Online Sexual Harassment

Issues & Solutions

by Mohamed Chawki, LL.B, BA, LL.M, Ph.D, St. Center for Terrorism Law, St. Mary's University, Texas, USA
Yassin el Shazly, LL.B, LL.M, Ph.D, University of Ain-Shams, Cairo, Egypt

Abstract: This paper addresses and analyses the growing threat of sexual harassment in cyberspace. Digital transactions and communications have, over the past decade, been increasingly transpiring at an increasingly accelerated rate. This non-linear progression has generated a myriad of risks associated with the utilization of information and communication technologies (ICTs) in cyberspace communications, amongst the most important of which is: the threat of sexual harassment. On such account, this paper aims to provide an overview of the issues and risks pertinent to sexual harassment and seeks to offer some solutions based on the necessity of pursuing a tri-fold policy encompassing strategic and regulatory, technical, and cultural approaches.

Keywords: Social Networking Sites (SNS); Bullying; Sexting; Legislation; Regulation

Recommended citation: Mohamed Chawki, Yassin el Shazly, Online Sexual Harassment: Issues & Solutions 4 (2013) JIPITEC 2, para 71.

A. Introduction

> *Sexual harassment is a well-known social problem that affects people at work, school, military installations, and social gatherings. (Barak, 2005)*
>
> *A worldwide phenomenon, it has been thoroughly investigated in recent decades in terms of prevalence, correlates, individual and organiational outcomes, and prevention; the range of studies provides an interdisciplinary perspective covering psychological, sociological, medical, legal, and educational aspe1cts of the phenomenon. (Ibid)*

1 Although men face harassment, women are the most likely victims.[2] In many environments on the Internet, some users find themselves so captivated by their cyberspace lifestyle that they want to spend more and more time there, sometimes to the neglect of their in-person life (Suler, 1999). They may not be entirely sure why they find themselves so engrossed. They can't accurately verbalize an explanation for their 'addiction'. The humorous substitution of words in the Palace Spa suggests that it is an unnameable 'thing' – a compelling, unnameable, hidden force. It's not the chat room or the newsgroup or the e-mail that is eating one's life, but the internal, unconscious dynamic it has ignited (Ibid). Indeed, the Internet has two faces, positive and negative (Barak and King, 2000). Its positive aspect is that it enables the enrichment and improvement of human functioning in many areas, including health, education, commerce and entertainment. On its negative side, the Internet may provide a threatening environment and expose individuals to great risks (Ibid).

2 In the context of women using the Internet, Morahan-Martin (2000) noted the 'promise and perils' facing female Net users. Sexual harassment and offence on the Internet is considered a major obstacle to the free, legitimate, functional and joyful use of the Net, as these acts drive away Net users as well as cause significant emotional harm and actual damage to those who remain users, whether by choice or by duty.

B. Harassment in Cyberspace

3 'Sexual harassment is a prevalent phenomenon in face-to-face, social environments' (Barak, 2005). The harassment of women in the military (Fitzgerld, Magley, Drasgow & Waldo, 1999), at work (Richman et

al., 1999) and schools (Timmerman, 2003) is receiving increased attention from both policymakers and the popular media. 'Sexual harassment is not a local phenomenon, but exists in all countries and cultures, although its perceptions and judgment, and consequently definitions, significantly differ from one culture to another' (Barak, 2005).

I. Classification of Sexual Harassment Behaviours

4 Till (1980) classifies sexual harassment behaviours into five categories: (1) sexist remarks or behaviour, (2) solicitation of sexual activity by promise or rewards, (3) inappropriate and offensive, but sanction-free sexual advances, (4) coercion of sexual activity by threat of punishment and (5) sexual crimes and misdemeanours. Following extensive pilot work, the suggestion was made (by Fitzgerald et al., 1995) to change the classification of types of sexual harassment into three different categories: gender harassment, unwanted sexual attention and sexual coercion. According to this study,

> *[g]ender harassment involves unwelcome verbal and visual comments and remarks that insult individuals because of their gender or that use stimuli known or intended to provoke negative emotions. These include behaviors such as posting pornographic pictures in public or in places where they deliberately insult, telling chauvinistic jokes, and making gender related degrading remarks. (Barak, 2005)*

5 Unwanted sexual attention covers a huge range of behaviours from being touched without permission, causing fear or distress, sexual name calling and harassment to rape and sexual assault.[3] Unwanted sexual attention can happen to both women and men and between people of the same and opposite sex.[4]

6 Sexual coercion exists along a continuum, from forcible rape to nonphysical forms of pressure that compel girls and women to engage in sex against their will. The touchstone of coercion is that a woman lacks choice and faces severe physical or social consequences if she resists sexual advances.[5]

7 All three types of sexual harassment may exist offline or on the Internet. 'However, because of the virtual nature of cyberspace, most expressions of sexual harassment that prevail on the Net appear in the form of gender harassment and unwanted sexual attention' (Barak, 2005).

> *Sexual coercion is distinctly different online than it is offline in that tactile force is not possible; however, the prevalence of verbal uses of threats, rewards, intimidation or some other form of pressure can be perceived as just as forceful as if it were in person. A unique feature of online interactions is that a perpetrator may possess technical skills which allow hacking into the victim's computer and/or 'cyberstalking' to follow a victim from digital place to place, which is often perceived as quite threatening to the victim. (Ibid)*

II. Gender Harassment

8 'Gender harassment in cyberspace is very common. It is portrayed in several typical forms that Internet users encounter very often, whether communicated in verbal or in graphical formats and through either active or passive manners of online delivery' (Barak, 2005). Active verbal sexual harassment mainly appears in the form of offensive sexual messages, actively initiated by a harasser toward a victim. 'These include gender-humiliating comments, sexual remarks, so-called dirty jokes, and the like' (Ibid).

9 This type of gender harassment is usually practiced in chat rooms and forums; however, it may also appear in private online communication channels, such as the commercial distribution through email (a kind of spamming) of pornographic sites, sex-shop accessories, sex-related medical matters, such as drugs such as Viagra and operations similar to penis enlargement. (Ibid)

10 Some scholars (Biber, Doverspike, Baznik, Cober & Ritter) investigated people's responses to online gender harassment in academic settings compared with traditional face-to-face forms of harassment (Li, 2005). A survey was administered to 270 undergraduate students in the US. The study examined a total of eight potential sexual harassment acts: (1) sexually explicit pictures; (2) content; (3) jokes; (4) misogyny; (5) use of nicknames; (6) requests for company; (7) requests for sexual favours; and (8) comments about dress (Ibid). The results showed that certain behaviour, such as requests for company, misogyny, the use of sexist nicknames, and comments about dress were seen as differentially harassing depending on the discourse medium (Ibid). Participants did not hold more relaxed standards for online behaviour. Rather, they had similar or even more stringent standards for online behaviour. Females perceived online jokes as more harassing than the same behaviour in a face-to-face environment, while males rated jokes as more harassing in the traditional environment (Ibid). Females tended to act rather cautiously (in comparison with a face-to-face setting) in defining the parameters of sexual harassment online. Compared with their male counterparts, they were more stringent in their judgment of behaviour as harassment because they took sexually explicit online pictures, jokes and requests for company more seriously (Ibid).

11 'Passive verbal sexual harassment on the other hand, is less intrusive, as it does not refer to one user communicating messages to another. In this category, the harasser does not target harassing messages directly to a particular person or persons but, rather, to potential receivers' (Barak, 2005). Nicknames and terms or phrases clearly attached to personal details often encompass this form of sexual harassment,

e.g. 'Sweet Tits' as a nickname or 'Want to blow my pole?' as an offensive phrase (Schenk, 2008). This category also includes explicit sexual messages attached to one's personal details in communication software or on a personal web page (Barak, 2005).

12 On a different note (Scott, Semmens, and Willoughby, 2001), illustrated how flaming creates a hostile environment for women.

> *Although flaming is not necessarily aimed at women, it is considered, in many instances, to be a form of gender harassment because flaming is frequently, typically, and almost exclusively initiated by men. The common result of flaming in online communities is that women depart from that environment or depart the Internet in general—what has been termed being 'flamed out'. Flamed out highlights the fact that the use of male violence to victimize women and children, to control women's behaviour, or to exclude women from public spaces entirely, can be extended into the new public spaces of the Internet. (Barak, 2005)*

13 A constructive solution has been the design of women-only sanctuaries that offer communities where flaming is rare and obviously not identified with men.

14 Graphic-based harassment can be active or passive.[6] Active graphic gender harassment refers to the intentional sending of erotic, pornographic, lewd and lascivious images and digital recordings by a harasser to specific or potential victims. Graphic harassment often occurs via email, instant messaging, redirected/automatic linking and pop-ups[7] (Schenk et al., 2008).

III. Cyberstalking

15 Another area of research that has provided insight into cybersexual harassment is cyberstalking. Bocji (2004) defined cyberstalking as a group of behaviours in which the use of information and communications technology is intended to cause emotional distress to another person. Behaviours associated with cyberstalking include making threats, false accusations (false-victimization), abusing the victim, attacks on data and equipment, attempts to gather information about the victim, impersonating the victim, encouraging others to harass the victim, ordering goods and services on behalf of the victim, arranging to meet the victim and physical assault (Schenk, 2008).

16 Imagine a distressed woman discovering the following message on the Internet that was falsely attributed to her:

> *Female International Author, no limits to imagination and fantasies, prefers groups macho/sadistic interaction...stop by my house at [current address]. Will take your calls day or night at [current telephone number]. I promise you everything you've ever dreamt about. Serious responses only.*[8]

17 Or imagine the fear generated by the following email messages sent over and over again from someone who remained anonymous, but seemed to have specific knowledge of the recipient's personal life:[9]

> *I'm you worst nightmare. Your troubles are just beginning.*

18 Some scholars believe that cyberstalking is synonymous with traditional offline stalking because of the similarities in content and intent (Goodno, 2007).

19 Similarities that are pointed to include a desire to exert control over the victim, and, much like offline stalking, cyberstalking involves repeated harassing or threatening behaviour, which is often a prelude to more serious behaviours. While these similarities do exist, cyberstalking differs from offline stalking in the following ways (Ibid):

- Cyberstalkers can use the Internet to instantly harass their victims with wide dissemination. For example, an offline stalker may harass the victim by repeatedly telephoning the victim. However, every telephone call is a single event that requires the stalker's action and time. This behaviour can easily snowball online because, with only one action, the stalker can create a harassing email message that the computer systematically and repeatedly sends to the victim thousands upon thousands of times.

- Cyberstalkers can be physically far removed from their victim. Offline stalking often entails situations where the stalker is physically near the victim. Cyberstalkers, however, can use the Internet to terrify their victims no matter where they are; thus, the victims simply cannot escape. The Internet provides cyberstalkers a cheap and easy way to continue to contact their victim from anywhere in the world. In addition, there is a sinister element to the secrecy of the cyberstalker's location. The uncertainty of the cyberstalker's location can leave the victim in a state of constant panic as she is left wondering whether her stalker is in a neighbouring house or a neighbouring state. Finally, the physical location of the cyberstalker can create several jurisdictional problems, because this act can take place across state lines.

- Cyberstalkers can remain nearly anonymous. The environment of cyberspace allows offenders to overcome personal inhibitions. The ability to send anonymous harassing or threatening communications allows a perpetrator to overcome any hesitation, unwillingness or inabilities he may encounter when confronting a victim in person. Perpetrators may even be encouraged to continue these acts.

- Cyberstalkers can easily impersonate the victim. Unlike offline stalking, the cyberstalker can easily take on the identity of the victim and create havoc online. While pretending to be the victim, the cyberstalker can send lewd emails, post inflammatory messages on multiple bulletin boards and offend hundreds of chat room participants. The victim is then banned from bulletin boards, accused of improper conduct and flooded with threatening messages from those the stalker offended in the victim's name.

20 In many ways, the Internet makes many of the frightening characteristics of offline stalking even more intense. It provides cyberstalkers with twenty-four-hour access, instantaneous connection, efficient and repetitious action and anonymity (Goodno, 2007). On top of all this, cyberstalkers can easily pretend that they are different people. The possibilities open to cyberstalkers are as endless as the borders of the ubiquitous Internet.

IV. Online Sexual Harassment on Social Media

21 Online Social Networks or Social Networking Sites (SNS's) are one of the most remarkable technological phenomena of the 21st century, with several SNS's now among the most visited websites globally. SNS's may be seen as informal but all-embracing identity management tools, defining access to user-created content via social relationships.[10]

22 Over the past five years, the popularity of Social Networking Sites (SNS's) has increased spectacularly, attracting an extraordinary number of users, of which a significant proportion are teenagers. An EU Kids Online study showed that in Europe, 77% of 13- to16-year-olds have a profile on a social networking site (Lievens, 2012), even though most social network sites put the minimum age required to create a profile at 13. The study also found that 38% of 9- to 12-year-olds are already active on SNS's (Ibid). According to a US study which examined the social media use of 12- to 17-year-olds, 80% of American teenagers are active on social network sites, of which 93% are present on Facebook (Ibid).

23 Sociologically, the natural human desire to connect with others, combined with the multiplying effects of Social Network (SN) technology, can make users less discriminating in accepting 'friend requests'. Users are often not aware of the size or nature of the audience accessing their profile data, and the sense of intimacy created by being among digital 'friends' often leads to disclosures which are not appropriate to a public forum.

24 As the Council of Europe put it in 2011 in their Recommendation on the protection of human rights with regard to social networking services, SNS's have 'a great potential to promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom to express, to create and to exchange content and ideas, and the freedom of assembly' (Lievens, 2012). However, the fact that SNS's allow users to communicate through status updates, through messages on 'walls' or through instant messaging, to share photo or video fragments, and to connect with old or new 'friends', also entails a number of risks, the most important of which include stalking and bullying.[11]

1. Stalking on Social Media

25 Stalking typically involves threatening behaviour in which the perpetrator repeatedly seeks contact with a victim through physical proximity and/or phone calls (offline stalking), but also by electronic means, such as Instant Messenger and messaging on SNS's. Statistics on cyberstalking suggest that stalking using SNS's is increasing.[12]

26 In a 2005 study of one university's Facebook network, between 15 and 21% of users disclosed both their full current address as well as at least two classes they were attending. Since a student's life is mostly dominated by class attendance, the combination of address and class schedule provides the physical location of the user throughout most of the day (and night).[13] A much larger number of users, 78%, provided instant messaging (IM) contact information suitable for tracking their online status. Emerging mobile-based social network sites such as Twitter tend to emphasise location data even more. It can also be seen from the other threat descriptions that SNS's provide many other more subtle methods for stalkers to track their targets.[14]

27 The impact of cyberstalking via social networks on the victim is well known, and can range from mild intimidation and loss of privacy to serious physical harm and psychological damage. In Seattle two girls aged 11 and 12 were charged in 2011 with first-degree computer trespassing and cyberstalking, for allegedly posting sexually explicit photos and comments on the Facebook page of a 12-year-old classmate.[15] The two girls charged in the case were also accused of using the third girl's computer address to send out instant message solicitations for sex using her name. The children involved are all middle-school classmates and live in the suburban city of Issaquah, east of Seattle. The two accused offenders are believed to be the youngest individuals ever charged with cyberstalking and computer trespassing in King County.[16]

2. Bullying on Social Media

28 On a different note, social networks like Bebo, Facebook, Twitter, Youtube and MySpace are sometimes sites of cyberbullying, because people can post abusive messages and pictures on other people's walls, pages or profiles.

29 In a study of 799 youth ages 12-17, it was found that 90% of youth using social media said that when they witness online meanness, they ignore it (Levy et al., 2012). Eight per cent of youth reported having experienced some form of online bullying, such as through email, a social network site or instant messaging. Eighty per cent said they have defended the victims (Ibid). Seventy-nine per cent said that they have told the other person to stop being mean. About 67% of teens who have witnessed online cruelty have also witnessed others joining in – and 21% said they have also joined in the harassment (Ibid).

30 In addition, a 2006 study found out that 'about one out of ten youngsters have been involved in frequent cyberbullying: 3.3% exclusively as a victim, 5.0% exclusively as a perpetrator, and 2.6% as both a victim and a perpetrator'.[17] 'The majority of youngsters (63.8%) believe cyberbullying is a "big problem". This figure may reflect either a general assessment of the issue in the eyes of the youngsters, or it may indicate that they find it a serious problem for those being bullied'.[18] Whether this is due in whole, in part or in combination to the increased use and development of social networks, increased platform compatibility, increased access to the Internet, ease of multimedia creation and distribution, or indeed to the increasing recognition that there are a group of acts which utilise technology that are identifiable as bullying is not currently known.[19] Social networks tend to offer an array of tools to users – for example, in addition to profile and people search there may also be blogging or micro-blogging facilities, instant messaging, chat rooms, community and collaboration areas etc. which together constitute a very useful 'suite' of tools for the bully. Each of these elements can be used positively or potentially misused.[20] The forms of cyberbullying behavior that can be carried out on social networks include the following:[21]

- Flaming: Online fights using electronic messages with angry and vulgar language.
- Harassment: For example, repeatedly sending hurtful or cruel and insulting messages; gaining access to another's username and password in order to send inappropriate messages to friends' lists.
- Denigration: Setting up accounts pretending to be people in order to humiliate them; sending or posting gossip or rumours about a person to damage his or her reputation or friendships, e.g. the creation of 'Hate' websites, the posting of jokes, cartoons, gossip and rumours, all directed at a specific victim; posting harmful, untrue and/or cruel statements or pictures, and inviting others to do the same, or to comment on them.
- Impersonation: Pretending to be someone else and sending or posting material to get that person in trouble, put them in danger or to damage their reputation or friendships.
- Outing: Sharing someone's secrets or embarrassing information or images online.
- Trickery: Talking someone into revealing secrets or embarrassing information, then sharing it online.
- Exclusion: Intentionally and cruelly excluding someone from an online group, for example, a group of offline friends deciding to ignore a specific individual as a form of punishment.
- Threatening behaviour: Either direct or indirect (interestingly, Willard includes threats to hurt someone or to harm oneself).

V. Online Grooming

31 Online grooming can be described as 'an adult actively approaching and seducing children via the Internet (especially through social network sites, profile sites, chat rooms, news groups, etc.), with the ultimate intention of committing sexual abuse or producing child pornographic material depicting the child concerned' (Kool, 2011). Although grooming has always existed, the online version thereof is relatively new. Digital communication has enormously increased in Western societies. Research into young people's Internet behaviour has shown that they spend a considerable part of their free time roaming the Internet, often with insufficient supervision (Ibid). The Internet offers potential abusers ample opportunity to enter into digital contact with children in relative anonymity, which can lead to offline and/or online sexual abuse (Ibid).

32 For grooming to be a criminal offence, as referred to in European regulations, at least one act towards committing the offence is required, aiming to organise a meeting with the child and intending to have sexual contact (Ibid).

33 In the process of grooming, the perpetrator creates the conditions which will allow him/her to abuse the children while remaining undetected by others, and the child is prepared gradually for the time when the offender first engages in sexual molestation (Childnet International, 2009). Offenders may groom children through a variety of means. For example, an of-

fender may take a particular interest in the child and make him or her feel special. He may well treat the child emotionally like an adult friend, sharing intimate details about his sex life and adult relationships (Ibid). Another grooming technique is through the gradual sexualisation of the relationship. Offenders thus test the child's reaction to sex by bringing up sexual matters, having sexual materials around or engaging in sexualised talking (Ibid).

34 In December 2012, Daniel Enright, 21, from Australia was charged with sexually assaulting two teenagers he allegedly groomed online.[22] The offender approached the girls via the social networking website 'Facebook' before sending them text messages where he allegedly posed as a photographer looking for models. The charges included 11 counts of grooming girls under the age of 16 for sexual activity by sending them text messages. [23]

35 Enright was also charged with soliciting child pornography via text messages and sending menacing or harassing text messages.[24]

VI. Sextortion

36 Sextortion is 'a form of sexual exploitation where people are extorted with a nude image of themselves they shared on the Internet' (De la Cerna, 2012). Victims are later coerced into performing sexual acts with the person doing the extorting, and are coerced into performing hard-core pornography (Ibid).

37 Sextortion also refers to a form of sexual blackmail in which sexual information or images are used to extort sexual favours from the victim.[25] Social media and text messages are often the source of the sexual material and the threatened means of sharing it with others.[26]

38 Incidents of sextortion have been prosecuted under various criminal statutes, including extortion, bribery, breach of trust, corruption, sexual coercion, sexual exploitation, sexual assault, child pornography, computer hacking and wiretapping.

39 In April 2010 an offender from Alabama, USA, was sentenced to 18 years in prison after he admitted sending threatening emails on Facebook and MySpace extorting nude photos from more than 50 young women in Alabama, Pennsylvania and Missouri (Wilson, 2010).

40 In Wisconsin, New Berlin, Anthony Stancl, 18, received 15 years in prison in February 2010 after prosecutors said he posed as a girl on Facebook to trick male high school classmates into sending him nude cell phone photos, which he then used to extort them for sex (Ibid).

41 In the same year, a 31-year-old California man was arrested on extortion charges after authorities said he hacked into more than 200 computers and threatened to expose nude photos he found unless their owners posed for more sexually explicit videos. Forty-four of the victims were juveniles. Federal prosecutors said he was even able to remotely activate some victims' webcams without their knowledge and record them undressing or having sex (Ibid).

42 In October 2012, a Canadian teen girl began an online relationship with a boy, during which she sent him intimate photos of herself.[27] The boy then used the photos in an attempt to manipulate and coerce the girl into sending him a video of herself.[28] When she refused, the boy gained access to her email account and sent the photos to several of her email contacts. The boy was charged with making, possession and distribution of child pornography, extortion, and threatening death.[29]

43 In another case, "'In [i]n January 2013 a Glendale man allegedly hacked hundreds of online accounts and extorted some 350 women and teenage girls into showing him their naked bodies'" (Los Angeles News Online, Jan 29, 2013). This incident is further described as such:

> *The offender hacked into the women's Facebook, Skype and email accounts. He then changed the passwords to lock victims out of their own accounts and then searched emails or other files for naked or seminaked photos of the victims (Ibid). He then posed as a friend, persuading them to strip while he watched via Skype, captured images of them, or both. When the women discovered that the offender was posing as a friend, he often blackmailed them with the nude photos he had fraudulently obtained to coerce more stripping. In some cases, he's accused of posting the nude photos to the victims' Facebook pages when they refused his demands. (Ibid)*

VII. Age Play

44 "'Second lLife'" is not even immune from sexual offences. In everyday language, "'Second lLife'" is often referred to, as an online computer game.[30] Avatars are frequently called "'players'" and the conditions set up by "'Linden Lab'" are considered the rules of the game (Hoeren, 2009). The established Second Life practice of so-called "'age play'", in which users request sex with other players who dress up as child avatars, has encouraged a growth in players posing as children in order to make money (Kierkegaard, 2008). Age play is in world sexual activity between a child avatar and an adult avatar. Sex is an important feature in Second lifeLife. Participants can make their avatars look like anything they want and create software renderings of whatever equipment they want to use (Ibid). They even go to the extent of actually purchasing scripts and making the avatars engage in simulated sex.

C. Prevalence of Sexual Harassment in Cyberspace

45 Many authors refer to sexual harassment on the Internet and describe it as prevalent and risky. Leiblum and Döring (2002) argued that the Internet provides a convenient vehicle, commonly used, to force sexuality on women through non-social (logging into web pages) and social (interpersonal communication) uses of the Net.

46 Sexual harassment appears on the Internet in a peculiarly virulent form.[31] This is because there are many more men than women using online services, and each male user seems to spend more time online than female users.[32] Surveys suggest the proportions of people are around 94% male, and that the male presence is dominant in content. Also, the anonymity of the Net gives an atmosphere of seclusion, where the harasser feels that he may behave in an unacceptable manner with impunity.[33]

47 Casey & McGarth consider cyberspace as an ideal environment for sex offenders to commit sexual harassment and imposition because of its characteristics. Firstly, it is difficult to locate the IP address of cybercriminals (Lovet, 2009). Secondly, cybercriminals may use cryptography to encrypt evidence (Ibid). Thirdly, the transnational nature of cybercrime raises an issue because legal and repressive systems in the world are currently based on sovereign jurisdictions with borders. Frequently, in a cybercrime scenario, the attacker sits in country A, and without moving an inch, engages in cybercriminal action targeting a victim in country B. The theoretical problem is therefore: as follows: knowing the crime occurs in country B, while the criminal is in country A, how can the criminal be prosecuted and under which jurisdiction? (Ibid).

48 Cunneen and Stubbs (2000) reported an incident in which an Australian citizen solicited sex among Filipino women through the internetInternet in return for economic privileges. Cooper et al., (2002) mentioned the case of an internetInternet user with a paraphilia-related disorder who obsessively used chat rooms to communicate his sexual thoughts to women.

49 According to "Journal of Adolescent Health (47, 2010"), only 18% of youth use chat rooms, ; however, the majority of Internet-initiated sex crimes against children are initiated in chat rooms.[34] In 82% of online sex crimes against minors, the offender used the victim's social networking site to gain information about the victim's likes and dislikes.[35] 65% of online sex offenders used the victim's social networking site to gain home and school information about the victim.[36] 26% of online sex offenders used the victim's social networking site to gain information about the victim's whereabouts at a specific time.[37]

50 In 2006 one in seven kids received a sexual solicitation online. Over half (56%) of kids sexually solicited online were asked to send a picture; 27% of the pictures were sexually- oriented in nature. 44% per cent of sexual solicitors were under the age of 18.[38] 4 % of all youth Internet users received aggressive sexual solicitations, which threatened to spill over into "'real life"'. These solicitors asked to meet the youth in person, called them on the telephone or sent offline mail, money or gifts. Also, four per cent of youth had distressing sexual solicitations that left them feeling upset of extremely afraid.[39]

51 Of aggressive sexual solicitations of youth (when the solicitor attempted to establish an offline contact via in-person meeting or phone call), 73% of youth met the solicitor online. 80% of online offenders against youth were eventually explicit with youth about their intentions, and only 5% concealed the fact that they were adults from their victims. The majority of victims of Internet-initiated sex crimes were between 13 to 15 years old; 75% were girls and 25% were boys.[40]

52 In 2008, 14 % of students in 10th- to 12th grade have accepted an invitation to meet an online stranger in-person and 14 % of students, who are usually the same individuals, have invited an online stranger to meet them in-person.[41] 14 % of 7th- through 9th grade students reported that they had communicated with someone online about sexual things; 11 % of students reported that they had been asked to talk about sexual things online; 8 % have been exposed to nude pictures and 7 % were also asked for nude pictures of themselves online.[42] 59 % of 7th- through 9th grade victims said their perpetrators were a friend they know knew in-person; 36 % said it was someone else they know; 21 % said the cyber offender was a classmate; 19 % indicated the abuser was an online friend; and 16 % said it was an online stranger.[43] 9 % of children in 7th- through 9th grade have accepted an online invitation to meet someone in-person and 10 % have asked someone online to meet them in-person. 13 % of 2nd- through 3rd grade students report that they used the Internet to talk to people they do not know, 11 % report having been asked to describe private things about their body and 10 % have been exposed to private things about someone else's body.[44]

D. Legal Regulation

53 There have been calls in the United States for specific cyberstalking legislation (Elison et al., 1998). It is argued that victims of cyberstalking are inadequately protected as existing laws are too inflexible to cover online harassment (Ibid). Under this section,

we shall focus on the legal regulation of online sexual harassment in the USA, the United Kingdom and according to the Council of Europe & the European Union.

I. United States

54 Under 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, email, beepers or the Internet.[45]

55 Although 18 U.S.C. 875 is an important tool, it is not an all-purpose anti-cyberstalking statute. First, it applies only to communications of actual threats. Thus, it would not apply in a situation where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat). Also, it is not clear that it would apply to situations where a person harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person.[46]

56 Certain forms of cyberstalking also may be prosecuted under 47 U.S.C. 223. One provision of this statute makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy abuse, harass, or threaten any person at the called number. The statute also requires that the perpetrator not reveal his or her name. (Ssee 47 U.S.C. 223(a)(1)(C)). Although this statute is broader than 18 U.S.C. 875 – in that it covers both threats and harassment – Section 223 applies only to direct communications between the perpetrator and the victim. Thus, it would not reach a cyberstalking situation where a person harasses or terrorizes another person by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person. Moreover, Section 223 is only a misdemeanormisdemeanour, punishable by not more than two years in prison.

57 In addition, Title VII of the Civil Rights Act of 1964, a federal law, prohibits sex harassment in employment, including harassment based on sex, pregnancy, childbirth, and related medical conditions. The Equal Employment Opportunity Commission (EEOC) is the federal agency charged with enforcing these provisions. Under Title VII, online content can be considered illegal sexual harassment if it is unwelcome, of a sexual nature, and is severe or pervasive enough to create a hostile work environment.[47]

58 President Clinton signed a bill into law in October 1998 that protects children against online stalking. The statute, 18 U.S.C. 2425, makes it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity.[48] While this new statute provides important protections for children, it does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes.

59 California was the first state to pass a stalking law in 1990, and all the other states have since followed. The first US State state to include online communications in its statutes against stalking was Michigan in 1993. Under the Michigan Criminal Code, "'harassment'" is defined as 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. Unconsented contact under the Michigan Code specifically includes sending mail or electronic communications to that individual. A number of other US States states besides Michigan have anti-stalking laws that include electronic harassment. These states include: Arizona,[49] Alaska,[50] Connecticut,[51] New York,[52] Oklahoma,[53] and Wyoming.[54]

60 In the US, Michigan was the first state to charge someone with online stalking (Ellison, 1998). Andrew Archambeau refused to stop sending email messages to a woman he met through a computer dating agency and was charged under Michigan stalking laws in May 1994. Archambeau's lawyers sought to challenge the constitutionality of these anti-stalking laws. In January 1996, however, Archambeau however pleaded no contest to the stalking charge (Ibid).

61 McGraw highlights further difficulties in using anti-stalking legislation to combat online harassment (Ellison et al., 1998). In a number of states, McGraw explains, the language of the statute requires physical activity, thus exempting email harassment (Ibid). Some state statutes also require a "'credible threat'" of serious physical injury or death. In such states, email harassment is unlikely to meet this standard (Ibid). This was true in the Jake Baker case.[55] Using the pseudonym "'Jake Baker'", Abraham Jacob Alkhabaz, a student at the University of Michigan, posted stories to a newsgroup called "'alt.sex.stories'". One of Baker's stories described the rape, torture and murder of a woman. Baker used the real name of a fellow student from the University of Michigan for the victim. Baker also corresponded with a reader of the story via email who used a pseudonym of "'Arthur Gonda'" in Canada. In over 40 emails both men discussed their desire to abduct and physically injure women in their local area. Baker was arrested and held without bail and was charged with the interstate transmission of a threat to kidnap or injure another. Though most described Baker as a quiet

"'computer geek'" with no history of violence, the stories he posted on the Internet were horrific and disturbing. Nevertheless, a US District Court Judge dismissed the case against Baker, ruling that the threats lacked a specific intent to act or a specific target required under the Michigan stalking law.

62 Finally, federal legislation is needed to fill the gaps in current law. While most cyberstalking cases will fall within the jurisdiction of state and local authorities, there are instances – such as serious cyberharassment directed at a victim in another state or involving communications intended to encourage third parties to engage in harassment or threats – where state law is inadequate or where state or local agencies do not have the expertise or the resources to investigate and/or prosecute a sophisticated cyberstalking case. Therefore, federal law should be amended to prohibit the transmission of any communication in interstate or foreign commerce with intent to threaten or harass another person, where such communication places another person in fear of death or bodily injury to themselves or another person. Because of the increased vulnerability of children, the statute should provide for enhanced penalties where the victim is a minor. Such targeted, technology-neutral legislation would fill existing gaps in current federal law, without displacing the primary law enforcement role of state and local authorities and without infringing on First Amendment-protected speech.

II. United Kingdom

63 Existing UK laws are sufficiently flexible to encompass online stalking, email harassment, child pornography offences and online grooming.[56] The Telecommunications Act 1984, Section 43, for example, makes it an offence to send by means of a public telecommunications system a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. For the purposes of the Act, a public telecommunication system is any telecommunications system[57] so designated by the Secretary of State and is not confined to British Telecom's telephone system. The Act therefore potentially covers the sending of offensive email messages in some instances.[58] The Act will not apply, however, in cases where the data is transmitted by using a local area network unless part of the transmission is routed through a public telecommunications system.[59] So, whether the Act applies to email harassment will depend upon the telecommunications network used, but the Act is not limited to voice communications.

64 The Protection from Harassment Act 1997 may also be invoked in cases of online harassment. This Act provides a combination of civil and criminal measures to deal with stalking. It creates two criminal offences, the summary offence of criminal harassment[60] and an indictable offence involving fear of violence.[61] Under Section 2 it is an offence to pursue a course of conduct which amounts to the harassment of another where the accused knew or ought to have known that the course of conduct amounts to harassment. A person commits an offence under Section 4 if he pursues a course of conduct which causes another to fear, on at least two occasions, that violence will be used against him. It is sufficient that the accused ought to have known that his course of conduct would cause the other to so fear on each of those occasions.

65 The Act also gives courts the power to impose restraining orders on convicted defendants, prohibiting them from further conduct which may be injurious to the victim. Breach of such an order carries a potential sentence of five years' imprisonment. Harassment includes both alarm and distress, though harassment, alarm and distress are not specifically defined in the Act and so these terms are to be given their ordinary meaning. The range of behaviour covered by the Act is thus potentially extremely wide. The sending of abusive, threatening emails or the posting of offensive material would constitute an offence under Section 2 of the Act, as long as it amounts to a course of conduct (for example, more than one e-mail must be sent) and the offender knew or ought to have known that his conduct amounted to harassment.

66 On a different note, sections 14 & 15 of the Sexual Offences Act 2003 make it an offense to arrange a meeting with a child, for oneself or someone else, with the intent of sexually abusing the child. The meeting itself is also criminalized. The Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 introduced a similar provision for Scotland.

67 Thus, a crime may be committed even without the actual meeting taking place and without the child being involved in the meeting (for example, if a police officer has taken over the contact and pretends to be that child).

68 In January 2012, Scotland Yard investigated what was believed to be one of the first cases of cyber-stalking involving Twitter in the United Kingdom.[62] The Metropolitan Police confirmed it examined claims that a 37-year-old man has had allegedly been targeting two women who claim to have received offensive, racist and sexually demeaning tweets and emails. It is believed the alleged harassment has had gone on since the beginning of November 2011 and involved as many as five victims.[63] The pair are were thought to have been targeted because of their views on Israel and the Iraq war. According to those familiar with the case, the man has had allegedly sent more than 16,000 tweets to the victims and tried to contact one of them at work. Although they blocked

the tweets, the sender has varied his Twitter address as his messages have becoame more threatening. His alleged tweets included the warnings: "'I am in a war to the death. Stay well clear for your own safety. Don't ever tweet me again'"; "'Remember watch your back 24 hours a day 7 days a week for life'"; and "'Want me to tweet you your death place?'" Twitter has consequently taken down all of the offensive tweets.[64]

III. The Council of Europe

69 The Council of Europe has pointed to the importance of addressing cyberbullying in several documents, such as the Recommendation on empowering children in the new information and communications environment (Council of Europe, 2006), the Declaration on protecting the dignity, security and privacy of children on the Internet (Council of Europe, 2008), the Recommendation on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment (Council of Europe, 2009) and the Recommendation on the protection of human rights in social networks (Council of Europe, 2012).

70 Aside from these recommendations and declarations, the European Convention on Human Rights (ECHR), one of the cornerstones of human rights protection in Europe, provides guarantees with regard to the freedom of expression (article Article 10 ECHR) and the right to privacy (article Article 8 ECHR).

71 The right to freedom of expression protects a broad range of speech. Already in 1976, the European Court of Human Rights (ECHR) argued in the case Handyside v. UK that article Article 10 is applicable not only "'to information or ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb'" (Lievens, 2012). Whether an act which can be classified as cyberbullying (for instance, a series of negative comments on someone's Facebook wall which may be hurtful to the person who is targeted) may be considered a protected 'expression' or not will need to be judged on a case-by-case basis, taking all circumstances into account (Ibid). An important element in this delicate consideration might be the motivation or intent of the offender. However, it is important to note that article Article 10 is not an absolute right. According to paragraph 2, restrictions on the freedom of expression may be imposed if they are (1) prescribed by law, (2) introduced with a view to specified interests such as the protection of health or morals or the protection of the reputation or the rights of others, and (3) necessary in a democratic society (Ibid).

72 Acts of cyberbullying may also infringe on the right to privacy of an individual, guaranteed by article Article 8 ECHR. An interesting case in this context is K.U. v. Finland (Lievens, 2012). The case dealt with an advertisement on a dating site, placed by unknown persons, in the name of a 12-year-old boy without his knowledge. This advertisement included the age of the boy, a description of his physical characteristics, a link to his website which contained a picture and a telephone number, and a statement that he was seeking an intimate relationship with a boy. At the time of the facts it was not possible according to Finnish legislation to obtain the identity of the person who placed the advertisement from the Internet provider (Ibid). The Court considered the applicability of article Article 8 ECHR indisputable and emphasised that "'[c]hildren and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives'". The fact that no effective steps could be taken to identify and prosecute the person who placed the advertisement, and thus the failure by the Finnish government to fulfillfulfil its positive obligation to provide a framework of protection, led the Court to decide that article Article 8 ECHR had been violated (Ibid).

IV. The European Union

73 In December 2011, the European Union adopted the Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child pornography.[65] The approach of this Directive to offences concerning child pornography is similar to the approach of the Lanzarote Convention.[66] Article 5 contains the (range of) punishments that should be applied to the acquisition, possession, knowingly obtaining access to, distribution, dissemination, transmission, offering, supplying or making available of child pornography. In addition, article Article 8 specifically allows Member States to decide whether article Article 5(2) and (6) apply to the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse. As recital 20 put it:

> *This Directive does not govern Member States' policies with regard to consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development, taking account of the different cultural and legal traditions and of new forms of establishing and maintaining relations among children and adolescents, including through information and communication technologies. These issues fall outside of the scope of this Directive. Member States which avail themselves of the possibilities referred to in this Directive do so in the exercise of their competences.*

74 The European Union has also repeatedly pointed out that cyberbullying is an important issue that needs to be tackled, for instance in the framework of the Safer Internet Programme, or in the European Strategy for a better internetInternet for children (European Commission, 2012). With regard to legislation, the most relevant and applicable provisions are included in the Data Protection Directive. As the European Data Protection Supervisor has stated:

75 *"When individuals put information about third parties, for example, comments on their appearances or behaviors, independently of whether this constitutes legally cyber-harassment, they disclose personal information of their victims. For example, their real name, their address, school, etc. The principles and obligations embodied in the EU data protection legislation are fully applicable to the disclosure of this information, which under EU legislation qualifies as personal data, in forums or social networks. For example, data protection legislation requires informing and in many cases obtaining the consent of individuals before publishing information that relates to them. Obviously, those engaged in cyber harassment do not inform, much less ask for the consent of their victims to publish their personal data, thus, automatically breaching data protection legislation". (Lievens, 2012).*

76 It is possible to file a complaint with the national Data Protection Authority or go to court in case of a violation of the Data Protection Directive.

E. Tackling Online Sexual Harassment

77 From logical, theoretical, and pragmatic perspectives, knowing the associated problem, and risks associated therewith, and the ills resulting therefrom them is an indispensable step towards a possible solution. Furthermore, such a determination constitutes an integral part of devising effective vaccines and serums to eradicate and prevent this evil. Having discussed the diverse aspects of the vexing problem of online sexual harassment, we shall now address some of the its potential solutions thereto. Thus, we shall analyzeanalyse in this section the importance of establishing multinational public – -private collaboration, educating internetInternet users, perpetrators and victims and regulating the liability of internetInternet service providers.

I. Establishing Multidimensional Public-private Private Collaboration

78 To tackle online sexual harassment effectively, it is essential to establish multidimensional public-private collaboration between law enforcement agencies, the information technology industry and ISPs. Without efficient private –- public cooperation, online sexual harassment will never be tackled effectively.

79 The private sector needs to be assured of a confidential relationship in which information can be exchanged for investigative and intelligence purposes. Furthermore, law enforcement, prosecutors and judges often do not have the necessary technical means and knowledge to investigate and prosecute these types of crimes. Law enforcement agencies must work in partnership with those who will influence the operating environment so that all concerned can better anticipate changes in criminal behaviorbehaviour and technological misuse.

II. Using Innovative Software

80 New and innovative software programs which enable users to control the information they receive are constantly being developed. There are, for example, technical means by which internetInternet users may block unwanted communications. Tools available include "'kill"' files and "'bozo"' files which delete incoming email messages from individuals specified by the user. Such tools are included with most available email software packages. In addition, programs such as Eudora and Microsoft Outlook have filter features which that can automatically delete emails from a particular email address or those which contain offensive words. Chat- –room contact can be blocked as well.

81 There is also specially designed software to filter or block unwanted email messages. These tools, such as CyberSitter[67] and Netnanny,[68] are designed mainly to block the access of children to sexually explicit websites and newsgroups, but can also be used to filter out and block email communications. Some of this software can additionally filter words through the incoming and outgoing email messages. The mandatory use of such software, especially at access level, by libraries and ISPs is criticized within the US, because the decisions taken to block certain websites are arbitrary and within the discretion of the private companies that develop these systems (Ellison et al., 1998). They are also defective, since most of them block such websites as the Middlesex County Club or Mars Explorer, while trying to block the word "'sex"'; or block websites by looking at the keywords in the meta-tags offered by the individual html files (Ibid). These tools may be of some use to victims of cyber-stalkers to filter out unwanted messages, nonetheless.

82 These approaches may be useful in situations where the communications are merely annoying but may be useless in situations in which threatening communications are not received by the intended victim. A victim who never "'receives"' the threat may not know he or she is being stalked, and may be alerte-

red, for the first time, when the stalker shows up to act on his or her threats.

III. Educating Internet Users, Perpetrators and Victims

83 The education of potential perpetrators on how to behave online is one of the important steps to in tackle tackling internetInternet sexual harassment. In addition, the education of internetInternet users and victims is the first step towards self-protection.

84 The reason educational approaches are so vital is because they can help teach perpetrators how to behave in and victims how to respond to a wide variety of situations (Szoka et al., 2009). Education teaches lessons and builds resiliency, providing skills and strength that can last a lifetime. That was the central finding of a blue-ribbon panel of experts convened in 2002 by the National Research Council of the National Academy of Sciences to study how best to protect children in the new, interactive, "'always-on"' multimedia world (Ibid). Under the leadership of former U.S. Attorney Attorney-General Richard Thornburgh, the group produced a massive report that outlined a sweeping array of methods and technological controls for dealing with potentially objectionable media content or online dangers (Ibid). Ultimately, however, the experts used a compelling metaphor to explain why education was the most important strategy on which parents and policymakers should rely (Ibid):

> *"Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning. Does this mean that parents should not buy fences, alarms, or locks? Of course not—because they do provide some benefit. But parents cannot rely exclusively on those devices to keep their children safe from drowning, and most parents recognize that a child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify".*

85 In addition, there are many websites and books which provide information for self-protection from cyber-stalkers for online users. Women are also advised, where possible, to adopt either a male or gender neutral user name. Internet users should regularly check their online profile (finger files) or biography to see what information is available to a potential stalker. They are also advised to understand how the privacy settings of their social network sites work and customize these privacy settings to block strangers from obtaining personal information.

IV. Regulating the Liability of Internet Service Providers

86 Although the status of ISPs in some European countries is very much debatable , – for instance, whether they are publishers, distributors or common carriers – , the Internet industry should also have a similar responsibility (Chawki, 2009). The tricky question remains: how to achieve this? While it may be difficult to control the content of the Internet, its provision by the ISPs may be controlled. In France, for example, La Loi pour la Confiance dans l'Economie Numérique LEN defines the liability and clarifies the role and responsibility of ISPs.[69] The objective of this law is to provide impetus to the digital economy in France in order to reinforce confidence in the use of such new technology and thereby ensure its growth.[70] This law has transposed the E-commerce Directive 2000/31/CE into French law together with part of the Directive on Privacy and Electronic Communications 2002/58/EC. The (LEN) has been heavily modified during its passage through the pipeline of parliamentary procedure,[71] and has been the subject of criticism and has met with vociferous opposition from a number of quarters, in particular ISPs and user groups, claiming the draft (LEN) threatened free expression on the Internet and placed a significant and unfair burden on ISPs to censor online content (Taylor, 2004). Many actions have also been undertaken by EDRI[72] member IRIS, which launched a petition against this provision in the draft law, together with the French Human Rights League, the G10-solidaires association of trade- unions, and two non-commercial providers.[73] The petition has been signed by more than 8,000 individuals and 170 organisations.

87 Other actions have been undertaken by ODEBI, an association of Internet users, and by Reporters without Borders (RSF).[74] Considerable lobbying continued prior to the second reading of the Bill by the Senate, which took place on 8th April, 2004. At the second reading, the Senate voted to adopt the (LEN), but with certain crucial modifications. Actually, article Article 6 provides that ISPs are not liable for information transmitted or hosted unless they have actual knowledge of illegal activity or information of facts or circumstances from which the illegal activity or information is apparent; or if upon obtaining such knowledge or awareness they act expeditiously to remove or to disable access to the information. With respect to contractual provisions on an ISP's liability, it should be noted that these provisions are not enforceable against third parties in France. As a result, a contractual exemption of liability cannot be used with regard to a third party (not subscribing with an ISP) who has suffered harm as a result of unlawful content broadcast on the networks, for example, or an act of infringement. person habitually engaged in prostitution.[75]

88 On a different note, The Association des Fournisseurs d'Accès et des Services Internet (AFA)[76] requires its members to offer their customers tools for (i) the filtering of illegal or harmful content; (ii) the regulation of unwanted bulk mail; and (iii) a point of contact for the reporting of illegal or harmful content. In this way the responsibility for receiving or sending content is passed back to the customers – the customers are given the tools to determine themselves what information (illegal, harmful, necessary, etc.) they would like to receive or send.[77] The AFA makes a specific reference to the workings of the Internet Content Rating Association (ICRA) in offering systems capable of filtering content (both against illegal and harmful content and for the protection of minors) and members are expected to abide with by ICRA's procedures. The implication of the rules relating to illegal and harmful content is as follows: [78]

- An ISP has no responsibility to monitor and remove material on its own initiative;
- If the ISP removes information at the request of law enforcement agencies or private organisations acting as monitors of Internet content it should not be held responsible for the removal;
- If on the other hand an ISP does not follow the requests of law enforcement agencies and private organisations then it is in breach of these rules and may be liable for the consequences.

89 AFA does not have a formal complaints mechanism. When complaints are received they are passed onto the member and it is up to the member to handle the complaint.[79] The Statute founding AFA as an association, however, allows for a member to be expelled from the association, amongst other reasons, if the member acts against rules set by the AFA. In both cases, member ISPs apparently follow the rules of their association.[80] It can be argued that in certain circumstances, it is in the ISP's own interest to do so for this guarantees a certain amount of protection against liability. An ISP that does not follow the rule of its own association exposes itself to legal liability. Furthermore, AFA is represents strong lobby groups with government and with policy groups. It thus benefits an ISP to be a member of the association and not risk expulsion.[81]

F. Future Prospects

90 It's clear that online sexual harassment is not going to disappear. While cybercrime is an unwanted side effect of the Internet age, it's also part of a broader crime landscape. If there's a use for something, someone will always find a way to abuse it, and this includes computer technology and the connectivity provided by the Internet. Crime can never be eliminated, so tackling online sexual harassment is less about "'winning the war"' than about mitigating the risks associated with using the Internet. To manage the risk, the global society clearly needs a legal framework, together with appropriate and effective law enforcement agencies. There's little question that law enforcement agencies have developed increasing expertise in dealing with high-tech crime during the last decade, including joint policing operations across national borders. This must be further developed if we are to deal effectively with online sexual harassment. In particular, the extension of international legislation beyond developed countries, and the development of a "'cyber-Interpol"' to pursue criminals across geo-political borders, would contribute greatly to the fight against online sexual harassment. Law enforcement, however, is only part of the solution. We also need to ensure that individuals understand the risks and have the knowledge and tools to minimise their exposure to this threat. This problem is exacerbated by the growing number of people accessing the Internet for the first time. Society must find imaginative and varied ways of raising public awareness about online sexual harassment and about methods which can be used to mitigate the risks. The "'information super-highway"' is no different to any other public road. We need well-designed roads, safe cars, clear signs and competent drivers. In other words, we need a blend of appropriate legislation, effective policing and public awareness.

G. Conclusion

91 Due to the seeming invisibility and anonymity of the Internet, online sexual harassment has become a serious and social concern. The solution is not necessarily to avoid the Internet and other digital technologies; rather, more Internet safety education and prevention information are needed to raise awareness for youths, adults and practitioners. Adults, including helping professionals, who are not confident and do not feel well-versed in new digital technologies, must acknowledge that the Internet is a new space for individuals to connect and converse, both positively and negatively. Having the knowledge and skills to help online sexual harassment victims is necessary in this new era.

References:

A. Barak, Sexual Harassment on the Internet, Social Science Computer Review , vol. 23 no. 1, [2005].

A. Barak, Cross – c-Cultural Perspectives on Sexual Harassment. In W. O'Donohue (Ed.) Sexual Harassment: Theory, Research & Treatment, (Boston, Allyn & Bacon), [1997].

A. Barak & A. King, The Two Faces of the Internet: Introduction to the Special Issue on the Internet and Sexuality. CyberPsychology and Behavior, 3, [2000].

A. Chaudhuri, Are Social Networking Sites a Source of Online Harassment for Teens? Evidence from Survey Data, Net Institute, Online Working Paper, [2008].

A. Cooper, I. McLoughlin, P. Reich, J. Kent-Ferraro, Virtual Sexuality in the Workplace: A Wake-up Call for Clinicians, Employers and Employees. In A. Cooper (Ed.) Sex and the Internet: A Guidebook for Clinicians, (New York, Brunner – Routledge), pp. 109 – 128, [2002].

A. Cooper, G. Golden & J. Kent-Ferraro, Online Sexual Behaviors in the Workplace: How Can Human Resource Departments and Employee Assistance Programs Respond Effectively? Sexual Addiction and Compulsivity, 9, [2002].

B. Szoka et al., Cyberbullying Legislation: Why Education is Is Preferable to Regulation, The Progress & Freedom Foundation, Volume 16, Issue 12, [2009].

C. Cunneen & J. Stubbs, Male Violence, Male Fantasy and the Commodification of Women through the Internet. Interactive Review of Victimology, 7, [2000].

C. Wilson, Feds: Online Sextortion of Teens on the Rise, Online, NBCNews, available at <www.nbcnews.com>, (visited (16/3/ March 2013).

D. Harvey, Cyberstalking and Internet Harassment: What the Law Can doDo, Online, Internet Safety Group, available at <www.netsafe.org.nz>, [2003].

D. Sacco et al., Sexting: Youth Practices and Legal Implications, Berkman Center for Internet & Society, Research Publication No. 2010 – 8, [22 June, 22, 2010].

D. Taylor, Internet Service Providers (ISPs) and their Responsibility for Content under New French Legal Regime, Computer Law and Security Report, Vol. 20, Issue 4.

E. Lievens, Bullying & Sexting in Social Networks from a Legal Perspective: Between Enforcement and Empowerment, ICRI Working Paper 7/20102, [20 June 20, 2012].

F. Till, Sexual Harassment: A Report on the Sexual Harassment of Students. (Washington DC, Advisory Council on Women's Educational Programs), [1980].

G. Lovet, Fighting Cybercrime: Technical, Judicial & Ethical Challenges, Virus Bulletin Conference, September [2009], available at <www.fortiguard.com>.

J. Morahan- – Martin, Women and the Internet: Promise and Perils. CyberPsychology and Behavior, 3, [2000].

J. Richman et al., Sexual Harassment and Generalized Workplace Abuse among University Employees: Prevalence and Mental Health Correlates, American Journal of Public Health, 89, [1999].

J. Suler, To Get What You Need: Healthy and Pathological Internet Use. CyberPsychology and Behavior, 2, [1999], 385 – -394.

K. Mitchell, D. Finkelhor & J. Wolak, The Exposure of Youth to Unwanted Sexual Material on the Internet: A National Survey of Risk, Impact, and Prevention. Youth & Society, 34, [2003].

L. Ellison & Y. Akdeniz, Cyberstalking: The Regulation of Harassment on the Internet, Criminal Law Review, December, [1998].

L. Fitzgerald, M. Gelfand & F. Drasgow, Measuring Sexual Harassment: Theoretical and Psychometric Advances. Basic and Applied Social Psychology, 17, [1995].

L. Fitzgerld, V. Magley, F. Drasgow & C. Waldo, Measuring Sexual Harassment in the Military, The Sexual Experiences Questionnaire (SEQ – DoD). Military Psychology, 11, [1999].

M. Chawki, Online Child Sexual Abuse: The French Response, Journal of Digital Forensics, Security & Law, Vol. 4, No. 4, [2009].

M. de la Cerna, Sextortion, [Online], Cebu Daily News, available at: <www.newsinfo.inquirer.net>, (visited 16/03/2013).

McGuire & E. Casey, Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace. Journal of the American Academy of Psychiatry and the Law, 30, [2002].

N. Levy et al., Bullying in a Networked Era: A Literature Review, Berkman, Research Publication No. 2012 – 17, [2012], available online.

P. Bocij, Cyberstalking: Harassment in the Internet Age and How to Protect Your Family, Westport, CT: Praeger, [2004].

Q. Li, Gender and CMC: A Review on Conflict and Harassment, Australasian Journal of Educational Technology, 2005, 21 (3), pp. 382 – 406.

R. Kool, Prevention by All Means? A Legal Comparison of the Criminalization of Online Grooming and Its Enforcement, Utrecht Law Review, Vol. 7, No. 3, [2011].

S. Kierkegaard, Cybering, Online Grooming and Age Play, Computer Law & Security Report, 24, [2008].

S. Leiblum & N. Döring, Sex and the Internet: A Guidebook for Clinicians, New York: Brunner- – Routledge, [2002].

S. Schenk et al., Cyber- – Sexual Harassment: The Development of the Cyber- – Sexual Experiences Questionnaire, McNair Journal, Vol. 12, Issue 1, [2008].

T. Hoeren, The European Liability and Responsibility of Providers on Online – Platforms Such as Second Life , JILT, 1 [2009].

1 Mohamed CHAWKI, LL.B, BA, LL.M, Ph.D is a Senior Judge; Founder and Chairman of the International Association of Cybercrime Prevention (IACP) , Paris, France; & and Research Fellow at the Center of Terrorism Law , St. Mary's University School of Law, Texas, USA. ; Email: chawki@cybercrime-fr.org; . Yassin el SHAZLY, LL.B, LL.M, Ph.D is a Senior Lecturer at the Faculty of Law, University of Ain-Shams, Cairo, Egypt; & and Legal Expert at the National Telecommunication Supervisory Authority. ; Email: yassin_shazly@hotmail.com.

2 See B. Roberts & R. Mann, Sexual Harassment in the Workplace: A Primer, available at: <www3.uakron.edu>, (visited 14/02/ February 2013).

3 See Unwanted Sexual Attention, available at: <www.getiton/nhs.uk>, (visited 17/03/ March 2013).

4 Ibid.

5 See The Center for Health and Gender Equity, Ending Violence against Women, [1999], available at <www.info.k4health.org>, (visited 14/02/ February 2013).

6 See Internet Harassment, available at <www.unc.edu>, (visited 14/02/ February 2013).

7 Ibid.

8 See N. Goodno, Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws , Missouri Law Review, Vol. 72, [2007].

9 Ibid.

10 See ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, [October 2007]. Available at <www.enisa.europa.eu>, (visited 18/03/ March 2013).

11 Ibid.

12 See ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, [October 2007]. Available at <www.enisa.europa.eu>, (visited 18/03/ March 2013).

13 Ibid.

14 Ibid.

15 See E. Porterfield, Facebook Cyberstalking Shocker: Preteen Girls Charged In Issaquah Case, available at <www.huffingtonpost.com> (visited 18/03/ March 2013).

16 Ibid.

17 See ENISA Position Paper No. 1 "'Security Issues and Recommendations for Online Social Networks"', edited by Giles Hogben, [October 2007]. Available at <www.enisa.europa.eu>, (visited 18/03/ March 2013).

18 Ibid.

19 Ibid.

20 Ibid.

21 Ibid.

22 See Online Grooming Accused in Court, available at <www.theherald.com.au> , (visited 21/03/ March 2013).

23 Ibid.

24 Ibid.

25 See Sextortion, available at <www.gistmania.com>, (visited 17/03/ March 2013).

26 Ibid.

27 See Teen Arrested on Sexting Extortion Charges, available at <www.newstalk1010.com>, (visited 18/03/ March 2013).

28 Ibid.

29 Ibid.Ibid

30 See <www.secondlife.com>.

31 See Catherine Waerner, Thwarting Sexual Harassment on the Internet, available at: <www.uow.edu.au>, (visited (14/3/ March 2013).

32 Ibid.

33 Ibid.

34 See Predator Statistics, available at <www.internetInternetsafety101.org> , (visited 18/03/ March 2013).

35 Ibid.

36 Ibid.

37 Ibid.

38 Ibid.

39 Ibid.

40 Ibid.

41 Ibid.

42 Ibid.

43 Ibid.

44 Ibid

45 See Cyberstalking, available at <www.cyberguards.com> , (visited 21/03/2013).

46 Ibid

47 Ibid.

48 Ibid.

49 Arizona Criminal Code (1995): 13 -– 2921.

50 Alaska Criminal Law Sec. 11.41.270.

51 Connecticut Penal Code Sec. 53a -– 183.

52 New York Penal Code § 240.30.

53 Oklahoma Code (1996): § 21 -– 1173.

54 Wyoming Code, 6 – 2 -– 506.

55 See United States v. Baker, 104 F. 3d 1492, [Jan. 29, 1997].

56 See Sexual Offences Act 2003, Sections 45 and 15.

57 A 'telecommunications system"' is defined in section 4(1) of the Telecommunications Act 1984 as "'a system for the conveyance, through the agency of electric, magnetic, electromagnetic, electro-chemical or electro-mechanical energy, of: (a) Speech, music and other sounds. (b) Visual images. (c) Signals serving for the impartation.....of any matter otherwise than in the form of sounds or visual images..."'.

58 The Criminal Justice and Public Order Act 1994, s.92 increased the maximum fine for an offence under section 43 to level 5 from level 3 and made it an imprisonable offence with a maximum term of six months. The new sentencing powers brings the penalty more into line with the maximum sentence for transmitting indecent or obscene material through the post (which is 12 months' imprisonment) contrary to section 11(2) of the Post Office Act 1953.

59 Also note that the Malicious Communications Act 1988 s.1 creates an offence of sending letters which convey, inter alia, threats with the purpose of causing distress or anxiety. The

Act does not however cover telecommunications messages, however.

60 A person guilty of this offence is liable to imprisonment for a term not exceeding six months: s.2(2).

61 A person guilty of this offence is liable to imprisonment for a term not exceeding five years: s.4(4).

62 See Cyberstalker Targets Women in 16,000 Tweets, available at <www.quarduian.co.uk>, (visited 20/03/ March 2013).

63 Ibid.

64 Ibid.

65 See Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography.

66 Following the ratification by the Netherlands on 1 March 2010 and San Marino on 22 March 2010, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) entered into force on 1 July 2010.

67 See <www.cybersitter.com>.

68 See <http://www.netnanny.com/netnanny>.

69 Before adopting this law, the responsibility of ISPs was governed by the French law n°2000-719 of 1st August 2000. Under this law, ISPs were liable under French civil or criminal responsibility for the illegal content of the web sites to which they provide access, only if they have not promptly undertaken the appropriate measures to block access to such content after a judicial decision. See Estelle Halliday v Valentin Lacambre.

70 « 'Elle a pour objectif d'adapter la législation actuelle au développement de l'économie numérique afin de renforcer la confiance dans l'économie électronique et d'assurer le développement de ce secteur, tout en établissant un cadre juridique stable pour les différents acteurs de la société de l'information' ». Sénat (2007), Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Report, Paris. Available at <www.senat.frwww.senat.fr>.

71 In fact, the Senate has deleted the amendments to Article 2 of the LEN covering the regime governing the responsibility of ISPs that had been included by the National Assembly. This thereby removed the specific obligation to monitor certain types of content, including paedophilepedophile and racist material, which undermined the general principle of no obligation to monitor content generally, ; See see D. Taylor op. cit. p. 270.

72 European Digital Rights was founded in June 2002. Currently 35 privacy and civil rights organisations have EDRI membership. They are based or have offices in 21 different countries in Europe.

73 See French Draft Law Obliges Providers to Monitor Internet, available at <www.edri.orgwww.edri.org>.

74 Ibid.

75 Article 225 – 6.

76 The AFA was created in 2000; it is the amalgamation of two previous associations: the Association Française des Professionnels de l'Internet created in 1996 and the Association des Fournisseurs d'Accès à des Services en ligne et à l'Internet created in 1997. Both associations were set up mainly to define common practices regarding illegal content, especially child pornography.

77 See J. Bonnici, Internet Service Providers and Self –Regulation: A Process to Limit Internet Service Providers Liability in Cyberspace, available at <www.rug.nl>.

78 Ibid.

79 Ibid.

80 Ibid.

81 Ibid.