TEMIDA
Septembar 2009, str. 5-26
ISSN: 1450-6637
DOI: 10.2298/TEM0903005H

Cyber Socializing and Victimization of Women

Debarati Halder*
Karuppannan Jaishankar

Web 2.0[1] has redefined the virtual life of ordinary individuals and has given wide opportunities to internet users including women to exchange ideas, interact with like minded people and participate in the development of virtual societies as per one's own choices. Social networking websites (SNWs), a segment of Web 2.0 is very popular among the internet users. However, there is a dark side of these SNW's too. They have become havens for offenders to victimize women, the most vulnerable targets in the internet, after children.

In this paper, we examine the victimization of women in the social networking websites in general, analyze the trends of such victimization from socio – legal – victimological angle and ascertain the reasons for the growth of such victimization.

Key words: *cyber socializing, social networking, women, victimization*

[*] Debarati Halder is Managing Director, Centre for Cyber Victim Counselling, #28, SBO Colony, Maharaja Nagar, Tirunelveli, Tamil Nadu, India; Ph.D Candidate, National Law School of India University, Bangalore, India Email: ccvcindia@gmail.com URLs: http://www.cybervictims.edu.tf http://www.debaratihalder.co.nr

Karuppannan Jaishankar is Commonwealth Fellow, School of Law, University of Leeds, UK; Assistant Professor (Senior), Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India; Editor-in-Chief – International Journal of Cyber Criminology; Executive Director, Centre for Cyber Victim Counselling, India. Email: drjaishankar@gmail.com URL: http://www.drjaishankar.co.nr

[1] Web 2.0 is a concept which refers to "as a second generation of web development and web design. It is characterised as facilitating communication", http://en.wikipedia.org/wiki/WEB2.0 (accessed May 28, 2009). According to Tom O'Reilly, one of the first proponent of the concept of Web 2.0, the concept can be "visualized" as "a set of principles and practices that tie together a veritable solar system of sites that demonstrate some or all of those principles, at a varying distance from that core", http://oreilly.com/pub/a/web2/archive/what-is-web-20.html (accessed May 28, 2009).

Introduction

Socialization through social networking websites (SNWs) has become a favorite hobby for "gizmo freaks",[2] self supporting, educated, independent, modern women of the 21st Century. The social networking websites help users make new "virtual friends" and offer "promise" to reunite with old friends and relatives. Most women users avail this new way of socialization as a stress – reliever. Cyber socializing through SNWs help women users to share with like minded friends, their emotional needs, personal problems, culinary skills, tips for child care and health care including pregnancy and post pregnancy issues. These women users discuss these "needs", tips and even their "mood swings" with their virtual friends who become "emotional comfort zones" for them either by writing on walls of some group/community forums or on the walls of their friend's profiles. Fraim defines cyber socialization as the *"computerized interaction with known or unknown individuals for the purpose of research, entertainment, establishment of friendships or relationships due to feelings of loneliness, and sexual gratification"* (Fraim, 2006). Internet socializing is *"electronic interaction"* (Fraim, 2006) with virtual friends through chat rooms, emails, forums (created by domain hosts like Google, Yahoo, etc) and social networking websites.

Even though social networking websites have opened a wide window for socializing, they have also opened flood gate for various crimes against women in the cyber space. It is unfortunate that even though European Union (EU) conventions on cyber crimes established strict rules to control content related offences, child pornography and identity theft related offences for securing e-commerce have proliferated.

The draftsmen as well as the world leaders who are parties to the EU conventions, never considered victimization of women in the cyber space as a big issue like child pornography or hacking. Women victims therefore remained as a secondary concern for all developed cyber savvy nations. This lacuna reflects very much in the growing crime incidences targeting women in the SNWs. On going psychological and legal researches on perilous cyber behaviors and its after effects established that SNWs raise more dangers than the traditional internet chat rooms (Clemmit, 2006) which literally give women a "chilling effect" (Citron, 2009). These crimes do not limit themselves in the

[2] A person who loves to use many contemporary gadgets like computers, ipods, mobile phones etc.

traditional concepts of cyber crimes like hacking, pornography, stalking or hate crimes only. They can shape up in to various traditional yet new forms of cyber crimes against women which await a deeper study.

This article discusses the victimizing effect of a typical segment of Web 2.0, namely, social networking websites (SNWs) on women netizens.[3] This paper is limited to victimization of women in the cyber social networking websites and does not cover victimization in other cyber socializing tools like emails, blogs, online chatting etc, even though we agree that victimization in SNWs will also attract victimization in other cyber socializing components.

The paper is presented in four parts. The 1st part discusses about cyber socializing, the growth of hi-tech crimes targeting women members in the SNWs and the need for conceptualizing such offences. The 2nd part sets out the typology and pattern of victimization of women users in the SNWs. The 3rd part discusses about the emotional and physical risk factors of the women users of SNWs due to the offences generating from cyber socializing. The 4th part establishes reasons for the victimization of women members of the SNWs and the growth of it.

Cyber socializing and the growth of hi-tech crimes

Cyber socializing dates back to mid seventies when email was invented. Even though mainly used for scientific and academic interactions (Clemmit, 2006), usage of emails and internet communications for commercial interactions and personal conversations as well as chatting gained tremendous popularity within no time. The traditional internet chat rooms can be divided into two categories, a) chat room for normal interactions, b) chat rooms used solely for sexual purposes where users could log on and enjoy either "sex chat" with single partner or "group sex chat" with more than two users. Some chat rooms also show pornographic pictures. However, these chat rooms never reveal individual's private information publicly. Even though

[3] The word "netizens" was coined by Michael Hauben. Netizens are internet users who "engage in activities of extended social groups, such as giving and receiving viewpoints, furnishing information, fostering the Internet as an intellectual and a social resource, and making choices for the self-assembled communities", http://en.wikipedia.org/w/index.php?title=Netizen&oldid=313547527 (accessed May, 2009).

these sex-chats earlier attracted teens and young adults, soon it started to loose its attraction (Clemmit, 2006).

Adult internet has a sexual as well as non sexual entertainment (Morahan-Martin, 2000) started getting popularity challenges from the social networking websites where communication became more transparent. In the SNWs users could create their own "profiles" providing their names, residences, schooling and college information, likes and dislikes to "find new friends" or "to relocate long lost friends". These social networking websites were able to attract teens and women as they felt the danger of unknown sexual predator or problems of privacy could be lesser here. But mostly they remained oblivious of the fact that their identity could be exposed for worst (Clemmitt, 2006) making them potential victims for online sexual assault, stalking, identity theft (Finn & Banach, 2000), cyber gender harassment (Citron, 2009), internet infidelity (Whitty, 2005) and even domestic violence by a suspicious spouse or even ex-spouse (Jenson, 1996). Popularity of social networking reached its highest peak with the new millennium ushering in 2000. Simultaneously at this time, US saw severe clash of fundamental freedom of speech and expression and evolving of modern ideologies of liberalization due to Web 2.0 developments in transparent internet communications via different mediums like blogs, open discussion forums, interactive websites and especially social networking websites. This led to the inevitable growth of gender harassment (Moraham-Martin, 2000) in the cyber space globally.

Problems involved in conceptualizing cyber offences targeting users of SNW's

The 10th United Nations Congress on the Prevention of Crimes and Treatment of Offenders, which was held in Vienna in 2000, made the first move towards recognizing the universal need for preventive measures against cyber crimes. The declaration in Vienna regarding cyber crime preventive measures was well developed in Council of Europe's Convention on cyber crime, held in Budapest, 2001. Even though several cyber offences were defined from criminological perspectives as early as in seventies and eighties, it was only after the EU convention on cyber crime (2001), that these offences were universally "criminalized". Hacking of emails, personal data and personal computer system could be said to be one of the earliest concept of cyber offence, which was brought under the category of criminal offences against computer system by the EU convention, 2001.[4] However, the resolutions of the Convention were mainly drafted to protect e-commerce and not to prevent attacks on human privacy and dignity. But cyber victimization of ordinary net users by ways of racial and other various types of hatred – violence, sexual abuse of adult women, including typical gender harassments like eve teasing, stalking, threatening to mutilate her virtual identity, had already started getting its momentum since 2000 and it was rising rapidly due to easy access to personal information of the women in target, easy ways to communicate through SNWs and absence of any proper preventive legal measures. On the whole, other than hacking, unauthorized access to computer contents and child pornography, no cyber offence was legally defined or recognized.

The year 2001 saw many cyber savvy countries adopting the draft definitions of cyber crimes and the preventive measures that were projected by the EU convention, 2001. But the convention as well as the nations who adopted the convention to make their own domestic laws to prevent cyber crimes, failed to note that cyber crimes cannot be confined within the offences of hacking, child pornography or cyber economic frauds; but that this the "cancer" has spread to a far extent to destroy ordinary adult internet user's peace as well. The other traditional offences which were identified by ongoing researches as "cyber crimes targeting individuals" are stalking (Basu and Jones, 2008; Ellison and Akdeniz, 1998; Jaishankar and Uma Sankary, 2005), identity theft (Berg, 2008), phishing, email spoofing (Halder and Jaishankar, 2008), morphing (Halder and Jaishankar, 2008; Nash, 2008), cyber bombing (which is often used in relation to terrorism), cyber flame war (abusive/ hate speech), cyber cheating (impersonation), cyber fraud (which is often used in relation to monetary crimes), cyber sex and issues of cyber privacy including cyber child pornography (Jaishankar, Halder and Ramdoss, 2008). On the contrary of cyber child pornography, which was dealt by the EU convention in 2001 and identity theft, which was dealt under the EU conventions in 2001 and 2005, none of the above mentioned cyber offences got universally accepted legal definitions, nor universal criminal sanctions. We assert that this was the breeding reason for cyber victimization of women. The concept of online gender harassment remained completely unidentified. Along with the few offences as was demarcated by the EU conventions,

[4] EU convention on cyber crime, 2001, Chapter II, Section 1

different cyber savvy nations extended/stretched already existing definitions of penal offences targeting human dignity and privacy to suit the needs of protecting their own cyber space only.

Universally, cyber stalking has never been legally defined. In the US, stalking has been treated as an extended version of stalking with the digital aid. A good example would be the provisions in the Violence against Women and Department of Justice Reauthorization Act of 2005 which treat crimes like stalking. The section 226 1A of title 18 of United States Code was amended by section 114 of the Violence against Women and Department of Justice Reauthorization Act of 2005, has redefined the behavior of stalking as:

> travels in interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States, or enters or leaves Indian country, with the intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel places that person in reasonable fear of the death of, or serious bodily injury to, or causes substantial emotional distress to that person, a member of the immediate family (as defined in section 115) of that person, or the spouse or intimate partner of that person; or (2) with the intent – (A) to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate, or cause substantial emotional distress to a person in another State or tribal jurisdiction or within the special maritime and territorial jurisdiction of the United States; or (B) to place a person in another State or tribal jurisdiction, or within the special maritime and territorial jurisdiction of the United States, in reasonable fear of the death of, or serious bodily injury to – (i) that person; (ii) a member of the immediate family (as defined in section 115 of that person; or (iii) a spouse or intimate partner of that person; uses the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury to, any of the persons described in clauses (i) through (iii) of subparagraph (B).

To accommodate the needs of digital stalking, various provinces of the US have made their own stalking laws. But none have defined "cyber stalking" and drawn its legal boundaries. The term has been used as a synonym for cyber harassment in many provincial laws of the US. For instance, the

Michigan criminal code in its definition to "harassment" included **"**conduct directed toward a victim that includes 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 (Citron, 2009).

Again, cyber harassment has also not been defined anywhere legally. The term has been construed in a very broad prospect to include various online disturbances. However, after the Megan Taylor Meier suicide,[5] cyber bullying has attracted proper legal attention in the US and has been well defined.[6] Still, whether the definition and the law can be stretched to cover bullying incidences of the adult women remain a debatable issue. Unfortunately, cyber bullying is still considered a "behavioral fault" in many countries like India and no legal definitions are available to prevent the same.

It is deplorable that the majority of the cyber offences targeting individual users of SNWs, including women had remained subject matters for theoretical discussions and failed to attract any legal prescription. New types of online offences are emerging every day but most of these offences are generalized under a broad concept, which often over looks the inherent nature of the crime. For instance, cyber harassment has been used as a holistic term for other cyber offences like cyber stalking, cyber eve teasing or even cyber defamation. Concerning the emerging researches on natures of cyber crimes (Halder and Jaishankar, 2008), each of them differ from the other. Due to less or no individual conceptualization of these digitally reincarnated offences of the traditional offline crimes social networking sites are becoming hubs of cyber offences targeting individual internet users.

[5] Megan Meir was an American teenager who became a victim of cyber bullying and committed suicide. "Her suicide was attributed to cyber-bullying through the social networking website MySpace". Wikipedia contributors, „Suicide of Megan Meier," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/w/index.php?title=Suicide_of_Megan_Meier&oldid=317698588 (accessed October 4, 2009).

[6] Megan Meir Cyber bullying Prevention Act 2008 was passed by the US Congress to prevent cyber bullying children in the cyber space.

Typology and Patterns of victimization of women in the SNWs

Women in the SNWs are victimized in different patterns by the abuser who can be an individual or even a group of individuals. The victimization type differs on the basis various factors, for example, on the basis of the victim's sexuality, her ideologies, her marital status, her profession and professional commitments, the regularity of her participation in some chosen groups, the language she may use, her popularity in the groups etc. Again, the abuser can be both male or female. Similarly, the offences can be either sexual or non sexual in nature.

In most cases male harassers attack the victim for sexual purposes like morphing, using the image for pornographic purposes, cyber stalking etc and non sexual purposes such as harassment and bullying. Female perpetrators however, victimize the victim mainly for ideological differences, hatred or for taking revenge. Such attacks may not be sexual in nature.

Based on the above criteria the typology of the offences against the women victims in the SNWs is framed as follows:

1) *Cyber verbal abuse by groups of perpetrators expressing hatred:* Citron best describes this as "cyber mob attack" (Citron, 2009) where a female member of the SNW may be attacked by a group of perpetrators both in the community wall and also in her own message board.
2) *Cyber defamation targeting the individual self* (Citron, 2009; Halder and Jaishankar, 2008): Emotional breakups may lead the male member to spread lies about the female member to other members through his own posts, community walls etc.
3) *Cyber stalking*: The female member is stalked in all the groups she joins, her friends' walls are constantly watched for seeing her posts, her own write ups and her activities online (Basu and Jones, 2008; Ellison and Akdeniz, 1998; Jaishankar and Uma Sankary, 2005).
4) *Morphing* (Nash, 2008; Halder and Jaishankar, 2008): The photographs of the female members are taken from the personal albums and they are morphed for pornographic purposes by using parts of the pictures, for instance, the head or up to breast.
5) *Cloning:* Cloned profiles or fake profiles of female victims are created by stealing the personal information of the female member. The cloned profile presents the original profile in such a manner that people are duped. The cloned profile then asks the friends of the original member to become his/

her friend and crack the privacy of other members besides using the original member's information for evil purposes. Female members in the popular SNWs like Facebook, Myspace and Orkut often face this problem (Halder, 2007).

6) *Cyber obscenity* (Citron, 2009): The victim's photograph is used, morphed and distributed in the internet with obscene postures. The harasser may also post messages using obscene languages to her wall. Cyber obscenity can also be practiced by way of hacking the profile of the female member. Then the original photographs posted in the mentioned profile are morphed and the profile name and information as well as the morphed photographs are used to send obscene messages to the "friends" of the original profile owner and also to wider audience.
7) *Hacking:* Particular targets are chosen and their profiles are hacked. Their personal information is used for evil purposes. The harasser may even distribute open invitations for having sex with the profile owner at her home address (Halder and Jaishankar, 2008).
8) *Cyber harassment*: This may include constant messaging to the profile's wall or personal email id (Halder, 2007) which is shown in the profile, regular peeping in as a visitor and leaving messages in her wall, continuously sending request for friendship, joining groups where she is member and constantly posting messages disagreeing with her, etc (Citron, 2009).
9) *Virtual rape* (Citron, 2009; Whitty, 2005): This is a violent type of cyber victimization where the targeted woman is taken up by a harasser. He either posts constant messages like "I will rape you", "I will tear you up" or "your internet identity will be f…ed off" etc, or particular community members may "mob attack" the targeted female with such words which successfully generates more enthusiasm among other unrelated members to comment on the victim's sexuality. The profile owner then becomes a hot topic for erotic discussions, vulgar name calling etc.
10) *Banning a female member and restraining her from expressing her views*:

This generally happens in a male dominated group or community where the moderator or owner or group members may victimize the targeted female member by banning her for her own feminist ideologies even through the group or the community could have been created for letting people express their own ideologies. The reason could be that the majority of the group may be pro feminist or some individual members dislike the straight forwardness of the female members in discussing the problems of women in every day world.

11) *Cyber bullying and name calling* (Citron, 2009; Halder and Jaishankar, 2008): The harasser may constantly bully the target in the SNW, both in her wall and in the groups or communities where either he or she is member. Even though this is a gender neutral cyber offence, women are most chosen targets for their sexuality, emotional breakups or even domestic violence. The ex spouse or the ex lover constantly bully the woman to vent out his anger in public.
12) *Domestic violence and cyber flame*: As mentioned above, separated partners may take up SNWs to vent out their anger against the female member. In such cases the ex-partner starts bullying the woman first and then provokes her to have "online fights" (Citron, 2009; Southworth, Finn, Dawson, Fraser and Tucker, 2007).
13) *Impersonation and cheating:* SNWs give wide options for creating profiles under pseudo names, hiding one's real age, sex and other information. Further, the creation of multiple profiles of the same individual using different email ids is also possible in the SNWs. This gives the opportunity for mischief mongers to impersonate and flirt with female members' (Halder and Jaishankar 2008; Whitty, 2005). The harasser drags the victim in an emotional relationship and she is encouraged to share her secrets, and even have erotic chats with the harasser. When the victim finally pressurizes to meet him in person, either he blackmails the victim or cheats the victim. However, impersonation and cheating can even happen for financial issues in the SNWs as well. The harasser may promise the victim some online or offline monetary gain by showing his fake credentials and there by later on dupe the victim.
14) *Blackmailing and threatening:* This happens due to the easy availability of the personal information of the women members in the SNWs. "Jilted lovers", ex spouses, mischief mongers and stalkers may threaten and blackmail the woman for various reasons which may even lead to shut down the profile of the female member. This can even have an offline effect where miscreants may physically threat and blackmail the woman with her secrets that she may have shared with her friends in groups or communities.

The Emotional and Physical Risk Factors of Women Members of SNWs

The emotional suffering

Finn and Banach (2000) feel that even though internet helps women to better their physical as well as mental health, it is not hazard free. The risks involve loss of privacy, disinhibited communication, online harassment, and stalking. The internet has grown faster than the laws governing the internet. Doring (2000) points out that the biggest danger of internet socializing lies in cyber sex, which leaves a deep never ending traumatic effect on women users. The word "cyber sex" is used by Doring (2000) as a compact term to cover online gender harassment, cyber prostitution or virtual rape. Doring (2000) emphasizes that liberalization of women encourages them more to become victims of cyber sex. Hence women users must learn from past experiences of other victims to protect themselves from online sexual abuse (Doring, 2000).

Whitty (2005), mentions that, cyber socializing can bring in emotional relationships between men and women, where, women can be victims of cyber cheating. Even though in some cases cyber cheating may not have great impact on real life like offline cheating, Whitty apprehends that this may give birth to offline revenge taking mentality. Southworth et all (2007) points out that cyber socializing breeds domestic violence as well as violence against women in the way of cyber stalking, online abusive behavior, and gender harassment. They succinctly put that "ever-changing and increasingly inexpensive technologies make it easier than ever before for abusers to monitor and control their victims". They also feel that there is an urgent need to build support group to prevent and protect such online harassment of women. They also apprehend that laws are insufficient. Citron feels that social net working can breed many instances of gender harassment like cyber hate speech, cyber bullying and morphed photographs (Citron, 2009).

Ellison and Akdeniz (1998) feel that the phenomenon of cyber-stalking and on-line harassment looks set to be the focus of the next Internet-related moral panic. They feel that transnational nature of the cyber space should encourage actions by individual governments and international organizations to have a profound effect on the rights of the law-abiding internet users, or "netizens", around the world. They contend that successful cyber regulation cannot be achieved at the cost of fundamental freedoms of speech and privacy.

Halder (2007) has pointed out that social networking websites like *Orkut* posses a threat to Indian women's privacy as users. Many women register themselves as members without reading the privacy policies or being aware of the safety tips of such websites. The victims often become trapped due to their own negligence. As such, when cloned profile is created of the victim or her morphed photograph flashes up in her own wall or in the scrap books of others or even when she is informed of her harassment by other users, a sense of guilt and shame engulfs her. The experience becomes more traumatic when the victim is refused any police help due to non recognition of offences or lack of awareness of officials. Citron (2009) has pointed out that cyber hate speech targeting women is more distressing than other online offences. The trauma deepens when the harasser is "anonymous", leaving no immediate solution to find out who he is and why is he attacking. Citron (2009) has also shown how anonymous profile users can vandalize the social networking of women. Anonymous mob attacks (Citron, 2009), anonymous postings in individual user's wall or community walls (Citron, 2009) make women victims more panicked. Citron (2009) also feels that the broad concepts of US freedom of speech which is randomly followed by many social networking websites attracting non Americans as well, give a huge opportunity to users of the internet to publish their thoughts as "anonymous". This is well supported by SNWs and users get enough freedom to hide under the term "anonymous" when they go for "postings" in harsh, rude or abusive languages in the groups or community walls. We agree that most of such publications are targeted against women. The perpetrator successfully insults the "target" in public and generates similar hatred among the group members who follow him in teasing or bullying the victim. Eventually anonymity leads to greater dangers in the SNWs like stalking, threatening, abusive posting by other members of the group.

The following case studies[7] show how cyber socializing creates emotional suffering.

[7] Some of these case studies were provided by Working to Halt Online Abuse (WHOA) (URL: www.haltabuse.org*)*, where the first author is engaged as an Internet Safety Advocate and some were taken from the cases handled by the first author as the Managing Director for Centre for Cyber Victim Counseling (CCVC) (Url: www.cybrvictims.edu.tf) with the permission from the victims. Due to issues of confidentiality, victim's identity is not disclosed.

Case study 1:

The victim and the perpetrator met in a social networking website. Eventually they started having regular postings to one another's wall, online chatting and came to know about each other's families through photographs that were posted in the personal albums of the perpetrator and the victim. Eventually they fell in love with each other. The perpetrator was staying in a foreign country for his professional commitments and promised the victim to marry her once he returns within a year. After the stipulated date when the victim contacted the perpetrator, he completely denied the "promises". Once the victim tried to contact his family members, they shunned her off and threatened her with dire consequences if she tried to meet the man. The victim felt cheated, emotionally broken and publicly humiliated.

Case study 2:

The perpetrator was the former husband of the victim. Both of them were members of the same SNW. The perpetrator found out the victim after random name search and started following her. He also found out the chosen communities where the victim was regularly participating and started stalking the victim. He started becoming member of those groups and contacted the friends of the victim only to harass her. The perpetrator started enquiring about the private life of the victim from the friends of those groups and humiliated the victim. The victim felt panicked and her privacy was disturbed. The victim started feeling that somebody is always watching in the cyberspace and she became averse of the use of technology.

Case study 3:

In this case, the victim's sibling was the perpetrator. She was a member of an SNW which encouraged people to tell about their emotional out bursts, mood swings etc. Since the victim and her sibling were not in good terms, the perpetrator (the victim's sibling) used this SNW to tell the wider audience that the victim was the "main cause" for her failures in her life and defamed her in every possible way. The members started believing the perpetrator and started abusing the victim in every possible way. The victim felt humiliated and emotionally distressed.

The physical threat

The other danger which crops up with cyber socializing is offline threats created by online rendezvous. In many instances women victims become friends of other individual profile owners whom they have never met in real life. The problem starts when the online relationship turns unpleasant. These individuals, who can be either male or female, may have come to know about the victim's real life from the victim herself and later constantly use such information to threat her. The victim remains in constant danger of being physically hit by the perpetrator (Whitty, 2005), if the victim and the perpetrator stay in the same locality or even in the same state. The following case study would prove how online socialization can create physical threat to the victim.

Case study:

The victim and the perpetrator became friends in a social networking website. The local members of the SNW group used to meet weekly at a city pub to chit-chat and also to celebrate member's birthdays, anniversaries etc. The victim became target of the perpetrator after an emotional relationship (as was "presumed" by the perpetrator) did not finally materialize. The perpetrator threatened the victim by telephone that in the next weekly meeting in the pub she will be physically assaulted by him and his followers.

Reasons for the growth of victimization of women in cyber socialization

Easy availability of victims' (women's) personal information

SNWs are made to let other people know the existence of the profile owner. Hence users give away their vital information like residential address, marital status, age, phone numbers, likes and dislikes etc. Even though many SNWs provide options for using pseudo names and publication of such information as only "optional", many first time registrants, including women, float their personal information in the web through these SNWs without actually knowing the dangerous effect of it. This gives a huge opportunity for harassers to victimize the targets.

Ignorance and negligence of the users

Halder and Jaishankar (2008) have pointed out that women are prone to all sorts of cyber crimes like hacking, stalking, morphing, cyber cheating, cyber defamation, and cyber sexual abuse. Social networking websites have become breeding grounds for such crimes. The question which haunts researchers is: why women are the targeted majority in the SNWs? We feel that among several factors which push women to become victims in the SNWs, the ignorance of the policy guidelines and safety measures stands first. The SNWs presently give wide options to protect one self from being harassed in various modes like setting up security measures, "locking "personal albums and message boards, blocking the harasser, preventing aliens from seeing one's personal information, preventing unknown persons from writing in one's message board, blocking and banning individuals from community and groups and hiding one's profile from the internet search.[8] Halder (2007) cautions that majority of the women join the social networking sites without checking any of such safety measures.

Halder (2007) did a minor research with a small sample size of 20 on the awareness of female members of Orkut, a popular social networking website. The findings are: Maximum of the respondents have never read policy guidelines before registering with the SNW, many of them have checked available safety – tips only after they were victimized themselves or have heard of their friend's experiences; almost all of them have personal photographs even though they know displaying of photographs is not very safe in a public SNW. A majority of them have turned on their security button and "locked" their albums and message book only after they had experienced some sort of harassment. Some of them had their "cloned" profile where their personal information was used to dupe their friends. These cloned profiles sent friend's request to the already existing friends with the statement "I have deleted my older account, please accept me now". Some had their profiles hacked and photographs used for pornographic purposes. These women users (whose profiles were either cloned or hacked) had deleted the old account themselves and created fresh accounts. Some had reported abuse to the Orkut authorities; some felt these incidents were not to be reported. Many of respondents know that posting personal photographs is not safe, but they

[8] Popular SNWs like Facebook, Myspace, Orkut , Hi5 etc, in their privacy policies give wide options for users to exercise all the safety measures like locking the album, hiding profile visitor's, banning unwanted "friends", removing unwanted messages from one's scrapbook etc.

cannot resist from showing photographs of themselves, of their families or their homes to other "friends" with whom they might have never met.

Many of them don't trust friends from Orkut whom they have never met earlier, but at the same time they feel "comfortable" in sharing their interests, photographs or personal secrets with those friends whom they have seen in Orkut for a longer period and who had been pretty active in the groups and communities they are members. However, a majority of them do not know that sharing of such information can bring in more problems by way of "third party" peeping in the wall or message board of one of the two friends, who may not be the common friend for both. The problems which may arise thus are creating a fake profile with available information or even blackmailing the women with her secrets. Some had seen their photographs in other's album who are no way connected to them. But they did not report this incident to the authorities. Some had verbal disagreements between group mates and suspect that their profiles were cloned or even hacked by such people. Except two, none had any idea that they have a legal right to preserve their privacy in the SNW and almost all of them had experienced either major or minor harassments in the SNW.

Scheming ways to hide one's real identity under camouflaged profiles

The ever expanding freedom of speech and expression in the US has accepted the right to be "anonymous" in the SNWs (Citron, 2009). At the same time, the SNWs allow a user to change his pseudo name and address at a regular interval. Even though this step was taken up by the SNWs for benefiting the members to change their physical and geographical location and at the same time saving themselves from perpetrators, this has encouraged the perpetrators to commit a crime and hide under a new identity. These hide and seek (Jaishankar, 2008) games by the perpetrators increase the risk factor of women members of the SNW.

Lackadaisical response of the SNWs

In most cases cyber socializing becomes dangerous due to nonchalant response of the SNWs. Most of the SNWs have an option to report any abuse of their services. This includes reporting of cyber harassment, cyber bullying, cyber threats, and cyber pornography. But in most cases SNWs have their own policies to treat the post as defamatory or harassing. For example, Adult friend finder.com solicits semi-nude images of women, lewd remarks about female members by their male friends and even sending pornographic pictures to fellow members.[9] Similarly ventyouranger.com encourages members to vent out their frustrations and anger towards particular individual who may not be the member of the group.[10] On the contrary, SNWs like Facebook, Myspace, and Orkut considers such written expressions as "unwanted" and can be banned only if the website authorities think that as an "offence". As such, for instance if a woman is constantly targeted at for cyber bullying, or the perpetrator creates fake profiles, the website directs the complainant to lodge a complaint with the bullying messages or the cloned profile. They also point out that the stipulated time for taking action can vary from 24 hours to 15 days.[11] But the impact of the offence may be so that the victim needs to take action within 24 hours; the victim either has to withdraw herself from the "societies" she is member of or she has to cancel her entire profile to wave off all the hazards. The delayed response or even nil response from the website authorities increase the panic in the victim and the harasser gets infinite opportunities to harm the victim's reputation within the stipulated time.

It is noteworthy that, most of the SNWs declare in their privacy policies that they will not take any responsibility for any sorts of harassment caused to the users by other users.[12] However, they provide safety tips in the menu bar and warn the users that their profile may be removed if it is reported that the said profile is harassing others, creating hate campaign, soliciting pornography etc.[13] It is unfortunate that these guidelines are not followed properly.

[9] Adultfriendfinder.com is an SNW for adults which is registered in the US and encourages having online sexual and erotic conversations with like minded people.

[10] www.ventyouranger.com is an SNW for adults which is registered in the US and encourages people to vent out their frustrations, anger etc in public forums.

[11] SNW like Orkut and Facebook stipulate minimum 24 hrs to 15 days' time to take action against the abuser, http://www.google.com/support/orkut/bin/answer.py?answer=57444 and http://www.facebook.com/safety/ (accessed October 4, 2009).

[12] This information was gathered from the privacy policies of SNWs like Orkut, Facebook, Myspace etc.

[13] ibid

Lack of uniform laws, conventions and rules

As we have already discussed earlier, that most of the offences that are charted out here as most -happening in the SNWs, are not universally recognized by any uniform law, convention or rules. More over, most of the SNWs are registered under the US laws and they are immunized from being sued as the defamatory media by section 230 of the Communication Decency Act, 1996. But this creates bigger problem for victims, especially women. As decided by the Miller's case (Miller vs. California, 413 U.S. 15 (1973),[14] the ideas of obscenity differ from society to society. US protects under 18 members of the SNWs from cyber bullying by the Megan Meir Cyber bullying Act, and women are protected from cyber harassment or cyber stalking which may result from domestic violence or broken emotional relationships by the Violence Against Women and Department of Justice Reauthorization Act of 2005. On the contrary, UK does not have any compendium of laws to protect cyber offences against women. However, there are some major laws like the Computer Misuse Act 1990, Police and Justice Act 2006, Sexual Offences Act 2003, The Prevention of Sexual Offences (Scotland) Act 2005, Protection from Harassment Act 1997, Malicious Communications Act 1988 which are widely used to prevent atrocities against women in the internet. But at the same time, the offences are not legally defined; hence perpetrators often escape punishment. Canada regulates victimization of women in online socializing through specific chapters of Canadian Criminal code which are meant for both men and women and there are no special laws to protect women. Indian law does not recognize many of the offences that occur online socializing like cyber bullying, cyber eve teasing, cyber harassment, cloning of the profile etc, in the Information technology Act (2000, the original and 2006 the amended version). The lack of universal laws to regulate social networking websites and the nil legal recognition of the offences that happen against women in the cyber space thus encourage the growth of online victimization of women.

[14] Miller vs California, 413 U.S. 15 (1973)

Conclusion

The main aim of cyber socializing is to give the users opportunity to meet with old and new friends, increase networks and socialize without actually going in person to the social gatherings. But this is not a hazard free zone. The main drawback of cyber socializing is the uncertain reliability of the "virtual friend" we meet up every day in the SNWs. At the same time, many users treat cyber socializing as a space for over riding their freedom of speech and expression (Citron, 2005). This attracts many offences like cyber flame, cyber hate speech, cyber bullying and cyber eve teasing etc. Online socializing never remains risk free for women mainly due to their sexuality. Majority of the cyber crimes targeting women happen in the SNWs (Citron, 2009; Halder and Jaishankar, 2008) but as no society can be crime free, online societies are no exception. Cyber crime exists and it is growing in number (Wall, 2007) through SNWs, mails, online chat rooms etc.

Social networking websites provide a wide range of social activities to be carried out in the cyber space. It is therefore very obvious that online socializing is also as vulnerable as real life socializing. But the patterns may differ due to the hi-tech nature of the offences. The attackers may or may not be known to the victims and reasons and motives behind victimization are mostly emotional issues. The harasser also uses the broader platform of the cyber space to victimize the target under camouflaged identities. Moreover, the unequipped, not-so-fitting, or developing laws, where such offences are not recognized or are yet to be recognized, help to expand the pattern of victimization day by day.

The two main reasons which attribute towards the growth of online victimization of women in the SNWs are: absence of proper gender sensitive universal cyber laws and lack of awareness of the safety modes among users of the SNWs. The SNWs are considered as a large global platform to express one's ideologies, thoughts and feelings about others. Every individual is supposed to use this platform at his or her own risk (Wall, 2007). Unfortunately, there are less laws and policy guidelines to regulate cyber space and this insufficiency gives full freedom to the perpetrators. This is a perfect example of how ignorance of cyber-social rules and norms coupled with weak laws can encourage criminalization in the online socialization. Laws can draw a defining line for limiting individual's behavior. But it depends upon the individual to make use of the laws to make their living space including cyber space more safe and beautiful.

References

Basu, S., & Jones, R. (2008) Regulating cyber stalking In: F. Schmallager, M. Pittaro (eds.) *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall, pp. 141-165.

CERT (2002) Spoofed/Forged Email, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, viewed 25 June 2009, http://www.cert.org/tech_tips/email_spoofing.html.

Citron. K. D. (2009) Cyber civil rights. *Boston University Law Review*, 89, pp. 61-125, viewed 25 June 2009, http://ssrn.com/abstract=1271900

Clemmitt, M. (2006) Cyber Socializing, *CQ Researcher*, Vol 16, No 27, pp. 625-648.

Döring, N. (2000) Feminist Views of Cybersex: Victimization, Liberation, and Empowerment, *CyberPsychology and Behavior,* Vol 3, No 5, pp. 863-884.

Ellison, L., & Akdeniz, Y. (1998) Cyber-stalking: the Regulation of Harassment on the Internet, *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, pp. 29-48.

Finn, J., & Banach, M. (2000) Victimisation online: The downside of seeking human services for women on the internet, *CyberPsychology & Behavior,* Vol 3, No 5, pp. 785-796.

Fraim, L. N. (2006) *Cyber Socialization: What's Missing in My Life?* Paper presented at The Nordic Youth Research Information Symposium, 9, 2006, Stockholm, viewed 25 June 2009, http://webappo.sh.se/C1256CD200369F7E/0/0A9064B157EF97AAC12570E40043DBF9/$file/Linda%20Nalan%20Fraim.doc

Halder D., & Jaishankar, K. (2008) Cyber crimes against women in India: problems, perspective and solutions, *TMC Academic Journal*, Vol 3, No 1, pp. 48-62.

Halder D. (2008) *Privacy in Orkut: A hopeless Story, CyberLawTimes.com, Monthly Newsletter, Vol 3, No 9, September 2008,* viewed 25 June 2009, http://www.cyberlawtimes.com/articles/108.html.

Halder D. (2007) *Cyber crime against women in India, CyberLawTimes.com, Monthly Newsletter, Vol 2, No 6, June 2007,* http://www.cyberlawtimes.com/articles/103.html.

Jaishankar, K., & Uma Sankary, V. (2005) Cyber stalking: A global menace in the information super highway, *ERCES Online Quarterly Review*, Vol 2, No 3, viewed 25 September 2007, http://www.erces.com/journal/articles/archives/volume2/v03/v02.htm.

Jaishankar, Halder, D., & Ramdoss S. (2008) Pedophilia, pornography and stalking: Analysing child victimization on the internet In: F. Schmallager, M. Pittaro (eds.) *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall, pp. 28-42.

Jaishankar, K. (2008) Space Transition Theory of Cyber Crimes In: F. Schmallager, M. Pittaro (eds.) *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall, pp. 283-301.

Jenson, B. (1996) Cyberstalking: Crime, enforcement and personal responsibility in the on-line world, viewed 25 June 2009, http://www.law.ucla.edu/classes/archiv/s96/

Morahan-Martin, J. (2000) Editorial: Women and the Internet: Promise and Perils, *CyberPsychology and Behavior,* Vol 3, No 5, pp. 683-691.

Nash, J. (2008) *Making Women's Place Explicit: Pornography, Violence, and the Internet*, Module composed for open education, Berkman Center for Internet and Society, Harvard Law School, p. 2.

Sara, E. B, (2008) Identity theft: causes, correlates and factors: A content analysis In: F. Schmallager, M. Pittaro (eds.) *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall, pp. 225-251.

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007) Intimate Partner Violence, Technology and Stalking, *Violence Against Women*, Vol. 13, No. 8, pp. 842-856.

Wall, D. S. (2007) *Cybercrime: The transformation of crime in the information age*. Polity: Cambridge.

Whitty, M. T. (2005) The Realness of Cyber cheating: Men's and Women's Representations of Unfaithful Internet Relationships, *Social Science Computer Review,* Vol 23, No 1, pp. 57-67.

Debarati Halder
Karuppannan Jaishankar

Sajber druženje i viktimizacija žena

Koncept „Web 2.0” je uticao na redefinisanje virtuelnog života običnih ljudi i dao široke mogućnosti korisnicima interneta uključujući i žene u smislu razmene ideja, interakcije sa istomišljenicima i učestvovanja u razvoju virtualnih društava po sopstvenom izboru. Sajtovi za socijalno umrežavanje, kao segment koncepta „Web 2.0”, su veoma popularni za korisnike interneta. Međutim, sajtovi za socijalno umrežavanje imaju i tamnu stranu. Postali su raj za nasilnike prema ženama koje pored dece, spadaju u ranjive „mete” na internetu. U ovom radu ispituje se viktimizacija žena putem sajtova za socijalno umrežavanje generalno, analiziraju se trendovi takve viktimizacije sa socijalno-pravno-viktimološkog ugla i preispituju razlozi za porast takve viktimizacije.

Dva glavna razloga koja doprinose porastu online viktimizacije žena putem sajtova za socijalno umrežavanje su: odsustvo adekvatnih rodno senzibilisanih i univerzalnih sajber zakona i nizak nivo svesti o načinima na koje korisnici sajtova za socijalno umrežavanje mogu da se zaštite. Sajtovi za socijalno umrežavanje smatraju se širokom globalnom platformom za izražavanje sopstvenih ideologija, mišljenja i osećanja prema drugim ljudima. Na svakom pojedincu je da koristi ovu platformu na sopstveni rizik (Wall, 2007). Nažalost, malo je zakona i procedura koji regulišu sajber prostor, što učiniocima daje veliku slobodu. Ovo je savršen primer za to kako ignorisanje sajber socijalnih pravila i normi udruženo sa slabim zakonima mogu ohrabriti kriminalizaciju u online socijalnim mrežama. Zakoni mogu da povuku liniju u ograničavanju ponašanja pojedinca. Ali na pojedincu je da doprinese zaživljavanju zakona i na taj način činjenju sajber prostora bezbednim i lepim.

Ključne reči: sajber druženje, socijalno umrežavanje, viktimizacija, žene