following..(v) Contacting that individual by telephone, (vi) Sending mail or electronic communications to that individual….*[71]*"*

The above provision of the MCC, can be resorted to for the purpose of regulating the offence of cyber stalking in Michigan. In the clauses mentioned above, the section defines the various terminologies forming an integral part of the crime, such as harassment, stalking etc. Clause (d) of the provision defines the various elements of harassment. It states all those things which cannot be considered to be part of the definition. Clause (e) of the provision generally defines the term stalking. It states that any repeated activity of the accused that terrorises or harasses the victim is termed as stalking. Clause (f) defines the contact wherein the stalker keeps on contacting the victim inspite of being shown complete disinterest on the part of the victim. Therefore, it is quite clear that the above section will be used to deal with the offence of online stalking if it happens to take place in Michigan.

<u>California</u>

The first statute, for the purpose of regulating instances of cyberstalking, was enacted in 1990 in California. It was enacted post the murder of television actress Rebecca Scaeffer who featured on the famous television series "*Sister Sam*"[72]. She was continuously being stalked by one of her obsessed fans who eventually attacked and murdered her. She tried to prevent him from doing so, but all in vain. Soonafter the above mentioned incident, several other states of the US as well as the federal

[71] Michigan Criminal Code Section 750.411i.

[72] WAYNE R LAFAVE, SUBSTANTIVE CRIMINAL LAW 575 (2d ed. 2003).

government also enacted laws on stalking so as to fulfil the loopholes in the legal system.[73].

The provisions of the statute 646.9 of the C.P.C. define "stalking as well as lays down the various elements of stalking". It states as under:

> *" (a) Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family is guilty of the crime of stalking, punishable by imprisonment in a county jail for not more than one year, or by a fine of not more than one thousand dollars ($1,000), or by both that fine and imprisonment, or by imprisonment in the state prison…..[74]"*

The above provision can be resorted to in the cases of online stalking in California. The section states that the definition of the term stalking and also specifies the corresponding punishment for the offence. It states that the person, who intimidates another person continuously to create fear in his mind, will be penalised for the offence of stalking with imprisonment or fine or with both.

[73] Curry v. State, 811 So. 2d 736, 741 (Fla. Dist. Ct. App. 2002)
[74] California Penal Code, Section 646.9.

3.3 POSITION IN UK

In the UK, there are presently several laws to deal with instances of stalking and cyberstalking. These include the following:

Firstly, there is the Protection from Harassment Act, 1997 which was originally enacted with the sole purpose of dealing with the instances of stalking. But the act deals with a wider range of issues in addition to the regulating of instances of stalking. These include harassment which is motivated by "race or religion", "some types of anti-social behaviour", and also "some forms of protests".

The Act provides for both civil as well as criminal remedies to the victims.

Provisions:

2A. Offence of stalking

"(1)A person is guilty of an offence if—

(a)the person pursues a course of conduct in breach of section 1(1), and

(b)the course of conduct amounts to stalking.

(2)For the purposes of subsection (1)(b) (and section 4A(1)(a)) a person's course of conduct amounts to stalking of another person if—

(a)it amounts to harassment of that person,

(b)the acts or omissions involved are ones associated with stalking, and

(c)the person whose course of conduct it is knows or ought to know that the course of conduct amounts to harassment of the other person.

(3)The following are examples of acts or omissions which, in particular circumstances, are ones associated with stalking—

(a)following a person,

(b)contacting, or attempting to contact, a person by any means,

(c)publishing any statement or other material—

(i)relating or purporting to relate to a person, or

(ii)purporting to originate from a person,

(d)monitoring the use by a person of the internet, email or any other form of electronic communication,

(e)loitering in any place (whether public or private),

(f)interfering with any property in the possession of a person,

(g)watching or spying on a person.

(4)A person guilty of an offence under this section is liable on summary conviction to imprisonment for a term not exceeding 51 weeks, or a fine not exceeding level 5 on the standard scale, or both.

(5)In relation to an offence committed before the commencement of section 281(5) of the Criminal Justice Act 2003, the reference in subsection (4) to 51 weeks is to be read as a reference to six months.

(6)This section is without prejudice to the generality of section 2"[75].

This provision can be resorted to in the cases of online stalking although it talks about physical stalking because the content and intent in the cases of both online as well as offline stalking is almost the same i.e. to pursue the victim and harass or intimidate him. The provision defines the various elements of the offence of physical stalking. It also talks about the conduct of the accused which is subject to penalty as per the provision.

S.2B. Power of entry in relation to offence of stalking

"(1)A justice of the peace may, on an application by a constable, issue a warrant authorising a constable to enter and search premises if the justice of the peace is satisfied that there are reasonable grounds for believing that—

(a)an offence under section 2A has been, or is being, committed,

(b)there is material on the premises which is likely to be of substantial value (whether by itself or together with other material) to the investigation of the offence,

(c)the material—

(i)is likely to be admissible in evidence at a trial for the offence, and

[75]Protection From Harassment Act, 1997, Section 2A.

(ii)does not consist of, or include, items subject to legal privilege, excluded material or special procedure material (within the meanings given by sections 10, 11 and 14 of the Police and Criminal Evidence Act 1984), and

(d)either—

(i)entry to the premises will not be granted unless a warrant is produced, or

(ii)the purpose of a search may be frustrated or seriously prejudiced unless a constable arriving at the premises can secure immediate entry to them.

(2)A constable may seize and retain anything for which a search has been authorised under subsection (1).

(3)A constable may use reasonable force, if necessary, in the exercise of any power conferred by virtue of this section.

(4)In this section "premises" has the same meaning as in section 23 of the Police and Criminal Evidence Act 1984"[76].

This provision basically speaks about the power of entry of the constable in case an offence pertaining to stalking as defined u/s 2A has been committed. Since s.2 (A) can be resorted to in the cases of online stalking so can this section. This provision states that a constable can enter into the boundaries of any premises after he makes an application to the concerned judicial authority who issues a warrant to that effect. The constable makes an application under those circumstances when he believes that in a given premises there is possibility of a crime having been committed u/s 2(A) has been committed or there is a possibility that an evidence pertaining to the crime is present that particular premises etc.

S.4A Stalking involving fear of violence or serious alarm or distress

"(1)A person ("A") whose course of conduct—

(a)amounts to stalking, and

(b)either—

[76] Protection From Harassment Act, 1997.Section 2B.

(i)causes another ("B") to fear, on at least two occasions, that violence will be used against B, or

(ii)causes B serious alarm or distress which has a substantial adverse effect on B's usual day-to-day activities,

is guilty of an offence if A knows or ought to know that A's course of conduct will cause B so to fear on each of those occasions or (as the case may be) will cause such alarm or distress.

(2)For the purposes of this section A ought to know that A's course of conduct will cause B to fear that violence will be used against B on any occasion if a reasonable person in possession of the same information would think the course of conduct would cause B so to fear on that occasion.

(3)For the purposes of this section A ought to know that A's course of conduct will cause B serious alarm or distress which has a substantial adverse effect on B's usual day-to-day activities if a reasonable person in possession of the same information would think the course of conduct would cause B such alarm or distress.

(4)It is a defence for A to show that—

(a)A's course of conduct was pursued for the purpose of preventing or detecting crime,

(b)A's course of conduct was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or

(c)the pursuit of A's course of conduct was reasonable for the protection of A or another or for the protection of A's or another's property.

(5)A person guilty of an offence under this section is liable—

(a)on conviction on indictment, to imprisonment for a term not exceeding five years, or a fine, or both, or

(b)on summary conviction, to imprisonment for a term not exceeding twelve months, or a fine not exceeding the statutory maximum, or both.

(6)In relation to an offence committed before the commencement of section 154(1) of the Criminal Justice Act 2003, the reference in subsection (5)(b) to twelve months is to be read as a reference to six months.

(7)If on the trial on indictment of a person charged with an offence under this section the jury find the person not guilty of the offence charged, they may find the person guilty of an offence under section 2 or 2A.

(8)The Crown Court has the same powers and duties in relation to a person who is by virtue of subsection (7) convicted before it of an offence under section 2 or 2A as a magistrates' court would have on convicting the person of the offence.

(9)This section is without prejudice to the generality of section 4"[77].

This provision talks about the various penalties that may be imposed on the accused if the offence of stalking when once committed increases possibility of violence. Therefore, this may be applicable in the cases of online stalking, the reason being that online stalking can also lead to the commission of physical violence by the accused on the victim.

Secondly, there is the Malicious Communications Act, 1988 which is an Act that makes it illegal in England as well as Wales to "send or deliver letters or other articles for the purpose of causing distress or anxiety". This is also applicable to cases of "electronic communications". The various provisions of this Act which will be attracted to regulate the offence of cyber stalking are as under:

S.1 Offence of sending letters etc. with intent to cause distress or anxiety

"(1)Any person who sends to another person—

(a)a letter, electronic communication or article of any description which conveys—

(i)a message which is indecent or grossly offensive;

(ii)a threat; or

(iii)information which is false and known or believed to be false by the sender; or

(b)any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature,

[77] Protection From Harassment Act, 1997Section 4A.

is guilty of an offence if his purpose, or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.

(2)A person is not guilty of an offence by virtue of subsection (1)(a)(ii) above if he shows—

(a)that the threat was used to reinforce a demand made by him on reasonable grounds; and

(b)that he believed, and had reasonable grounds for believing, that the use of the threat was a proper means of reinforcing the demand.

(2A)In this section "electronic communication" includes—

(a)any oral or other communication by means of an electronic communications network; and

(b)any communication (however sent) that is in electronic form.

(3)In this section references to sending include references to delivering or transmitting] and to causing to be sent, delivered or transmitted and "sender" shall be construed accordingly.

(4)A person guilty of an offence under this section is liable—

(a)on conviction on indictment to imprisonment for a term not exceeding two years or a fine (or both);

(b)on summary conviction to imprisonment for a term not exceeding 12 months or a fine (or both).

(5)In relation to an offence committed before section 154(1) of the Criminal Justice Act 2003 comes into force, the reference in subsection (4)(b) to 12 months is to be read as a reference to six months.

(6)In relation to an offence committed before section 85 of the Legal Aid Sentencing and Punishment of Offenders Act 2012 comes into force, the reference in subsection

(4)(b) to a fine is to be read as a reference to a fine not exceeding the statutory maximum."[78]

This provision talks about those acts of the accused which are committed so as to affect the mental wellbeing of the victim thereby making him anxious. The first part of the provision is worded somewhat similar to S.66 (A) of the IT Act, 2000 which has now been struck down. That provision was the regulatory provision in cases of online stalking. Similarly, the wordings of this section clearly reflect that it may be resorted to in cases of online stalking as it penalises those individuals who send such messages to another individual so as to threaten him, annoy or offend him. The provision clearly includes electronic communications under its ambit.

Thirdly, there is The Offences Against the Person Act, 1861 which basically consolidates all the provisions pertaining to offences against the person from all the previous statutes under the umbrella of a single legislation.

Fourthly, there is the Computer Misuse Act, 1990, which has provisions that may be used to deal with the offence of cyberstalking. This particular Act contains provisions to regulate those situations where one individual uses a computer so as to get unauthorised access to another's computer thereby hindering his privacy. Therefore, intruding into someone's privacy is an essential attribute of the offence of cyberstalking. The provisions of this Act assist the victim under those circumstances where the perpetrator has hacked his PC and has obtained access to his private information or has done something in his name without his prior permission etc. Therefore Ss. 1 to s.3 of the Act may be resorted for the purpose of regulating the criminal activities as stated above.

Fifthly, there is the Criminal Justice & Public Order Act, 1994 which was enacted with the view to amend certain existing laws. For example, it aimed at bringing about graver penalties in cases of certain "anti-social behaviours". Therefore, section 92 of the Act provides for increased penalty with respect to *"Obscene, offensive or*

[78] Malicious Communications Act, 1988, Section 1.

annoying telephone calls[79]*"*from what is laid down under Section 43(1) of the Telecommunication Act, 1984. The section is as under:

S. 43(1) "*Improper use of public telecommunication system*

1) A person who- (a) sends, by means of a public telecommunication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character ; or

(b) sends by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a message that he knows to be false or persistently makes use for that purpose of a public telecommunication system,

shall be guilty of an offence and liable on summary conviction to a fine not exceeding level 3 on the standard scale. (2) Subsection (1) above does not apply to anything done in the course of providing a cable programme service (within the meaning of Part IV of this Act[80]*)*".

This provision speaks about those communications which are initiated by one individual so as to threaten, annoy or offend the other individual. Therefore, it can be resorted in the cases of online stalking because one of the main aims of a cyberstalker is to send such messages so as to threaten or offend their victim. This provision also defines the punishment for those who resort to such communications.

Sixthly, as far as the Criminal Justice Act, 2003 is concerned; the provision that relates to cyberstalking is as under:

S.146-*"....Those circumstances are—*

a) *that, at the time of committing the offence, or immediately before or after doing so, the offender demonstrated towards the victim of the offence hostility based on—*

(i)the sexual orientation (or presumed sexual orientation) of the victim, or

(ii)a disability (or presumed disability) of the victim, or

[79] Criminal Justice & Public Order Act, 1994, Section 92.
[80] Telecommunications Act, 1984, Section 43.

b) that the offence is motivated (wholly or partly)—

(i)by hostility towards persons who are of a particular sexual orientation, or

(ii)by hostility towards persons who have a disability or a particular disability….[81]*".*

This provision is resorted in the cases where a crime has been committed specifically against any person who has different sexual set up, or is a person who is suffering or is believed to be suffering from any bodily disability. These persons may be potential targets of perpetrators of stalking over the internet. Therefore, this provision provides protection to those persons from being victimised by these criminal minds.

Sixthly, there is the Communications Act, 2003 which deals with cyberstalking. The relevant section is as under:

127. Improper use of public electronic communications network

"(1)A person is guilty of an offence if he—

(a)sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or

(b)causes any such message or matter to be so sent.

(2)A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—

(a)sends by means of a public electronic communications network, a message that he knows to be false,

(b)causes such a message to be sent; or

(c)persistently makes use of a public electronic communications network.

(3)A person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both.

[81] Criminal Justice Act, 2003, Section 146.

(4)Subsections (1) and (2) do not apply to anything done in the course of providing a programme service (within the meaning of the Broadcasting Act 1990 (c. 42))"[82].

This provision talks about those offences wherein the accused uses an electronic communication for the purpose of sending such messages to the victim so as to cause him to be threatened or harassed. The wording of this section is also quite similar to the wordings of s. 66(A) of the IT Act, 2000 which has now been repealed. Therefore, this section can be resorted to regulate the offence of online stalking for it talks about sending messages so as to intimidate another individual.

[82] Communications Act, 2003, Section 127.

4. JUDICIAL APPROACH: CASE LAWS

In this Chapter, we will look into the various cases that have taken place in India, U.S. and U.K. with respect to cyberstalking and also the approach of the Courts of the three countries to penalise the offenders and provide adequate remedy to the victims for the entire physical and psychological trauma he went through as a consequence of such stalking.

4.1 INDIA

1. Manish Kathuria's Case

In India, the first case pertaining to the offence of online stalking, popularly known as cyberstalking, took place in the year 2000. It was the first ever case in which the victim actually took the initiative to take an action against the perpetrator who had been harassing her over the internet. Due to this particular case, the judiciary felt the dire need to amend the current legislation which is resorted to for regulating the activities and crimes over the internet, i.e. IT Act, 2000. The act was amended in the year 2008, as a direct outcome of the instant case.

The summary of the facts of the case is that the victim, who was a woman named Ritu Kohli, was being cyber stalked by a man, named Manish Kathuria. One of the aspects of cyber stalking is that the perpetrator can use the private information of the victim and misuse it so as to terrorise the victim. Therefore, in this case, the perpetrator was engaged in pursuing the victim online, on some social networking platforms and used to send her harassing messages. Post that, he started impersonating her on a chatting website by the name of www.mirc.com and began sharing her personal information including her telephone number with strangers. Consequently, Kohli started receiving phone calls from anonymous men. For about three days, she received around forty calls from different men during odd hours. The victim was highly traumatised so her family complained the matter to the CBI who successfully traced the IP address of the perpetrator. They arrested him instantly and charged him u/s 509 of the IPC, 1860 which accords protection to the woman victims[83]. In this case the IT Act, 2000 could not come into play because this case dates back to somewhere in 2000 when this act was not being notified.

[83] P. Duggal, *India"s first Cyberstalking Case- Some Cyberlaw Perspectives*, (Mar, 10, 2017, 12:01 PM) http://cyberlaws.net/cyberindia/2CYBER27.htm.

There is no information available regarding what was the further progress made in this case. But still, this case opened the minds of the legislators a little bit for they felt the need of a legislation that would deal with the issue of cyber stalking. They introduced the section 66A in the IT Act, 2000. Now this section has been struck down from the act due to its vagueness. There exist several other provisions that may be useful in dealing with the instances of online stalking.

2. Karan Girotra v. State

This is the case which revolves around two concepts, one is online stalking and the other is anticipatory bail[84]. This case was successful enough to reach the judiciary. The facts of the case were that there was a woman by the name of Shivani Saxena. As her husband and she were unable to consummate their marriage, they decided to go ahead and file an application for divorce. Meanwhile, Shivani, who was victim in this case, started to chat with a man named Karan Girotra on some social networking platform. After a few days of talking, the man informed her that he wanted to pursue a romantic relationship with her and also marry her at the end of it. He falsely implicated her by telling her that he would make her meet with his family. Believing him, the victim went to his house, where he sedated her and then took sexual advantage of her.

After that day, he still continued to chat with her and told her he would still marry her. He then started sending her objectionable photographs of her and himself from the day where he had taken sexual advantage of her. He threatened her by saying that if she refused to marry him he would make the photographs go viral all over the internet.

Unfortunately, due to the immense physical and mental torture, the victim was convinced and decided to marry the accused. Once they got engaged, he still exploited her sexually and afterwards called off their engagement. Harassed, the victim filed a complaint against the accused u/s 66A of the IT Act, 2000.

The plea for anticipatory bail was rejected by the court. The court was of the opinion that objectionable and sexual pictures of the victim that had been circulated by the accused was a more severe form of crime which required a more profound

[84] Karan Girotra v. State, 2012 VAD (Delhi) 483 (India).

investigation. Coming on to the negative aspects of the judgment, the court decided that the victim did not disclose the fact that she was married to the accused, although she did disclose it when the accused confessed his interest in pursuing a love relationship with her. Also, the court held that the victim had given prior consent before engaging in a sexual relationship with the accused and that she was late in filing an FIR against him as she was previously happy but then as the accused called of their marriage, out of sheer annoyance, she thought to level false claims against the accused.

The above case clearly shows the fact that how lightly the cases of cyber stalking are being tackled by the judiciary in this country.

3. State of Tamil Nadu v Suhas Katti[85]

This case is known to be the first case which was disposed of by the Chennai Cyber Crime Cell in a span of seven months from the date of filing of the FIR. The facts of the case were that the accused used to stalk the victim online and started to post personal information about the victim on one of the chat rooms. The victim was a divorcee whereas the accused was a family friend of the victim. He started posting such information on the internet, which apparently was obscene as well as defamatory. The victim also started receiving messages from a fake account that was made in her name by the accused so as to intimidate her. Due to her personal information being posted in the chat groups, she started receiving telephone calls from anonymous men who believed that she was available for prostitution.

Being aggrieved by the whole situation, the victim complained the matter to the police who successfully traced the whereabouts of the accused. It was later learnt that the accused always had interest in pursuing a love relationship with the victim right before from the time she was married. When he got to know that her husband and she had ended their marriage, the accused started pursuing her all over again forcing her to marry him. The victim was reluctant so he resorted to harassing and annoying her over the internet.

There were several charges levelled against the accused. He was made liable u/s 67 of the IT Act, 2000 and sections 469 & 509 0f the IPC, 1860. The court relied on the

[85] State of Tamil Nadu v Suhas Katti (2000) (India).

various evidences that were produced on record and also the testimony of the owners of the Cyber Café from where the accused used to threaten the victim. Therefore, he was proven guilty in the case and was subjected to punishments as stipulated under the aforementioned provisions of the IT Act, 2000 and the IPC, 1860.

So far there have only been three cases revolving around the offence of cyber stalking. The need of the hour is to have stringent provisions to deal with the instances of online stalking. A proper mechanism is required so as to inform the public at large about what cyber stalking is and make them understand the gravity of the crime. Efforts shall be made to educate the people and make them realise the fact that if they get stalked online, they could always report the matter to the police thereby availing the different remedies available under the various legislations.

4. S. Raju Aiyer v. Jawaharlal Nehru University[86]

In this case, the accused used to harass the victim online by sending her e-mails which contained "offensive and derogatory words" and also contained images that were "sexually explicit" in nature. The accused used to make unwanted telephone calls to the victim at odd hours of the night and used to hurl abuses at her. Also, the victim used to go out for evening walks where the accused used to follow her so as to threaten her. He used to make "vulgar gestures" by touching himself inappropriately.
The conduct of the accused was punishable for the offence of cyber stalking because he used to intimidate her by his e-mail messages as well as telephone calls. He was also liable for physically stalking the victim as he used to follow her during her evening walks. The victim was terrorised by the activities of the accused which made her to reschedule her walking routine to an earlier time in the evening so as to avoid any confrontations with the accused. The accused was charged for "sexually harassing" the victim by the "GSCASH Committee".

[86] S. Raju Aiyer v. Jawaharlal Nehru University, 2013 LLR 1213 (India).

4.2 UNITED STATES

The first cyberstalking case in the United States resulted in the death of the victim. The summary of the case is as under:

1. United States v. David T. Matusiewicz[87]

In this case three accused were imprisoned for life for murdering Christine Belford, who was the ex-wife of on, and also the friend of Belford named Laura Mulford. They were murdered in the Delaware Courthouse at the New Castle County.

Before committing the murder, David and his family members had been involved in harassing, stalking and threatening David's ex-wife Christine Belford along with her children. On the 13th of February, 2013, when David as well as his father, Thomas got the information that Belford would be available near the courthouse, David and Thomas drove to the courthouse where they confronted Belford and thereafter shot her. They shot her numerous times so as to make sure that she was dead. Belford was present at the courthouse along with one of her friend's named Laura Mulford. As Laura saw her friend being shot, she ran so as to save her own life. Unfortunately, the accused noticed her running, so they shot dead her as well.

On investigating the car of the accused family, a red coloured notebook, which was properly spiral bound, was found. The prosecution called the book as a "stalking playbook". They called it so because the notebook contained a list by the heading "HL" meaning hit list bearing the names of all those people, whom the accused family thought had wronged him during the dispute regarding the custody of the children of David and his ex-wife Belford[88].

It was argued on behalf of the government that accused Lenore Matusiewicz and her children Newark, David Matusiewicz and nurse Amy Gonzalez for harassing, traumatising, threatening, stalking and spying on her deceased daughter-in-law and her three daughters repeatedly for a span of 3 years.

Furthermore, the government argued that the intention of the accused family was always to acquire the children's custody from the deceased victim, Belfored. In the year 2007, they even kidnapped the three daughters of one of the accused and his ex-wife and fled to Central America and even murdered Belford in the courthouse of

[87] United States v. David T. Matusiewicz, 165 F.Supp.3d 166 (2015).

[88] Available at http://www.delawareonline.com/story/news/local/2015/07/10/jury-finds-matusiewiczes-guilty/29960471/, (Mar 5, 2017, 14:00 PM).

Delaware. Both the actions of the accused corroborated the fact that the accused family were desperate to win the custody of the children.

There was a five-week trial in the District Court, U.S. in Delaware where the three accused were convicted for the various allegations levelled against them which included cyberstalking, conspiring to murder the deceased and also interstate stalking. The government also requested the Court to grant them a life imprisonment sentence for the double murder.[89]

2. United States v. Sayer[90]

This case is one of the most important cases of the US for it challenged the constitutionality of one of the anti-stalking legislations i.e. 18 U.S.C § 2261A. The accused in the instant case was a man named Shawn Sayer. He was accused of the offence of cyber stalking. He had been stalking a girl named Jane Doe on the internet, although he pled guilty. He could not prove his innocence in the court of law and the court decided to imprison him for a period of 60 months as envisaged under the statute. Consequently, the accused appealed against the decision of the court to the District Court and contended that the statute under which he was penalised was not constitutional.[91]

It was decided by the court that the statute in question was very much constitutional and was not vaguely worded. The accused was punished as per clause (2)(A) of the section 2261, and it was absolutely fair because that clause penalises those who indulge in such acts so as to harass or intimidate the victim. Therefore, the accused had no standing in the instant case to argue that the clause would not apply to his conduct. It was instead vague of him to contend that it would not be applicable in his case as it was not applied in the case of others when it was his conduct that is clearly a punishable act under the provisions of the statute.[92]

The district court was of the opinion that in the instant case, all the requisites pertaining to the offence of interstate stalking were clearly met, as are envisaged under 18 U.S.C. § 2261A(2)(A). The court held that the accused was involved in

[89] Available at http://www.jsonline.com/story/news/crime/2016/02/12/emergency-sentencing-today-hospital-lenore-matusiewicz/80299490/, (Mar,7.2017,14:01PM).
[90] United States v. Sayer
[91] Available at http://caselaw.findlaw.com/us-1st-circuit/1665132.html
[92] *Id*. at 55.

harassing his ex-girlfriend, i.e. the victim, who lived in an altogether different state via e-mails and other communicating methods available online. He even shared her personal information on different social networking platforms which is why anonymous men used to contact her through telephone calls or showed up at her house for they thought she was available for prostitution. This terrorised and intimidated the victim so much so that she had reasonable fear of being seriously injured or even killed by the stalker. At last it can thus be concluded that the decision given forth by the court was quite predictable seeing the conduct of the accused who was so desperate to stalk the victim that he used the internet when she happened to completely change her place of living.[93]''

3. United States v. Abraham Jacob Alkhabaz a.k.a. Jake Baker[94]

In October 1994, Alkhabaz, who was an undergraduate at the University of Michigan began submitting stories depicting the rape, torture, and murder of young women to the alt.sex.stories usenet group. One of the stories graphically described the rape, torture, and murder of one of his classmates, a woman to be called Jane Doe. A Michigan graduate who read the Doe story and recognized the victim's name contacted university authorities, who called the police.

When police searched Baker's computer, they found more stories and an e-mail correspondence he maintained with a Canadian known as Arthur Gonda. The e-mails outlined a plan by which the men would meet in real life, abduct a young woman, and carry out the fantasies in Baker's stories and e-mails to Gonda. The police believed Baker and Gonda represented a threat to Jane Doe and other potential victims, so they brought in the FBI.

Charges were brought under 18 U.S. Code § 875(c), which makes it a federal crime to transmit ''…any communication containing any threat to kidnap . . . or to injure the person of another.'' Baker argued that while he had sent communications neither his alt.sex.stories postings nor his e-mails to Gonda constituted ''threats'' to kidnap

[93] Sarah R. Gitomer, Cyberstalking: A New Phenomenon, United States v. Sayer, No. 2:11–cr–113–DBH, 2012 WL 2180577 (D. Me. Jun. 13, 2012).

[94] United States v. Abraham Jacob Alkhabaz a.k.a. Jake Baker, 104 F.3d 1492 (1997).

and/or injure anyone. Baker said they were fantasies he was sharing with Gonda. The district court agreed and dismissed the charges.

The government appealed.

The judges found that although Baker's stories were disturbing, they were not "threats."

They noted that to constitute a ''threat,'' a communication must ''be such that a reasonable person . . . would take the statement as a serious expression of an intention to inflict bodily harm."

The Sixth Circuit held that Baker's stories and e-mails did not constitute a threat under this standard.

4. This case which revolves around a student who had been stalking his school teacher online. He met his teacher on an online dating service[95]. He tried to threaten her on a video call. The name of the accused is Andrew Archambeau. Both, the accused as well as the teacher had been talking and chatting over the dating site for round about five days.

   Soon the teacher realised that she was not interested in any romantic engagement with her student Andrew, the accused in the instant case. The accused was reluctant to put an end to the talking sessions he was having with his teacher and wanted to get into a relationship with her. The victim (teacher) stopped talking to him but he repeatedly sent her twenty e-mails so as to persuade her to talk to him which for the teacher, was traumatising. When the accused learnt about the allegations instituted against him, he contended that there was someone leaving messages one after the other on his caller ID. It showed the location of the victim, so he believed that it must be she who had been calling him anonymously for she was still interested in pursuing a relationship with him. The teacher on hearing the same denied the claim and consequently, went to the police. The accused still left a message on her answering machine saying that he was keeping his eyes on her. He knew the exact time when she left home for work.

[95] Lewis PH: Persistent e-mail: electronic stalking or innocent courtship? New York Times, Sept 16, 1994, p Bl1

Soon the case was brought before the court. The accused student contended that he was in love with the victim. Just because he was repeatedly sending messages, he cannot be prosecuted. Also, his messages were in no way threatening or harassing the victim, who had a choice to read or to avoid his messages. But the anti-stalking law makes non-consensual contact through an electronic medium as a punishable offence.[96]Thereafter, the accused was sent on probation for a year. The court also ordered him to undergo a psychiatric evaluation[97]."

5. This is a case which was reported in Georgia. It revolved around one Cynthia Armistead-Smathers who was the victim of cyberstalking. She was being stalked by one Richard Hillyard. [98] He used to send her obscene e-mails so as to harass and terrorise her. Thereafter, she started receiving messages from anonymous accounts. Eventually, she reported the account of Hillyard as a result of which his account was deleted by his ISP. But the problem did not stop and it only increased. Cynthia started to receive harassing mails from Hillyard's professional account. Hillyard worked at the Center for Disease Control and Prevention in Atlanta. Hillyard had posted a nude picture of a woman that went viral online. People assumed it to be an image of Cynthia. Soon she was flooded with hundreds and thousands of messages from different men. The image posted online also contained her name, telephone number and e-mail address with a message saying that she was available for prostitution during the time of Olympics. On seeing this, Cynthia was highly traumatised which made her change her place of living for over three times. Not only this, she changed her telephone number uncountable times and also kept a licensed gun with her for to keep her safe from any potential threat.

   She then reported the matter to the police. On investigating the matter, the police informed her that they were not very successful in catching the perpetrator, i.e. Hillyard. Then again she received a message from an

[96] Michigan Criminal Code, Section 750.41 1h (1998).

[97] Associated Press, *E-mail stalker sentencing likely will influence future cases*, THE DETROIT NEWS HOME PAGE, Mar 23, 1996.

[98] Hendren J, *Online harassment bill gains momentum*, LOS ANGELES TIMES, May 25, 1997, at E4.

anonymous sender telling her that he had been following her 5 year old daughter and her. He even followed her the other day when she was returning with her daughter from the post office. He followed her until she was back home. Soon the accused, i.e. Hillyard was arrested and charged for online stalking. Later, it was learnt that once he was released from jail, he started sending harassing messages to Cynthia so as to harass and threaten her all over again but when he was confronted he denied all the allegations made against him[99].

6. A $10 million lawsuit was filed by one Jayne Hitchcock claiming defamation and harassment against the Woodside Literary Agency of New York[100]. The agency had posted an advertisement which she had replied to. In response, before representing her, the agency asked from her, a few monetary payments and fees. This led Hitchcock drown in suspicion because no legitimate agents earn even before selling the work of an author. Subsequently Hitchcock together with some more suspicious authors, put in all grave efforts towards informing and making aware, the other writers about the suspected fraud. Hitchcock further claims that the agency subjected her to assaults and also defamed her. The given incidents had been stated in her complaint: e-mails used by Hitchcock and others [including her literary agent, and her employer (the University of Maryland)] dealt with mail bombing; in newsgroups, rousing and provocative messages were posted with Hitchcock's name. Also, under Hitchcock's name, a post that was, sexually-oriented, was posted along with her full name, address and phone number. This led to various unknown phone calls, a suspicious package containing incense, magazine subscriptions (unsolicited) etc. Even though she contacted the local police & FBI, it was quite not evident how she could substantiate the accusations only because any actual threat hadn't been made against her. Moreover, the tormentors had made it very hard to track their accounts because in order to hide their identity they had already altered their basic information. Then took place, the

[99] Hendren J, *Online harassment bill gains momentum*, LOS ANGELES TIMES, May 25, 1997 at E4.
[100] I*d.* at 97.

establishment of Jayne Hitchcock legal fund. Jayne Hitchcock gave testimony before a sub-committee in order to punish the prime devisers of the mail harassment in Maryland[101]".

7. This case revolves around the founders of Dallas's largest internet access provider, Internet America, Robert and Teresa Maynard, who noticed that there were certain threatening messages being posted on an internet newsgroup.[102] The messages that were posted on the newsgroup stated a poem saying that "Lord grant me the serenity to accept the things I cannot change…and the wisdom to hide the bodies of the people I had to kill." One of the messages also included a message defaming Maynard. It was written about her that she was unfaithful. There was another message that stated the name of the perpetrator, his age and how he was being accused for burglary and possessing weapons. It was also, stated that he was a computer consultant. When the perpetrator was confronted, he contended that it was Maynard and his employer who had been threatening him. Therefore, in an effort to respond to these attacks, the accused had been posting threatening messages over the newsgroup. The accused tagged himself to be "The Cyberstalker".

8. This is the first successful case in the United States for prosecuting the accused of a cybercrime. In this case, the accused was a former student of the University of California named Richard Machado. He was accused for sending threatening e-mail messages to the Asian students of the university thereby violating their civil rights. The students were round about 59 in number who received a mail from the accused. Below each message, he wrote "Asian hater".[103] In the messages he wrote that it was his life's main aim to find each one of these Asian students and then murder all of them. Furthermore, he wrote that he was very determined to kill all of them and he hopes that his message was loud and clear. Also, he stated thereby threatening them that, if these students did not withdraw their enrolment from the university, he would

[101] McFadden RD, *Suspect in New Jersey strangling was reportedly sex-case victim*, N.Y. TIMES, Oct 3, 1997 at p A1.
[102] Whitelaw K, *Fear and dread in cyberspace*, US, WORLD & NEWS REPORT, 121 (1 8):50, 1996.
[103] Maharaj D, *U.S. to retry man in hate e-mail case*, LOS ANGELES TIMES, Dec 2, 1997 at p A3.

kill them all. The case was brought before a jury, who previously was deadlocked nine to three in the favour of acquitting the accused. The accused was sentenced to imprisonment for a year. The accused was in the jail for a year and once he was released, he underwent another trial where he was charged with a fine of $1000 and was ordered to go on probation for one year. He was prohibited from using the computers of the university's laboratories.[104] The attorney on behalf of the accused contended that the messages sent by him to those 59 Asian students were annoying rather than being harassing. On the other hand, the victims were traumatised so much so by the messages, that they were all prepared with pepper sprays from any potential threat. Also, they withheld from going out at night all alone.

9. U.S. v. Bowker[105]

This case is one of the most important cases on online stalking. In this case, the accused named Bowker started stalking a reporter of a local newspaper named Tina Knight. The incident took place in the year 2000, when the accused started sending umpteen numbers of mails to her and to the organisation where she worked. Many of the mails that were sent to her and the station contained her photographs along with harassing messages concerning her. Some of the messages said "Thanks for my daily Tina Knight fix. Thanks for helping me get my nuts off," and "More Tina Knight, that is what I want and need."

There were other harassing messages as well which explained how he had been continuously stalking her and had been keeping his eyes on her as to when she left from home and when she reached back home. As result, the victim was highly terrorised so she left her hometown and moved to an altogether new state. Even this did not prevent him from not stalking her. He repeatedly sent her harassing e-mails and even sent letters to her via post to her new house. Eventually, he was being arrested and imprisoned for the

[104] Hua T, *Ex-student sentenced for hate e-mai*, LOS ANGELES TIMES, May 5, 1998, p A24
[105] United States v. Bowker, 372 F.3d 365.

offence of not only online stalking but also offline stalking. Therefore, he appealed by challenging the constitutionality of the statute under which he was sentenced. The statute was declared to be absolutely constitutional prima facie by the Sixth Circuit Court. The court was of the opinion that since the case involved the rights of many individuals, it was not likely that the right to speech of the accused was being affected in any which way whatsoever.[106]"

[106] Available at http://cyberstalking.web.unc.edu/caselaw/, (Mar, 5, 2017, 21:01PM).

4.3 UNITED KINGDOM

The offence of stalking both physical as well as cyber, has received much attention of the media and the legislators. There have been several cases that have taken place over the years, but the gravity of the offence has been realised only now. Let us discuss the various cases that have taken place in UK pertaining to cyber stalking.

1. Andrew Meldrum Case

In this case, the accused named Andre Meldrum was alleged to have committed the offence of voyeurism as well as of getting unauthorised control over the computers of the two different women victims. The accused had installed on the two computers, a software bug that he used for the purpose of spying on the two victims. The bug had been installed on the webcam of the computer. The two women were suspicious about the software being installed on their PC by the accused bas they were acquainted with him. Both of them had met only sometime back with the accused. They went and reported the case with the police[107].

On investigation, it was discovered that the software had been present on their PCs for round about fifteen months. He had installed the software on their PCs for the purpose of seeing the two women take their clothes off, thereby filming him. The accused had about 11,000 photographs of the victims on his own computer[108]. The trial against the accused went on for about seven days and at the at end of it, he was declared guilty of the two offences.

2. R v Debnath[109]

In this case the accused name Anita Debnath was being prosecuted for having committed the offence of online stalking against the victim. The victim was her boss named Chay Ankers. The accused was obsessed with the victim after they had engaged in a sexual relationship just for one night. The accused had a misconception that the victim was suffering from a sexually transmitted disease and had transmitted the same to her after the night they had sexual intercourse. Therefore, they both

[107] Available at http://www.mirror.co.uk/news/uk-news/andrew-meldrum-peeping-tom-rigged-3204007, (Mar 13, 2017, 19:00PM).

[108] Available at http://www.telegraph.co.uk/news/uknews/crime/10866262/Cyber-stalker-bugged-womens-computers-to-spy-on-them-in-their-bedrooms.html, (Mar, 13, 2017, 19:05PM)..

[109] R v Debnath [2006] 2 Cr App R (S) 169.

underwent a test to check whether they were infected with the disease, but the reports were negative.

Post the incident the victim went into a love relationship with another a girl named Hamlet. The accused was annoyed; therefore she started sending e-mail messages to the victim's girlfriend under the false pretext of being the victim's friend and communicated to her about the sexual relationship he had with the accused. She also sent e-mails to the victim's boss impersonating the victim and confessing the fact that he was the one who had been threatening the accused. Not only this, the accused registered the name of the victim on a website named "www.chayisgay.com" mentioning the fact that he was suffering from a sexually transmitted disease. Next, she also posted articles on the site accusing him of engaging in "homosexual" practices.

Furthermore, the accused hired hackers for the purpose of getting access into the victim's account. The hackers sent e-mail messages to the victim's account with a link containing the virus named "Trojan". As soon as the victim tapped on the link, his account was being hacked and the accused was able to see the mailbox of the accused.

The victim on being harassed on so many occasions lodged a complaint against the victim. The court issued a restraining order against the accused thereby preventing her from posting false information about the victim over the internet.

3. Burnett v. George[110]

In this case, the accused used to harass the victim by phoning her at odd hours, showing up at her place unnecessarily. Not only this, he used to threaten the victim over the phone and was also alleged to have caused "damage" to her house. Consequently, the court of appeal granted an injunction as a remedy to the victim thereby preventing the accused from threatening or harassing her by calling her over the telephone or making unwanted visits at her place etc. These activities of the stalker had led to psychological impact on the victim in the sense that her health was continuously deteriorating.

[110]Burnett v. George , (1992) 1 FLR 525.

5. JURISDICTIONAL, CONSTITUTIONAL AND EVIDENTIARY ISSUES

This chapter deals with the unaddressed issues pertaining to Cyberstalking like jurisdiction, production of evidence and other constitutional incompatibilities.

5.1 JURISDICTIONAL ISSUES

Cyber stalking is a kind of cyber-crime which causes a lot of issues related to enforcement. These issues arise on account of several reasons, for instance anonymity, which is a plus point for the stalker. He may be sitting miles away, sometimes all together in a different country, from his victim which can cause several jurisdictional concerns like where was the crime actually committed and consequently which country would have the jurisdiction to try the matter. Just imagine a situation wherein you, being a citizen of India, are being stalked by a person who is sitting miles away from you, say in Canada. As a result of being harassed by the stalker, you decide to lodge a complaint against him for you have no clue about the whereabouts of the perpetrator. On completion of the investigation by the police, you are informed that the stalker is a citizen of Canada. Now arises the real problem as even if the police successfully established the fact that the stalker is a Canadian, how will they possibly proceed so as to arrest and make him liable under Indian Information Technology Act, 2000?

The issues pertaining to jurisdiction arise because the domestic statutes of a country, limit the application of the provisions of the statute to the country's own boundaries[111]. There are numerous legislations that come into play when the offence involves the use of the internet[112]. Whenever a cybercrime is committed and the victim and the accused belong to two different cities, districts or even countries, the enforcement of law becomes a tedious job if not impossible. Several problems, ranging from investigation up to prosecution crop up.

Whenever a cybercrime is committed, and the offender is sitting in an entirely different country then under those circumstances, the extradition laws come into play. It is a slightly tougher system of prosecution for the reason that extradition

[111] J. Petrocelli, *Cyber Stalking*, 53(12) LAW & ORDER 56 (2005).
[112] JR Reidenberg, *Governing Networks and Cyberspace Rule-Making*, 45 EMORY L. J. 911 (1996).

arrangements will have to be entered into between the two countries for the reason of prosecuting the accused. There are several countries who do not want to enter into these arrangements for the purpose of prosecuting the accused. For instance, let us talk about the New York District Attorney's office. They are highly unwilling to take up any case pertaining to extradition from another country with respect to cyberstalking. They do not accept it even if there is ample evidence on record to prove the guilt of the accused (citizen)[113]. Under this circumstance, at most what the victim's country can do is make an official request to the country of the accused to take up action against him as per their laws.

There is another problem that crops up in cases relating to extradition or requesting another country to take action as per their laws. The problem is that what is punishable under the laws of the victim's country may not be an offence as per the laws of the perpetrator's country[114]. In such a situation, the perpetrator's country may refuse to penalise their citizen for something which is not a crime under the statute of their country or extradite their citizen. They even may, not assist the victim's country to investigate into the matter. For example, in UK under the Telecommunications Act, 1984, if a person sends messages through a device which is not located in any place inside UK, then in that case no crime is considered to have been committed[115].

Section 354D of IPC, which is one of the main provisions for the purpose of regulating cyber stalking in India, also suffers from a lot of shortcomings. The language of clause (1) of the Section:

"(1) Any man who—

- *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*
- *monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking…*[116]*"*

[113] S. Hutton, *Cyber stalking*, (Mar, 7, 2017, 16:30PM), http://www.nw3c.org.
[114] P. Bocij, *Reactive Stalking: A New Perspective on Victimization*, 7(1) BRITISH J. FORENSIC PRACTICE 23 (2005).
[115] Telecommunications Act, 1984, §43.
[116] Indian Penal Code, 1860, Section 354D.

clearly indicates that it penalises all those men who are:

1. close to the victim or are involved in a relationship with her,
2. the relationship may be private or professional,
3. the perpetrator has access to her private online activities,
4. the woman has knowledge about the fact that the perpetrator has access to her internet related data and activities.
5. Also penalises those men, who are in no way related to the woman but invades her privacy.

Therefore, other than the above mentioned categories, it does not provide any remedy against "interstate stalkers". This raises the problem of jurisdiction in the sense that there is no explicit provision in those cases where the woman is being stalked and is being harassed by a man who is sitting miles away from her in an altogether different country as is mentioned under 18 U.S.C 2261A[117].

Now let us discuss one of the biggest hurdles in solving cases relating to online stalking which is the advantage of being anonymous[118]. Due to this anonymity, it is difficult to successfully enforce laws for we do not know the whereabouts of the perpetrator. It is one of the toughest jobs to trace the location of the accused. Due to technological advancements, it has become an easy task for the perpetrators to conceal their identities. One of the ways to do that is to create a fake e-mail account. For instance, a man named James Bond may use a fake e-mail ID like werocktheworld@yahoo.com solely for the purpose of harassing and intimidating others by sending messages through this particular account. This is one of the most common and simple ways by which one can easily harass another because ISP's do not have any mechanism for the purpose of authenticating the information that is available with them. Another and a more convenient method for the purpose of concealing the identity over the internet is by making use of "re-mailers". These are services that assist one to remove all the information from an e-mail address which could successfully help one to recognise the source of the information received. They replace the e-mail address of the perpetrator with a name which is untrue and

[117] Debarati Halder, *Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Lawsin India from Restorative Justice and Therapeutic Jurisprudential Perspectives.*
[118] R. Wacks, *Privacy in Cyberspace: Personal Information, Free Speech and the Internet in PRIVACY AND LOYALTY*, 93 (P. BIRKS ED., 1997).

misguiding thereby making it almost impossible to trace the location of the perpetrator[119]. There are various other mechanisms available which help the offenders to wipe out any possibilities of them being caught. They make use of these mechanisms so as to stalk others in the most secure way. These mechanisms enable them to remain untraceable as they make it impossible for one to track any kind of link between the sender's e-mail and the recipient's e-mail. Sometimes, these criminals make use of successive re-mailers wherein their message travels through a series of re-mailers leaving zero possibility of tracing the e-mail from where the message was originally sent to the victim. This method is popularly known as "chaining".

The IT Act, 2000 solves this jurisdiction concern only to a certain extent. There are provisions available in the act which can be resorted to in cases where the perpetrator is a national of a different country, but there lays a prerequisite[120]. What is required is that the offence being committed by a citizen of another country shall necessarily involve a computer system or network being operated in India[121]. The problem is only solved to very slight extent. The need of the hour is that there shall exist a proper legislation, which solely deals with cybercrimes and addresses all major issues pertaining to them with regards to jurisdiction etc.

[119] S. Greenberg, Threats, *Harassment and Hate On-line: Recent Developments*, 6 BOSTON PUBLIC INTEREST J. 673 (1997).
[120] S. Vadehra, Kan and Krishme, *Data Protection and the IT Act India*, (Ma, 11, 2017, 12:00PM) http://www.galamarketlaw.com/joomla4/index.php?option=com_content&view=article&id=261&Itemid=138.
[121] Section 75, IT Act,2000.

5.2 CONSTITUTIONAL INCOMPATIBILITIES

There exist several constitutional incompatibilities with regard to the offence of cyberstalking and the legislations which help in the regulation of this crime. We will elaborately discuss how Articles 14, 19 & 21 get violated due to the several aspects of cyberstalking and the various provisions resorted to for the purpose of dealing with the offence.

Let us first discuss how Article 14 of the Indian Constitution is being curtailed by one of the major provisions for regulating online and offline stalking i.e. S. 354D of the Indian Penal Code, 1860 along with few other provisions of the same legislation.

Article 14 envisages the Right to Equality, which is amongst the most basic rights that has been guaranteed to every citizen of India. It states as under:

"The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India Prohibition of discrimination on grounds of religion, race, caste, sex or place of birth."

The language of the article makes it very evident that equal treatment shall be accorded to men and women in the eyes of law. There shall not be any distinction made between the two sexes on any grounds whatsoever. But there are a few provisions of the Indian Penal Code, 1860, which clearly violate this basic human right. Sections like 354C, 354D and 509 of the IPC are gender biased on the very face of it. Sections 354C and 354D were inserted post the Delhi gang-rape case in the year 2012. Undoubtedly, stringent laws are required to penalise the perpetrators committing sexual offences, but at the same time, the legislators shall bear in mind the fact that crime can be committed by both a man as well as a woman.

In the world today, everything is possible. Also, women have managed to get an equal status as that of the men. Therefore, a crime can also be committed by a woman against a man. The language of the provisions clearly reflect the fact that they are gender specific and accord protection only to female victims and not the male victims. Not only this, these penal provisions define punishments for only male victims and if the same crime is being committed by a female, there is no provision to regulate her conduct. The legislators have overlooked several possibilities and have failed to make

note of famous foreign cases where a woman was the perpetrator of online stalking who used to harass another woman who was younger than her. The victim was so traumatised by the harassment that she finally took her life because of the immense emotional distress and fear she was going through[122]. There is no provision for regulation same sex stalking. What will be the position of law under above circumstances is unknown and not thought of by the legislature.

Secondly, let us see how Article 19 is getting curtailed by the offence of cyberstalking. One of the major attributes of cyberstalking is the concept of anonymity. It is like a boon for the perpetrators while a bane for the victims and the law enforcement agencies. Therefore, it has been contested by many scholars and legal persons, that this issue with regard to anonymity can be easily solved if proper restrictions[123] were placed on the people by asking them to refrain from adopting it. On the contrary, there are a few who do not support the claim and view it as a means to violate the basic fundamental right of an individual guaranteed u/A 19 of the Indian Constitution.

Article 19 talks about "Right to Freedom of Speech & Expression" which is given to every citizen of India, whether he is criminal or not. All over the world, this right has been guaranteed to the people by their respective countries[124]. It has been argued by most that anonymous communications has its own pros and cons. By the use of anonymity factor, various newspaper agencies can easily collect important information. Various renowned agencies such as the Amnesty International utilises it as a mechanism for the purpose of transmitting information. It is also being used by investigating agencies, for example the police, for the purpose of tracing law breakers and putting them behind bars thereby reducing the growing crimes[125].

---

[122]"A girl named Meir was being cyber bullied by another woman Lori Drew on a social networking platform, who bullied her in the disguise of a teenage boy. As a result of the bullying, the victim. Drew was acquitted. Later, a Bill was proposed to amend Title 18, USC in respect to cyber bullying, which was popularly known as H.R.1966 (111th) Megan Meir Cyber bullying Prevention Act".

[123] L. Ellison and Y. Akdeniz, *Cyber-stalking: the Regulation of Harassment on the Internet*, CRIM. L. REV. 29 (1998).

[124] Constitution of India, Article 19(1)(a); Constitution of USA, First Amendment; South African Bill of Rights, §12; European Convention on Human Rights, Article 11.

[125] L. Ellison and Y. Akdeniz, *Cyber-stalking: the Regulation of Harassment on the Internet*, CRIM. L. REV. 29 (1998).

As far as the scenario with respect to anonymity is concerned, the Supreme Court of United States in one of the cases held that just because there was a possible threat due to the anonymous perpetrator, it was legally incorrect to violate the right to freedom of speech and expression by restricting anonymous communications. Therefore, it can only be supressed under those circumstances where the threat involved was a serious one[126].

On the other hand, courts in UK in one the recent case held that there should be balance between the right to privacy and the right to freedom of speech of an individual. Therefore, the court issued an injunction against the publication of private information of an individual into the newspaper[127].

Finally, coming on to the scenario in India, the Supreme Court in one of its latest judgment restated that the fundamental right guaranteed under Article 19(1)(a) of the Constitution is not an absolute right[128]. The S.C. in yet another case held that the right was not absolute, therefore restrictions could be imposed on the media to prevent them from reporting the details of a courtroom proceeding[129]. However, the position in US is different. Absolute protection has been accorded to this right.

Therefore, it can now be concluded that in India, if any case arises which pertains to online stalking and involves an anonymous offender then, in all those cases, the court will have the power to restrict the freedom of speech of an individual by disallowing anonymous communication via the Internet.

Lastly, let us now discuss as to how Article 21 of the Constitution is getting violated. In the instances of online stalking, the privacy of an individual is being invaded. Article 21 guarantees to every citizen of India the "Right to Privacy". Although there is no explicit mention of the same in the Article, but the Supreme Court through its various judgments has proved it to be under the umbrella of this Article. The Article states as under:

---

[126] Whitney v. California, 274 U.S. 357, 376-77 (1927).
[127] CTB v. News Group Newspapers, [2011] EWHC 1232 (QB).
[128] In re Ramlila Maidan Incident v. Home Secretary, Suo Motu Writ Petition (Crl.) No. 122 of 2011, decided on Feb. 23, 2012, (India).
[129] Sahara India Real Estate Corp. Ltd. v. Securities & Exchange Board of India, C.A. No. 9813 of 2011, decided on Sept. 11, 2012, (India).

"No person shall be deprived of his life or personal liberty except according to procedure established by law"[130].

As far as this right is concerned, it is one of the most essential and most basic needs of every individual. This right demarcates an area around the individual and no other person has the right to intrude into this space. This right to privacy implies that one person cannot and does not have the right to interfere into the private activities of another individual. Therefore, whenever an individual commits a crime involving the internet, as in the instant case, stalking online for the purpose of harassing another individual by securing his private information, then it can be inferred as violating the right to privacy of an individual thereby violating Article 21 of the Constitution.

[130] Indian Constitution, Article 21.

5.3 EVIDENTIARY ASPECTS

Whenever a crime is committed, and the victim as well as the offender are both present at the scene of crime, or there are several ways by which one can ascertain the details and whereabouts of the offender. Under those circumstances it becomes easy for one to gather evidence so as to prove the guilt of the offender. But the whole process of collecting evidence becomes a tedious job whenever the Internet gets involved.

In today's world, when the technology is continuously advancing at an alarming rate, there have developed numerous ways by which one can make wrongful use of this technology for the purposes of harassing others. In the cases of cyberstalking, it has become an extremely simplified job for the stalker to not only harass the victim, but also conceal his identity so that he is not caught. There have developed so many mechanisms, like re-mailers, by which it is almost impossible to detect the source of the information received by the victim, as we have already discussed in the earlier part of the chapter. Now let us discuss as how can a person victimised by online stalking, collect evidence so as to make out a case against the perpetrator.

There are certain provisions available under the Indian Evidence Act, 1872 which show whether an electronic record is admissible in the court of law or not. These sections include S. 65(B) & S. 88(A). The sections may be reproduced as under:

1. S. 65(B)-"Clause (1) of the section envisages that all the information that is present in the electronic form, for instance on a computer device or system, and is reproduced on the paper by way of printing etc. or other methods such as copying any image available on the system by means of optical or magnetic medium, then all that information will be considered to be as authentic as any other documentary evidence. Such paper on which the information is stored will be considered to be a document for the purpose of producing evidence in the court of law and will be considered admissible just like any other piece of document. Such piece of paper will be treated as a good piece of evidence in any court proceeding. Also, the provision says that the person producing such

evidence is not required to provide any other evidence in support of such paper or produce the original source of the facts stated. [131]"

The above is clause (1) of S. 65(B) which clearly reveals that electronic evidence will be admissible in the court of law just like the documentary evidence. Clause (2) of the section discusses the several conditions under which the information generated by the computer will be considered to be admissible.

2. S.88 (A) – this section states that any message that the recipient receives from the original sender of the message via e-mail will be considered to be the message that was stored in the computer device of the sender and will be treated as the same message that he meant to send to the receiver. Also, it states that the court shall not come to any conclusion regarding the original sender of the message.[132]

The above section reveals how the information in the electronic form is admissible in the court of law. It also states that the court shall not decide that the person to whom the e-mail address belongs is the original sender of the message. It could be anyone.

There is another section of the IEA, 1872 that may be used to regulate evidence that is available in the electronic form, i.e. S.39 of the Act. The provision states that when any evidence is produced of a statement that is originally part of a longer statement, a conversation, letter etc. or is a part of an electronic record, then evidence shall only be produced of such longer statement, or conversation or letter or electronic record if it is demanded by the court and no more. Therefore, this provision is also important from the point of view of regulating evidence in the electronic form.

There are various ways by which one can handle evidences in the cases of online stalking. Some of them may be listed as under:

1. Various experts and legal scholars have suggested that in all those situations where the victim and the cyber stalker are acquainted with each other, the victim shall exhibit a clear sign in the form of a warning to the stalker to stop

[131] Section 65(B), Indian Evidence Act, 1872.
[132] Section 88(A), Indian Evidence Act, 1872.

doing whatever he has been doing if he does not want the victim to take any legal action against him.

2. Once the victim sends a word of caution to the stalker, then no matter what, he shall never ever communicate with him in the future. All the conversations that he has had with stalker shall be saved in the electronic form as well as in the hard copy for the purpose of producing evidence if the need arises.
3. Once the victim realises the fact that he is being stalked online, then in all those situations, instead of feeling scared, the victim shall take note of the e-mail address of the stalker, along with any communication that the stalker happens to make with the victim. The victim shall start collecting evidence to support his claim both in the soft as well as the hard copy.
4. The victim shall also make note of the specific dates of contact and time of receiving the harassing messages from the stalker as important pieces of evidence.
5. The victim can then proceed with filing an FIR against the stalker if they feel that the problem is a serious one. They can even contact their lawyers so as to get an advice from them on how shall they proceed, what all charges can be levelled against the stalker and what remedies are available for them under the different legislations.
6. The victim shall be sure that their evidence is one which is fully authenticated because over the internet, one of the major problems is that the ISPs do not have any method to check the authenticity of the information available online.

Listed above are the few ways by which a victim can record evidence so as to prove the guilt of the accused. Although, the law makers should formulate new laws to regulate not only the evidentiary aspects of the crime of cyber stalking but also the crime itself.

6. CONCLUSION & SUGGESTIONS

Just a few years back, online stalking was never considered a grave offence. The legislators all the world never focussed much of their attention on it, as a result of which there has never been any concrete legislation dealing with the offence. This paper has tried to prove that the two forms of stalking i.e. online as well as offline are two independent form of cybercrimes. The fact that there does not exist any sole provision that deals with the offence of online stalking and the same is regulated by the provisions that define and penalise offline stalking. The legislative regime is mostly the same in India, US as well as UK in their response to cyberstalking. All those laws that regulate physical stalking are resorted for the purpose of dealing with the offence of cyber stalking[133].

The need of the hour is to formulate new provisions to deal with the offence of online stalking because the provisions on offline stalking are insufficient to deal with it. What needs to be understood are those intricacies of this offence which are a little bit different from that offline stalking. After understanding and analysing every minute aspect of the crime, the legislator should take the initiative to frame new laws for the same which includes a provision for clearly defining the term, with the various conditions under which a person can be considered to be guilty of the offence, the different remedies available for the victims and the various penal provisions depending upon the gravity of the offence[134].

As regards the scenario in India with respect to the crime, the need of the hour is that amendments shall be proposed to the current IT Act, 2000 which deals with provisions relating to activities over the internet. No doubt that there are certain provisions that deal with the offence indirectly or can be used to deal with the offence indirectly, but the need is to have a provision that purely deals with online stalking as an offence. The procedure of introducing a new law is time consuming. The Bill needs to be introduced in the two houses of the Parliament, and then once it is passed by both the houses, it finally becomes a law after obtaining assent from the President.

---

[133] Ridhi Kabra ,*Cyberstalking: One Problem Control-Alt-Delete Can't Solve*, 2008-35, Vth Year BA LLB Hons.

[134] *Id.*. at 130.

Therefore, efforts shall be made at the earliest possible to bring about a change in the legislative system[135].

Previously, Section 66A of the IT Act, 2000 could be used to deal with the problem of online stalking but because the section has now been declared vague and void by the judiciary, it becomes more than necessary to have a new provision in place so as to deal with the offence.

As we have already seen in the preceding chapters, there are many problems related to the enforcement of the laws relating to the offence of online stalking. One of the major issues arises when the victim as well as the accused belongs to two different countries. What is required is to have a convention entered to between the countries at an international level. Provisions of the conventions relating to cyberstalking shall be framed in such a way that all jurisdictional infirmities relating to the offence are snapped. The provisions shall allow the countries to hand over the accused to the victim state and be prosecuted as per the laws of the country of the victim. It is very tough to obtain a consensus on this issue from the different countries at the United Nations. Not all countries will be willing to handover their citizen, even if his guilt is produced beyond a reasonable doubt, to the laws of the victim's state.

There does exist the option of effecting extradition arrangements between two countries to decide up on a particular matter, but then the laws of the respective countries come in between as an obstacle. What is a crime in a particular jurisdiction may not be a crime as per the laws of the other country. This is a big problem which can be solved if there is a treaty entered into between the countries giving proper knowledge on the issue of jurisdiction. That is also another time consuming process, so the temporary to the problem may be changing and adding laws to the current domestic laws. For instance, in the IT Act, 2000 a new section may be inserted to ascertain the place of suing of the offender. It shall be mentioned in explicit terms that that offender can either be prosecuted as per the laws of that country from where the message was being sent to him or as per the country where the victim was or where he

[135] *Id.*at 131.

received the message. This would definitely help in solving cases where the accused and victim do not have the same nationality[136].

The above mentioned were some of the legal solutions to the problem. There can be some other non-legal ways too for the purpose of solving the problem. Firstly, all the people shall know how to regulate their own selves. Whenever a person wants to use the internet for the purpose of communicating on any social platform, then he shall create an e-mail address which does not indicate the sex of the person. The password for his account shall always be unusual and not predictable[137].

One shall not engage in uploading one's personal information on any social networking platform. All the private information shall always be kept private and one shall never engage in disclosing the same to complete strangers they happen to meet over the internet. Nowadays, children have started using these electronic devices much before their correct age use such gadgets. These children make e-mail accounts at a very young age. All this shall be monitored by their parents on a regular basis so that they are well informed about the activities of their child. The children shall be given proper guidance, including the positive as well the negative side of the internet[138]. Whenever a person is being cyber stalked, he should, in the first instance block the stalker so that he is not able to send the harassing messages. The victim can also try and change his own e-mail address, personal phone numbers etc. If the problem persists, the victim can try to get off all social networking platforms. If this option is no feasible, then he shall go and inform the matter to the police who will reduce it in the form of a formal complaint[139].

There shall be proper agencies for the purpose of educating the public at large thereby helping them protect themselves on their own. There are various governmental agencies that are already helping the people who extensively use the internet by educating them. A perfect example of such an agency is the U.S. Dept. of Justice has joined hands with ITAA for the purpose of educating the users of the internet about

---

[136] *Id.*

[137] Working to Halt Online Abuse, http://www.haltabuse.org/resources/online.shtml (Mar, 13, 2017, 17:15PM).

[138] Cyberangels, (Mar, 13, 2017, 17:30 PM) http://www.cyberangels.org/parents/childIDtheft.php.

[139] Available at, http://police.uncg.edu/information/pamphlet/Stalker/Stalker07-21-11.pdf (Mar, 13, 2017, 18:00PM).

the various crimes that may be committed on the internet. Through their joint effort, the had successfully, enacted an Act by the name of Cyber Partnership in the year 1999 for the sole reason of making the public infor0med in the cases of various crimes that may be committed on the internet[140].

Nowadays, lot of progress has been made in the improving the quality of the soft wares being invented. The newly discovered soft wares enable the receiver to destroy the messages or e-mails that he does not wish to receive from a particular person's email-ID. This is made possible by utilising certain internet tools[141]. In the case of children, where it is difficult for their parents to keep an eye on them all the time when they access the internet, new soft wares have been discovered that help the parents block access to certain adult websites and forums of discussion on the internet[142]. By resorting to these mechanisms would not help in solving the issue completely, but will provide some amount of relaxation in the area of regulating the crime of online stalking.

The role of the ISPs has also been crucial. They have made efforts to cater to threatening behaviour over the internet. These providers have made it possible for individuals to report behaviour which is harassing either straightaway to the provider, or any address as may be mentioned specifically to report harassing accounts. Such a provision is available on various social networking sites such as facebook[143] etc.

These ISPs have also created in-built mechanisms to send a specific harassing mail or messages received from a harassing account straightaway into the folder labelled as "spam folder".

The above legal as well as non-legal methods to solve the issue may work even more efficiently and effectively, if both of them go hand in hand. Whenever a case relating to online stalking is being reported, the same shall be investigated by the legal authorities with the continued and combined efforts of the ISPs.

---

[140] J. Reno, *Report on Cyber Stalking: A New Challenge for Law Enforcement and Industry*, United States Department of Justice, Feb. 18 2006, (Mar, 13, 2017, 10:00 AM) http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

[141] L. Ellison and Y. Akdeniz, *Cyber-stalking: the Regulation of Harassment on the Internet*, CRIM. L. REV. 29 (1998).

[142] http://www.netnanny.com/netnanny (Mar, 11, 2017, 10:00 AM).

[143] https://blog.facebook.com/blog.php?post=144628037130 (Mar, 11, 2017, 10:00 AM).

What we can do here is predict the possible future of the legal framework and advancements in the better regulation of the crime of cyber stalking. It is the legislators who need to open their eyes and see the various loopholes existing in the legislations today. They need to make continuous efforts to formulate such laws and policies that would solve the problem in totality by snapping it off right from its roots.

7. BIBLIOGRAPHY

ARTICLES USED:

- Amy C. Radosevich, Note, *Thwarting the Stalker: Are Anti-Stalking Measures Keeping Pace with Today's Stalkers?,* U. ILL. L. Rev. 1371, 1387 (2000).
- Debarati Halder, Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Lawsin India from Restorative Justice and Therapeutic Jurisprudential Perspectives.
- George F. du Pont, *The Criminalization of True Anonymity in Cyberspace,* 7 MICH. TELECOMM. & TECH. L. REv. 191, 196-216 (2000-2001).
- Harry Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, STAN. TECHNICAL L. Rev. 2, 54 (2004).
- JR Reidenberg, *Governing Networks and Cyberspace Rule-Making,* 45 EMORY L. J. 911 (1996).
- Louise Ellison, *Cyberstalking: Tackling Harassment on the Internet*, (David S. Wall ed., 2001).
- MG Mcgrath and E Casey, *Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace*, 30(1) J. AM. ACADEMY PSCYCHIATRY & L. 81 (2002).
- Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 Mo. L. Rev. 125 (2007).
- Neal Kumar Katyal, *Criminal Law in Cyberspace,* U. PA. L. Rev. 1003 (2001).
- P. Bocij, *Reactive Stalking: A New Perspective on Victimization*, 7(1) BRITISH J. FORENSIC PRACTICE 23 (2005).
- P. Duggal, *India"s first Cyberstalking Case- Some Cyberlaw Perspectives*, (Mar, 10, 2017, 12:01 PM) http://cyberlaws.net/cyberindia/2CYBER27.htm.
- R. Wacks, *Privacy in Cyberspace: Personal Information, Free Speech and the Internet in PRIVACY AND LOYALTY*, 93 (P. BIRKS ED., 1997).
- Renee L. *Servance, Cyberbullying, Cyber-Harassment, and the Conflict Between Schools and the First Amendment*, 2003 Wis. L. REV. 1213, 1215 (2003).
- Ridhi Kabra ,*Cyberstalking: One Problem Control-Alt-Delete Can't Solve*, 2008-35, Vth Year BA LLB Hons.

- Sarah R. Gitomer, *Cyberstalking: A New Phenomenon, United States v. Sayer*, No. 2:11–cr–113–DBH, 2012 WL 2180577 (D. Me. Jun. 13, 2012).
- S. Greenberg, Threats, *Harassment and Hate On-line: Recent Developments*, 6 BOSTON PUBLIC INTEREST J. 673 (1997).
- S. Vadehra, Kan and Krishme, *Data Protection and the IT Act India*, (Ma, 11, 2017, 12:00PM)
- Steven D. Hazelwood & Sarah Koon-Magnin, *Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis*,7 IJCC 155, 155-156 (2013).

NEWSPAPER ARTICLES CITED:

- Associated Press, *E-mail stalker sentencing likely will influence future cases*, THE DETROIT NEWS HOME PAGE, Mar 23, 1996.
- Hendren J, *Online harassment bill gains momentum*, LOS ANGELES TIMES, May 25, 1997 at E4.
- Hua T, *Ex-student sentenced for hate e-mai*, LOS ANGELES TIMES, May 5, 1998, p A24.
- Lewis PH, *Persistent e-mail: electronic stalking or innocent courtship?*, NEW YORK TIMES, Sept 16, 1994, p Bl1
- Maharaj D, *U.S. to retry man in hate e-mail case*, LOS ANGELES TIMES, Dec 2, 1997 at p A3.
- McFadden RD, *Suspect in New Jersey strangling was reportedly sex-case victim*, N.Y. TIMES, Oct 3, 1997 at p A1.
- Whitelaw K, *Fear and dread in cyberspace*, US, WORLD & NEWS REPORT, 121 (1 8):50, 1996.
- http://www.telegraph.co.uk/news/uknews/crime/10866262/Cyber-stalker-bugged-womens-computers-to-spy-on-them-in-their-bedrooms.html, (Mar, 13, 2017, 19:05PM).

LEGISLATIONS CITED:

- California Penal Code.
- Code of Civil Procedure, 1908. (India)
- Communications Act, 2003 (UK).
- Communications Convergence Bill, 2001.
- Computer Misuse Act, 1990. (UK)
- Constitution of India.
- Constitution of USA.
- Criminal Justice Act, 2003 (UK).
- Criminal Justice & Public Order Act, 1994.(UK)
- Federal Telephone Harassment Act, 47 U.S.C. §223.
- Indian Evidence Act, 1872.
- Indian Penal Code, 1860.
- Information Technology Act, 2000 (India).
- Interstate Communications Act, 18 U.S.C. §875(c).
- Interstate Stalking Punishment and Prevention Act, 18 U.S.C. §2261A.
- Malicious Communications Act, 1988 (UK).
- Michigan Criminal Code.
- Specific Relief Act, 1963. (India)
- Protection from Harassment Act, 1997 (UK).
- Protection of Children from Sexual Offences Act, 2012. (India).
- Telecommunications Act, 1984 (UK).
- The Offences Against the Person Act, 1861. (UK)
- 18 U.S. Code § 2425.

WEBSITES CITED:

- https://blog.facebook.com/blog.php?post=144628037130 (Mar, 11, 2017, 10:00 AM).
- http://caselaw.findlaw.com/us-1st-circuit/1665132.html
- Crown Prosecution Service, (Mar, 4, 2017, 12:30 PM), www.cps.gov.uk/ legal/s_to_u/stalking_and_harassment/.

- Cyberangels, (Mar, 13, 2017, 17:30 PM) http://www.cyberangels.org/parents/childIDtheft.php.
- *Cyber Security and Related Issues: Comprehensive Coverage,* (Mar, 4, 2017, 20:08 PM),http://www.insightsonindia.com/2014/11/25/cyber-security-related-issues comprehensive-coverage/
- http://cyberstalking.web.unc.edu/caselaw/, (Mar, 5, 2017, 21:01PM).
- http://www.delawareonline.com/story/news/local/2015/07/10/jury-finds-matusiewiczes-guilty/29960471/, (Mar 5, 2017, 14:00 PM).
- http://www.jsonline.com/story/news/crime/2016/02/12/emergency-sentencing-today-hospital-lenore-matusiewicz/80299490/, (Mar,7.2017,14:01PM).
- Joel Best, *Stalking*, (Mar, 3, 2017, 7:02PM), https://www.britannica.com/topic/stalking-crime.
- Joint Publication 1–02, DOD Dictionary of Military and Related Terms (Washington, DC: The Joint Staff, dated April 12, 2001, and amended through November 9, 2006), www.dtic.mil/doctrine/jel/new_pubs/jpl_02.pdf.
- http://www.mirror.co.uk/news/uk-news/andrew-meldrum-peeping-tom-rigged-3204007, (Mar 13, 2017, 19:00PM).
- Michigan Criminal Code, Stalking: Section 28.643(8), definitions. 1993 section 411h, (Mar, 4, 2017, 11:00 AM), www.haltabuse.org/resources/laws/michigan.shtm.
- N.Y. State Assembly. (N.Y. 2006), Available at http://assembly.state.ny.us/leg/?bn=A06016.
- http://police.uncg.edu/information/pamphlet/Stalker/Stalker07-21-11.pdf (Mar, 13, 2017, 18:00PM).
- *Sexual Assault Prevention And Awareness Center*, (Mar, 4, 2017, 11:00 AM), https://sapac.umich.edu/article/320.
- U.S. Dept. of Justice, *Stalking and Domestic Violence:Report to Congress* 1 (May 2001), Available at http://www.ncjrs.org/pdffilesl/ojp/186157.pdf.
- U.S. Dept. of Justice, *A Report on Cyberstalking: A new challenge for law enforcement and industry (Aug. 1999)*, Available at:

http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm; (Accessed 3/3/17).

- Working to Halt Online Abuse, http://www.haltabuse.org/resources/online.shtml (Mar, 13, 2017, 17:15PM).