International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

Cyber Stalking Threat to Networking & Legal Issues in Indian Cyber Law

Amit K Kashyap[1]

[1] Asst. Prof of Law, Institute of Law, Nirma University, Ahmedabad (#7600377946/ amit1law@gmail.com)

ABSTRACT

'Vasudhaiva Kutumbakam' an Indian philosophy has become International with social media by bringing the world closer & acting as a bridge for sharing sentiments. Although issues such as privacy and cyber-stalking seem to affect its largely positive reputation, yet the usefulness of networking easily dwarfs the fears surrounding its worthiness. Through this paper the researcher will try to study the problem of cyber stalking the laws relating to surrounding networking while analysing the legal provision providing for privacy rights of victims.

Keyword's: Cyber Stalking, Stalker, Cyber Crime, privacy, Information Technology Act, Indian Penal Code

INTRODUCTION

The advent of the third millennium has brought in an era of information society. The new era is the result of rapid changes brought about by the new technology and the cyber world. Obviously the information society offers vast scope and opportunities to human beings to identify information, to evaluate information, and to exchange information for the benefits of the citizens the world over. The information technology provides for a new environment, new work culture, new business links and trading networks. It allows information and knowledge based work to be located anywhere. It is virtually transforming and revolutionizing the world. The internet is a worldwide network of computers that share a common communication protocol which was initially conceived (as Fishnet and later ARPANET) by the US Military to communicate in the event of a nuclear attack. In 1989, Berners-Lee created the World Wide Web so as serve as a worldwide online store of knowledge but it has now been transformed into an infrastructure for providing commercial services.[2] To this end domain names are relied upon convenience.

A domain name is divided into two – numeric, also called an IP address, for instance 123.743.123.58, where "123" is the network, "743" and "123" are the sub-networks, and "58" is a specific computer and alpha numeric or domain name (www.nike.com). Browsers such as Internet Explorer automatically look up the numeric IP address that corresponds to the designated alphanumeric address primarily because numeric addresses are harder to remember and programming has come to replace the flaws of memory. It is for this reason that domain names have come to replace numeric addresses. **Moreover, domain names today have become business identifiers which signify the association of a particular web page and the information stated therein to the alphanumeric variable used.**[3]

[1] Asst. Prof of Law, Institute of Law, Nirma University, Ahmedabad (#7600377946/amit1law@gmail.com)

[2] V. K. Unni, *Trademarks and the Emerging Concepts of Cyber Property Rights* (2002), 15 [hereinafter UNNI]; *See also* Barry M. Leiner, et. al., "A Brief History of the Internet," *accessed on October 24, 2006* http://www.isoc.org/intenet-history/brief

[3] This has led to a substantial increase in the registration of domain names. As of October 29, 1998, the weekly growth rate of domain name registration was 74,087, and the number of registered domain names totaled over four million. Between October 28 and October 29, 1998, alone, over seven-thousand

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

The information technology is a double-edged sword, consistently presenting us with benefits and disadvantages. The increasing opportunities for productivities, efficiency and worldwide communications brought additional users in droves[4]. Today, the internet is a utility, analogous to the electric company and '.com' has become a household expression. The reliability and availability of the internet are critical operational considerations. Activities that threaten these attributes like spamming, spoofing, etc, have grave impacts on its user community. Any illegal act, for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution, is known as **cybercrime**.

Among the various problems emerging out of the internet are the menace of **hackers, cyber terrorism, spamming, Trojan horse attacks, denial of service attacks, pornography, cyber stalking etc.**

Anecdotal evidence suggests the majority of cyberstalking victims are women and perpetrators are men, although same - sex and female to male cyberstalking do occur. As with other forms of stalking, the victim and perpetrator often know each other, the stalking may begin after the relationship has ended and online threats and harassment can lead to more serious behaviours including violence.[5]

CYBER STAKING & CYBER STALKER

Cyber stalking, has been defined as the use of electronic communication including, pagers, cell phones, emails and the internet, to bully, threaten, harass, and intimidate a victim. Moreover, it can also be defined as nothing less than emotional terrorism.[6]

Cyber stalking can take many forms'. However, Ellison (1999) suggests, cyber stalking can be classified by the type of electronic communication used to stalk the victim and the extent to which the communication is private or public. Ellison (1999) has classified cyber stalking as either 'direct' or 'indirect'. For example, 'direct' cyber stalking includes the use of pagers, cell phones and the email to send messages of hate, obscenities and threats, to intimidate a victim. Direct cyber stalking has been reported to be the most common form of cyber stalking with a close resemblance to offline stalking (Wallace, 2000).

Generally, to be defined as stalking the behaviour must be unwanted and intrusive. Another important point is that the stalker must also have an intense preoccupation with the victim. The range of behaviour involved in stalking can be broadly grouped in three categories.

Firstly, there is following, which includes frequenting workplaces and homes, maintaining surveillance, and engineering "coincidences."

Secondly, there is communicating—by phone, letters, cards, graffiti, gifts, and, Increasingly, electronic mail and the internet ("cyber stalking").Often the stalker will order goods and services on the victim's behalf.

Finally comes aggression or violence, in which stalkers threaten their victims, harass their families, damage their property, make false accusations about them, and cause sexual or physical injury.

".com" domain names were registered. *See* John M. Tanner & Timothy W. Gordon, "The Interrelationship of Trademark & Internet Law: Protecting Trademarks," *Dispute Resolution*, accessed on October 27, 2004, http://www.fwlaw.com/tradeint.html

[4] .Mishra,RC , " Cybercrime: impact in the new millennium", 2002 ed., p.53

[5] Available at: http://naplesshelter.org/wp-content/uploads/2014/09/cyberstalking.pdf

[6] Laughren, J, CYBERSTALKING AWARENESS AND EDUCATION. Available on – http://www.acs.ucalgary.ca/~dabrent/380/webproj/jessica.html, last visited on (02-11-2007)

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

Sexual attractions and motives are other very important reasons for cyberstalking. In USA, the federal law enforcement agencies have encountered numerous instances in which adult paedophiles have made contact with minors through online chat rooms, established a relationship with the child, and later made contact for the purpose of engaging in criminal sexual activities.[7]

Considering the fact that the quantum of e-commerce had grown substantially over the years the association was of the opinion that the lack of a legislation to prevent cybersquatting could cause a substantial dent to e-commerce and therefore wanted to evolve a mechanism which limited customer confusion in cyberspace, protected the investment of trademark owners and maintained the goodwill associated with such trademarks. The call therefore was for an Act which while prohibiting acts of cybersquatting permitted for use which in legitimate exercise of the freedom of expression. All of these concerns have been incorporated into the Anti-cybersquatting Consumer Protection Act, 1999 which makes an act of cybersquatting illegal if committed in bad faith

CYBER STAKING: NATURE & APPROACHES

The nature of cyber stalking is ascertains by the medium which is used for its execution.

According to … cyber stalking had been classified into four kinds[8]

a) E-mail stalking
b) Chat stalking
c) Bulletin board systems
d) Computer stalking.

Email stalking

Electronic mail is an electronic postal service that allows individuals to send and receive information in matter of seconds. This sophisticated use of telephone lines allows communication between two people who may or may not know each other but can 'speak' to each other using a computer. In general Email is an insecure method of transmitting information or messages. Everyone who receives an email from a person has access to that persons email id. With some online services as AOL, a person's screen name is also an email address. In addition, when a person posts an item on a newsgroup, that peson's email id may be available to anyone who reads that item. It is unsurprising, then, that email is a favoured medium for cyber stalkers.

Technologically sophisticated email harassers send 'mail bombs', filling a persons inbox with hundreds or even thousands of unwanted mails in the hope of making the account useless. Others send electronic viruses that can infect the victim's files.[9]

Chat stalking

A chat room is a connection provided by online services and available on the internet that allows people to communicate in real time via computer text and modem. Cyber stalkers can use chat rooms to slander and endanger their victims. In such cases the Cyber stalking takes on a public rather than a private dimension. As live chat has become more popular amongst users of the internet with tools such as internet relay chat (IRC), it has also become more popular as a medium through which stalkers can identify and pursue their prey.

When a person enters a chat room, his screen name joins the list of names of others in the group. Depending on the nature of the chat software, that person can address others in the room and vise versa as a part of the group discussing from a smaller group in a private

[7] Mishra,RC , CYBER CRIME: IMPACT IN THE NEW MILLENNIUM, 2002 ed., p.54

[8] Jewkeys, Yuonne (ed.), DOT.COMS CRIME, DEVIENCE AND IDENTITY, THEFT ON THE INTERNET,,p.108

[9] Ogilvie, E. (2000).Cyberstalking., TRENDS AND ISSUES IN CRIME AND CRIMINAL JUSTICE, 166. Available at http://www.aic.gov.au

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

chat room or send private, one to one instant messages to others anytime.[10] During 'chat', participants type instant messages directly to the computer screens of other participants.

When a person posts a message to a public news group this is available for anyone to view copy and store. In addition, a persons name, email address and information about the service provider are easily available for inspection as a part of the message itself. Thus, on the internet, public messages can be accessed by anyone anytime- even years after the message were originally written. In IRC, the harasser may chose to interrupt a person's chat electronically or otherwise target a chat system, making it impossible for someone to carry on a conversation with anyone else. The Cyberstalker can engage in live chat harassment or abuse of the victim(otherwise known as 'flaming') or he/she may leave improper message o the message board or in chat rooms for or about the victim.

Bulletin board systems

A bulletin board system (BBS) is a local computer that can be called directly with a modem[11]. Usually they are privately operated and offer various services depending on the owner and the users. A bulletin board allows leaving messages in group forums to be read at a later time. Often a BBS is not connected to a network of other computers, but increasingly BBSs are offering internet access and co Cyber stalkers area using bulletin boards to harass their victims.[12]

Online have been known to known to post insulting messages on electronic bulletin boards signed with email addresses of the person being harassed. The Cyber stalker can also post statements about the victims or start rumours which spread through the BBS. In addition a Cyber stalker can 'dupe' another internet users into harassing or threatening a victim by posting a controversial or enticing message on the board under the name , phone numbers or email address of the victim, resulting in subsequent responses being sent to the victim.[13]

Computer stalking

With computer stalking, cyber stalker exploits the internet and the windows operating system in order to assume control over the computer of the targeted victim. An individual 'windows based' computer connected to the internet can be identified, allowing the online stalker to exercise control over the computer of the victim. A cyber stalker can communicate directly with his or her target as soon as the target computer connects to the internet. The stalker can also assume control over the victim's computer and the only defensive option for the victim is to disconnect and relinquish his or her current internet address.[14]

An example of this kind of cyber stalking was the case of a woman who received a message stating ' I'm going to get you'. The cyber stalker then opened the woman's CD-ROM drive in order to prove that he had control over her computer.

CYBERSTALKING TRENDS AND STATISTICS

Offenders

Previous studies that have investigated stalking offenders by and large, have focused on the offline stalking offender

Regardless for the offenders group such as 'simple', 'love' or 'erotomanic' statistics reports, male offenders to account for the majority of offline stalking offenders. Working to Halt Online Abuse (2000) statistics also support the gender ratio of

[10] Jewkeys, Yuonne (ed.), DOT.COMS CRIME, DEVIENCE AND IDENTITY, THEFT ON THE INTERNET,,p.109

[11] Jewkeys, Yuonne (ed.), DOT.COMS CRIME, DEVIENCE AND IDENTITY, THEFT ON THE INTERNET ,p.109

[12] id

[13] id at p.110

[14] id at p.110

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

offenders claiming, 68% of online harassers/cyber stalkers are male.

Furthermore, common social and psychological factors have been found within offline stalking offender population. For example, social factors such as the diversity in socio-economic backgrounds and either underemployment or unemployment have been found significant factors in offline stalking offenders[15].

In a research done on young stalkers between 9 and 18 years of age little difference was found between young and adult offline stalking offenders. For example, the majority of offenders were male, had some form of previous relationship with the victim and experienced social isolation.[16]

Victims

Currently, there are limited studies on the victims of cyber stalking. Although, anyone has the potential to become a victim of offline stalking or cyber stalking, several factors can increase the statistical likelihood of becoming a victim. Studies[17] that have investigated offenders of offline stalking, have found some common factors within the selection of victims. For example, contrary to public belief, a large proportion of stalking victims are regular people rather than the rich and famous.

Goode claimed[18], up to 80% of offline stalking victims are from average socio-economic backgrounds. In addition, the statistical likelihood of becoming a victim increases with gender.

Working to Halt Online Abuse (2000) reports, 87% of online harassment/cyber stalking victims are female. However, victim gender statistics may not represent true victims, as females are more likely to report being a victim of online harassment/cyber stalking than males.

Although studies have shown that the majority of victims are female of average socio-economic status, studies have also shown that offline stalking is primarily a crime against young people, with most victims between the age of 18 and 29.[19] Stalking as a crime against young people may account for the high prevalence of cyber stalking victims within universities. For example, the University of Cincinnati study showed, 25% of college women had been cyber stalked.[20].

Nevertheless, previous relationships have been shown to increase the likelihood of being stalked offline. For example, it was reported, 65% offline victims had a previous relationship with the stalker[21]. Although studies of offline stalking claim the majority of victims have had a previous relationship with the stalker

Working to Halt Online Abuse Statistics[22]

---

[15] Meloy, J.R. & Gothard, S.). DEMOGRAPHIC AND CLINICAL COMPARISON OF OBSESSIONAL FOLLOWERS AND OFFENDERS WITH MENTAL DISORDERS. American Journal of Psychiatry, 152(2), 1995 ed., 258-26

[16] McCann, J.T. (2000). A DESCRIPTIVE STUDY OF CHILD AND ADOLESCENT OBSESSIONAL FOLLOWERS. Journal of Forensic Sciences, 45(1), p.195-99

[17] Sinwelski, S.A. & Vinton, L. ,STALKING: THE CONSTANT THREAT OF VIOLENCE. AFFILIA: THOUSAND OAKS 2001 ed..

[18] Goode, M., STALKING: CRIME OF THE NINETIES?., Criminal Law Journal, 19, 1995, p.21-31.

[19] Brownstein, A. (2000). IN THE CAMPUS SHADOWS, WOMEN ARE STALKERS AS WELL AS THE STALKED, The Chronicle of Higher Education, 47(15),2002 ed., 40-42.

[20] Tjaden, P. & Thoennes, N. (1997). STALKING IN AMERICA: FINDINGS FROM THE NATIONAL VIOLENCE AGAINST WOMEN SURVEY. National Institute of Justice and Centres for Disease Control and Prevention. Washington DC. Available at http://www.ncjrs.org

[21] Zona, M.A., Sharma, K.K. & Lone, J. "A COMPARATIVE STUDY OF EROTOMANIC AND OBSESSIONAL SUBJECTS IN A FORENSIC SAMPLE", Journal of Forensic Sciences, 1993 ed. 38,p. 894-903.

[22] For more details refer to - http://www.haltabuse.org/resources/stats/relation.shtml

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

fails to support a previous relationship as a significant risk factor, for online harassment/cyber stalking. For example, 53% of victims had no prior relationship with the offender. Therefore, the risk factor of a prior relationship with the stalker may not be as an important factor in cyber stalking, as it is in offline stalking.

PSYCHOLOGICAL EFFECTS OF CYBERSTALKING

Currently, there are few studies on the psychological impact on victims. However, Westrup[23] studied the psychological effects of 232 female offline stalking victims. He found out that the majority of victims had symptoms of PTSD, depression, anxiety and experienced panic attacks.

Additionally, it was found that 20% of victims increased alcohol consumption and 74% of victims suffered sleep disturbances[24]. Nevertheless, social and psychological effects of offline stalking cannot be separated as social effects can impact on psychological effects and psychological effects can impact on the social effects. Although the majority of studies have focused on the offline stalking victims, there is no evidence to suggest that cyber stalking is any less of an experience than offline stalking (Minister for Justice and Customs, 2000), As shown, there are many common themes between offline stalking and cyber stalking.

For example, offenders are most likely to be male and offline stalking or cyber stalking is the response to a failed (offline/online) relationship. Additionally, young females account for the majority of victims. Furthermore, victims experience significant social and psychological effects from offline stalking or cyber stalking.[25]

CYBERSTALKING & CYBER LAW

Cyber stalking is are a relatively new phenomenon and many countries are only now beginning to address the problem. India has also witnessed cases of cyber stalking, cyber harassment and cyber defamation. However, as there is no specific law or provision under the IT Act, a number of these cases are either not registered or are registered under the existing provisions of Indian Penal Code—which are ineffective and do not cover the said cybercrimes.[26]

Since its promulgation, the IT Act 2000 has undergone some changes. One big change is the recognition of electronic documents as evidence in a court of law. Market players believe this will go a long way in giving encouragement to electronic fund transfers and promoting electronic commerce in the country. On these line some provisions has been amended and added by amendment of Information Technology Act in 2008.

Section 72 of the Indian Information Technology (Amendment) Act, 2008 which deals with breach of confidentiality and privacy which provides that the person who is passion of other persons information which includes electronic record, book, register, correspondence, information, document or other material, if disclose it to any other person without the consent of the person concerned shall be punishable. Further, section 72A of the said Act which prescribes punishment for disclosure of information for breach of lawful contract read with section 441 and 509 of the Indian Penal Code which

[23] Westrup, D., Fremouw, W.J., Thompson, R.N. & Lewis, S.F. THE PSYCHOLOGICAL IMPACT OF STALKING IN FEMALE UNDERGRADUATES. Journal of Forensic Sciences, (1999), 44(3), pp.554-557.

[24] Mullen, P.E. & Pathe, M. (1997). THE IMPACT OF STALKERS ON THEIR VICTIMS. British Journal of Psychiatry,",pp. 12-17.

[25] http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

[26] Keane Insight, WHAT'S WRONG WITH OUR CYBER LAWS? , Avaliable on – (http://www.expresscomputeronline.com/20040705/newsanalysis01.shtml)

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

deal with offences related to Criminal trespass and acts intended to insult the modesty of a woman respectively. The provisions under section 441 & 509 of IPC were being used to prosecute offenders for cyber stalking before coming into force of the Criminal Law Amendment Act, 2013. Cyber Stalking is also recognised via section 66A of IT Act 2000 which provides punishment for sending offensive messages through communication service.

Now such offensive activities are to be dealt with by Section 354D of the Indian Penal Code, (added by the Criminal Law Amendment Act, 2013 with effect from 3rd February, 2013) which specifically makes provision for prosecuting the perpetrator of cyber stalking with harsher punishment. [27] These provisions criminalise sexual voyeurism and stalking and would amend legal provisions to protect the privacy of individuals, such as discontinuing the practice of examination of the sexual history of the victim of a sexual assault for evidence.[28] The provision of new amendment hase removed lot of difficulties which police was facing while registering a case. Now, the new law disregard the reason or intent for the behaviour, and undoubtedly defining the elements of the offence and making stalking as a stand-alone offence.

It can be interpreted as, A man can monitor a woman's use of the internet all he wants, but to attract a charge of stalking, the woman has to show that it results in a fear of violence or serious alarm or distress in the woman's mind or interferes with her mental peace. Moreover, the monitoring must be of private content only. If a woman posts content on Facebook, Twitter or other social media platforms which, by their very nature, are public platforms, she allows her content and communication on such public platforms to be reviewed or read (i.e. "monitored"). Such use by the woman of the internet which becomes public due to the nature of the platform must be excluded. [29]

CONCLUSION

Cyber Stalking generally involves 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 online & in majority of case stalkers are men's & victims are women's. Stalking generally involves harassing or threatening behavior that an individual engages in repeated. However, The Information Technology Act 2000 does not cover cyber stalking and the Indian Penal Code 1860 does not have a specific provision that could help victims of cyber stalking but now the amendment in Information Technology Act in 2008 & other amendment in IPC in 2013 has provided for clear provision as to make cyber stalking a crime & punishable with severe punishment.

REFERENCES

[1.] Brownstein, A. (2000). In the Campus Shadows, Women are Stalkers as well as the Stalked, The Chronicle of Higher Education, 47(15), 2002 ed.

[2.] Charles, Computer Bulletin Boards and Defamation; Who Should be Liable and under What Standard' 2 Jl. and Tech

[3.] Cuterrca, Computer Network. Libel and the First Amendment, Computer Law Journal.

[27] Available at: http://www.haltabuse.org/resources/laws/india.shtml

[28] Available at: http://cis-india.org/internet-governance/blog/the-criminal-law-amendment-bill-2013

[29] Available at: http://www.firstpost.com/india/the-anti-rape-bill-and-its-problematic-definition-of-stalking-671184.html

[4.] Devashish Bharuka, Indian information technology Act, 2000: Criminal Prosecution made easy for Cyber Psychos , (Vol. 42, 2002), Journal of India Law Institute, New Delhi

[5.] Eugene R. Quinn, Jr., The evolution of Internet Jurisdiction: What a long strange trip it has been, Syracuse Law and Technology Journal, Spring, 2000: www.westlaw.com

[6.] Farooq Ahmed, Challenges of the information technology to the existing legal regime: Common law principles No more Panacea ,
(Vol. 46, 2004), Journal of India Law Institute, New Delhi.

[7.] Goode, M., Stalking: Crime of the Nineties. Criminal Law Journal, 19, 1995.

[8.] Gopika Vaidya-Kapoor, Byte by Byte. available on the website - http://www.rediff.com/netguide/2003/feb/18crime.htm

[9.] Hardy, "The Proper Legal Regime For Cyber Space" 55 Utah L Rev 993

[10.] Jewkeys, Yuonne (ed.), Dot.coms Crime, devience and identity, theft on the internet
Jim Puzzanghera, US lawmakers clamouring to regulate Internet, San Jos Mercury News 9th Apr 1999 available online from Lexis-Nexis.

[11.] Keane Insight, What's wrong with our cyber laws? , Avaliable on – (http://www.expresscomputeronline.com/20040705/newsanalysis01.shtml)

[12.] Laughren, J, Cyberstalking Awareness and Education , Available on – http://www.acs.ucalgary.ca/~dabrent/380/webproj/jessica.html, last visited on (02-11-2007)

[13.] McCann, J.T. (2000). A Descriptive Study of Child and Adolescent Obsessional Followers. Journal of Forensic Sciences.

[14.] Meloy, J.R. & Gothard, S.). Demographic and Clinical Comparison of Obsessional Followers and Offenders with Mental Disorders. American Journal of Psychiatry.

[15.] Mullen, P.E. & Pathe, M. (1997). The Impact of Stalkers on their Victims. British Journal of Psychiatry.

[16.] Murdock, "The Use and Abuse of Computerized In format ion" 44 ALB L Rev 589-619 (1980).

[17.] Ogilvie, E. (2000).Cyber Stalking, Trends and Issues in Crime and Criminal Justice, 166. Available at http://www.aic.gov.au

[18.] Sinwelski, S.A. & Vinton, L. ,Stalking: The constant threat of violence. Affilia: Thousand Oaks 2001 ed.

[19.] Stephanie Blumstein, The New Immunity in Cyber Space: The Expanded Reach of Communications Decency Act to the Libelous " Reposter", Boston university Journal of Science and Technology law, Summer 2003; www.westlaw.com
Suzi Seawell (et al), Cyber Defamation: Same old story or brave new world? : http://gsulaw.gsu.edu/lawand/papers/su98/defamation

[20.] Tim Ludbrook, Defamation and the Internet- Where we are and where we are going, Entertainment Law Review, 2000: www.westlaw.com

[21.] Tjaden, P. & Thoennes, N. (1997). Stalking in America: findings from the National Violence Against Women Survey. National Institute of Justice and Centres for Disease Control and Prevention. Washington DC. Available at http://www.ncjrs.org

[22.] Vipin V. Nair, Dark deeds remain in the dark, available on the website-(http://www.thehindubusinessline.com/ew/2003/09/10/stories/2003091000080100.htm)

[23.] Westrup, D., Fremouw, W.J., Thompson, R.N. & Lewis, S.F. The Psychological Impact of Stalking in Female Undergraduates. Journal of Forensic Sciences, (1999).

[24.] Yatinder Singh, cyber crime ,(Vol. 44, 2002), Journal of India Law Institute, New Delhi
Zona, M.A., Sharma, K.K. & Lone, J. "A Comparative Study of Erotomanic and Obsessional Subjects in a Forensic Sample", Journal of Forensic Sciences, 1993 ed.

Books referred

- Charlotte Waelde and Lilian Edwards (Ed.), law and the internet-a framework for electronic commerce, (2nd ed., 2000), Hart Publishing, Oxford
- Chris Reed (Ed.), computer law, (5th ed., 2000), Blackstone Press, London
- Gerald R. Ferrera (et al), cyber law-text and cases, (2nd ed.) Thomson south –western west, USA
- Graham J H Smith, internet law and regulation, (3rd ed. 2002), Sweet and Maxwell, London
- Rodney D. Rider, guide to cyber laws, (2nd ed. 2003), Wadhwa and Co., Nagpur
- Sallie Spilsbury, media law, 2000, Cavendish Publishing, London.

Legislations used

- Information technology act, 2000.
- Indian Constitution
- Indian Penal Code, 1872.