Cyber-stalking: the Regulation of Harassment on the Internet

By Louise Ellison and Yaman Akdeniz *

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

Summary: *This article highlights the issues surrounding on-line harassment and asks whether potential victims are adequately protected by existing national laws. It also examines the unique law enforcement problems which the Internet presents as well as addressing the implications legal regulation of the Internet may have for free speech and privacy on-line. Non-legal means of tackling harassment on the Internet are also explored.*

Introduction

Recent years have seen a series of "moral panics" regarding information accessible on the Internet and its use for criminal activity. These include the availability of sexually explicit material,[1] the use of the Internet by paedophiles to distribute child pornography,[2] the use of the Internet by Neo-Nazis and other racist groups,[3] the availability of hate speech and bomb-making instructions[4] and the use of encryption technology to secure private communications by terrorists and organised crime.[5] In reality, these fears are largely misplaced; while the Internet tends to produce extreme versions of problems, it rarely produces genuinely new ones.

The phenomenon of cyber-stalking and on-line harassment looks set to be the focus of the next Internet-related moral panic. In the US, a number of states have already introduced

---

* Louise Ellison is a Lecturer in Law at the University of Reading and Yaman Akdeniz is a Ph.D. student at the CyberLaw Research Unit, Faculty of Law, University of Leeds. The authors would like to thank Professor Clive Walker, Director of Centre for Criminal Justice Studies, University of Leeds for his comments on this article.

1 See Elmer-Dewitt, P., "On a screen near you: Cyberporn" *Time*, 3 July 1995; Rimm, M., "Marketing Pornography on the Information Superhighway" [1995] 83 *Georgetown Law Journal*, 1839. Note that Marty Rimm's 18 month study was later found to be misleading because it was based upon the many adult-oriented BBSs all around the US but not the Internet. For a critique of the Rimm study see Wallace, J., & Mangan, M., *Sex, Laws, and Cyberspace: Freedom and Censorship on the Frontiers of the Online Revolution*, (New York: Henry Holt & Company, 1996)

2 See "Paedophiles use encoding devices to make secret use of Internet" *The Times*, 21November 1995; "Two jailed for child porn on Internet" *The Daily Telegraph*, 25 May 1996; "Use of Computer Network for Child Sex Sets off Raids" *New York Times* September 14, 1995; "Minister calls for Internet controls" *The Daily Telegraph*, March 22, 1996; "Six years for priest who broadcast abuse of boys to Internet paedophiles", *The Daily Telegraph*, November 13, 1996.

3 See US Anti-Defamation League Report, "High-Tech Hate: Extremist Use of the Internet," October 1997.

4 See "Youths held after pipe-bomb blasts," *The Daily Telegraph*, 5 March 1998.

5 See Denning, D. E., and Baugh, Jr., W. E, "Cases Involving Encryption in Crime and Terrorism," October 1997, <http://guru.cosc.georgetown.edu/~denning/crypto/cases.html>. But see also Global Internet Liberty Campaign, *Cryptography and Liberty*, 1998, at <http://www.gilc.org/crypto/crypto-survey.html>, Akdeniz, Y., "No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights," (1998) *Web JCLI* 1.

specific cyber-stalking legislation. In the UK, extensive press coverage of stalking cases, which focused upon the bizarre and menacing behaviour of stalkers and the devastating effect stalking had on the lives of victims, ensured its place as the crime of the nineties.[6] The stalking debate within the UK was fuelled by a number of high-profile acquittals which served to highlight the deficiencies of both civil and criminal law in dealing with those who engage in stalking activity.[7] In March 1996, Charles Wilson was found not guilty of intentional harassment, having allegedly plagued Charlotte Sell for two years. The magistrate in the case, Geoffrey Breen, stated that while Sell had clearly been caused considerable alarm and distress by the defendant's actions, what the defendant had done amounted to stalking but stalking was not a criminal offence.[8] Dennis Chambers allegedly waged a campaign of harassment against Margaret Bent for four years but was acquitted of causing grievous bodily harm in September 1996, on the grounds that there was no evidence of intention to cause psychological injury.[9] At this time there were also important developments in both the criminal and civil law responding to the problem of stalking.[10] Concern that existing laws did not adequately protect victims of stalking finally led to the enactment of the Protection from Harassment Act 1997.[11]

This article sets out the case against the introduction of further legal measures to deal with on-line harassment. It argues that fears about on-line activity and content which prompt calls for heavy-handed legislation are often founded on misconceptions as to the nature and the scale of the problem. Such calls also invariably belie a certain naivety with regards to the unique law enforcement problems created by the Internet. In the case of on-line harassment, there are the difficulties of tracing the cyber-stalker who remains anonymous and problems of dealing with harassment that crosses national boundaries. The borderless nature of the Internet also means that actions by individual governments and international organisations can have a profound effect on the rights of the law-abiding Internet users, or "netizens", around the world. Legal regulation of the Internet, this article contends, should not be achieved at the significant expense of fundamental rights such as freedom of speech and privacy of on-line users around the globe.

What is on-line harassment?

Harassment on the Internet can take a variety of guises.[12] A direct form of Internet harassment may involve the sending of unwanted e-mails which are abusive, threatening or obscene from one person to another.[13] It may involve electronic sabotage, in the form of

---

6 Goode, M., "Stalking: The Crime of the Nineties," (1995) 19 *Cambridge Law Journal.* 21

7 See *The Independent,* 23 January 1995, *The Guardian*, 24 October 1996

8 See "Law on stalking may change to protect women", *The Daily Telegraph,* 6 March 1996

9 See "Victim is left alone with her fear as jury clears stalker", *The Daily Telegraph,* 18 September 1996

10 As regards criminal law, see *R. v. Ireland, R v Burstow* [1997] 3 W.L.R. 534. In *Ireland,* the defendant made repeated silent telephone calls to three women who suffered anxiety and depressive disorders as a result. He was convicted of assault occasioning actual bodily harm contrary to section 47 of the Offences Against the Person Act 1861 and sentenced to three years imprisonment. In *Burstow,* the defendant was convicted of maliciously inflicting grievous bodily harm, contrary to section 20 of the 1861 Act. Burstow waged a campaign of harassment against Tracy Slant during which he made abusive telephone calls to her, watched her house, stole clothing from her washing line and scattered condoms in her garden. See Allen, M., "Look Who's Stalking: Seeking a Solution to the Problem of Stalking," [1996] *Web JCLI* 4, Wells, C., "Stalking: The Criminal Law Response," [1997] *Crim.L.R.* 463.

11 See Home Office, *Stalking - The Solutions: A Consultation Paper,* (London: HMSO, 1996)

12 Nelson, D., "*Cyberstalking*," at <http://www.tccmweb.com/swcm/may97/stalk.htm>.

13 McGraw, D., "Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail" (1995) *Rutgers Computer and Technology Law Journal,* 492.

sending the victim hundreds or thousands of junk e-mail messages (the activity known as "spamming") or sending computer viruses. Indirect forms of harassment may involve a cyber-stalker impersonating his or her victim on-line and sending abusive e-mails or fraudulent spams in the victim's name.[14] Victims may be subscribed without their permission to a number of mailing lists with the result that they receive hundreds of unwanted e-mails everyday. One victim of cyber-stalking in the United States, Cynthia Armistead, received thousands of offensive telephone calls after her stalker posted a phoney advertisement on a Usenet discussion group offering her services as a prostitute and providing her home address and telephone number.[15] In another case, again in the United States, a woman who complained about a literacy agency on-line found that her home address and telephone number were posted on alt.sex. Usenet discussion groups.[16] Being the victim of on-line harassment undoubtedly causes considerable anxiety as well as annoyance. The real fear, however, is that offensive and threatening behaviour that originates on-line will escalate into "real life" stalking. If the name of the victim is known to the stalker, then it is relatively easy to find out further personal details such as the victim's address and telephone number. In the case of Cynthia Armistead, offensive e-mails were soon followed by abusive telephone calls. Fears in the United States have been fuelled by a number of cases of Internet dating which have been linked to assaults, stalking incidents, and even murders.[17] The arrival in Britain of a controversial new computer database, 192.com, which enables users to obtain an address and telephone number simply by typing in a name promises to make life even easier for stalkers.[18] The National Anti-Stalking and Harassment Campaign reports that between January 1994 and November 1995, 7,000 victims of stalking telephoned their helpline.[19] It is clear that stalking is a major real life problem but whether the Internet is to prove an attractive picking ground for stalkers remains to be seen.

Legal Regulation

There have been calls in the United States for specific cyber-stalking legislation.[20] It is argued that victims of cyber-stalking are inadequately protected as existing laws are too inflexible to cover on-line harassment.[21] Since its experiences in regard to the Internet tend to be more advanced than those in the UK, this section briefly examines the difficulties experienced in the United States in the legal regulation of e-mail harassment but argues that such problems are unlikely to be encountered in the UK.

---

14 See for example the case of *Zeran v. America Online, Inc*, 958 F.Supp. (1997); U.S. Court of Appeals, 4th Circuit, 129 F.2d 327 (1997); U.S. Supreme Court, Cert. Pet. 97-1488,

15 See <http://www.mindspring.com/~technomom/harassed/>.

16 Jayne Hitchcock wanted to let other writers know about a New York agency asking for $225 to review her book, so she posted a warning on the Internet. Before long, she was "mail bombed" with more than 200 electronic mail missives. Her name, telephone number and address appeared on racist and sex newsgroups, inviting suitors to call her or come to her home day or night. See "Author's real-life story is cyberspace nightmare", *The Washington Times*, 19 February 1998.

17 "Mainers log on, looking for love in cyberspace despite the dangers sometimes associated with anonymous, online romance, hundreds take the chance," *Portland Press Herald*, 30 March 1997.

18 See "Stalker fears over phones database disk", *The Scotsman*, 28 October 1997.

19 See Home Office, (1996), *op. cit.* See also Tjaden, P., & Thoennes, N., "Stalking in America: Findings From the National Violence Against Women Survey," Research in Brief, April 1998.

20 See "As Online Harassment Grows, Calls for New Laws Follow," *The New York Times* 2 April 1997.

21 See Barton, G., "Cyberstalking: Crime, Enforcement and Personal Responsibility in the On-line World," (1996) at <http://www.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm>.

United States

All US states now have legislation designed to deal with real-life stalking, but there have proved to be a number of difficulties in applying these State laws to e-mail harassment. California was the first state to pass a stalking law in 1990, and all the other states have since followed. The first US State to include on-line communications in its statutes against stalking was Michigan in 1993.[22] Under the Michigan Criminal Code, "harassment" means 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 besides Michigan have anti-stalking laws that include electronic harassment.[23] These states include: Arizona,[24] Alaska,[25] Connecticut,[26] New York,[27] Oklahoma,[28] and Wyoming.[29]

In the US, the constitutionality of state anti-stalking legislation remains undecided.[30] Anti-stalking legislation has been challenged on the grounds of being too vague and too broad.[31] Michigan was the first state to charge someone with on-line stalking. Andrew Archambeau refused to stop sending e-mail 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 the anti-stalking laws. In January 1996, Archambeau however pleaded no contest to the stalking charge.[32]

McGraw highlights further difficulties in using anti-stalking legislation to combat on-line harassment.[33] In a number of states, McGraw explains, the language of the statute requires physical activity, thus exempting e-mail harassment. Some state statutes also require a "credible threat" of serious physical injury or death.[34] In such states, e-mail harassment is unlikely to meet this standard. This was true in the Jake Baker case. 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.[35] 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 e-mail who used a pseudonym of "Arthur Gonda" in Canada. In over 40 e-mails 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

---

22 Michigan Criminal Code, Stalking: Section 28.643(8). Definitions. 1993. Sec. 411h.

23 See CyberAngels, "Cyberstalking and the Law," <http://www.cyberangels.org/stalking/stalk3.html>.

24 Arizona Criminal Code (1995): 13-2921

25 Alaska Criminal Law Sec. 11.41.270

26 Connecticut Penal Code Sec. 53a-183

27 New York Penal Code § 240.30

28 Oklahoma Code (1996):§21-1173

29 Wyoming Code, 6-2-506).

30 See Boychuk, K., "Are Stalking Laws Unconstitutionally Vague or Overbroad?" (1994) 88 *Nw.U.L.Rev.* 769, Hueter, J., "Will Washington Stalking Laws Survive Constitutional Scrutiny?" (1997) 72 *Wash. L.Rev. 213*

31 Jensen, B., "Cyberstalking: Crime, Enforcement and Personal Responsibility in the On-line World," <http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm>.

32 See "Man pleads no contest in stalking case" *The Detroit News*, 25 January 1996.

33 McGraw, D., (1995) *loc. cit.*

34 See generally for verbal threats, Nockleby, J. T., "Hate Speech in Context: The Case of Verbal Threats," (1994) 42 *Buff. L. Rev.* 653

35 Brook-Szachta, H., "Jake Baker Case: U.S. v. Jake Baker: The Role of Unique Features of Electronic Mail in a 'True Threat' Analysis," <http://www.libraries.wayne.edu/~jlitman/pbrooks.html>.

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. A US District Count 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.[36] It was the American Civil Liberties Union's ("ACLU") submission that this was a case of "pure speech."[37]

"No immediate harm results from the expression of a desire to commit a crime. The only warrant for proscribing such expression is the possibility that it will produce harm, should the speaker act on his desire, in the future.[38]

ACLU also quoted Brandeis J in *Whitney v. California* :

"Fear of serious injury cannot alone justify suppression of free speech.... To justify suppression of free speech there must be reasonable ground to fear that serious evil will result if free speech is practiced. There must be reasonable ground to believe that the danger apprehended is imminent."[39]

It was ruled that the sadistic fantasies contained in Baker's posting to Usenet were protected by the First Amendment.[40]

In the US, there are also difficulties in applying federal and state telephone harassment laws to e-mail harassment. According to Barton, few state telephone harassment laws presently apply to e-mail. Barton argues that e-mail harassment is best tackled by such telephone harassment laws, rather than by anti-stalking legislation, and therefore calls for their amendment by adding electronic communication provisions which adequately address the characteristics and scope of e-mail harassment.[41]

UK

In contrast to the situation described in the US, existing UK laws are sufficiently flexible to encompass on-line stalking and e-mail harassment. The Telecommunications Act 1984 section 43, for example, makes it an offence to send by means of a public

---

36 See See *U.S. v. Baker*, 890 F. Supp. 1375 (1995). See also Jake Baker Information Page at <http://www.mit.edu:8001/activities/safe/safe/cases/umich-baker-story/Baker/Jake_Baker.html>.

37 See ACLU amicus brief in *U.S. v. Jake Baker & Arthur Gonda* at <http://www.aclu.org/court/baker.html>. See also See *Watts v. United States*, 394 U.S. 705, 707 (1969).

38 *ibid.*

39 274 U.S. 357, at pp.376-77 (1927).

40 See 18 U.S.C. §875(c). See Wallace, J., & Mangan, M., (1996) *op cit.*, Haiman, F.S., *Speech Acts and the First Amendment* (Southern Illinois University Press, 1993); Haiman, F.S. *Speech and Law in a Free Society* (University of Chicago Press, 1981), Baker, C.E., *Human Liberty and Freedom of Speech* (Oxford University Press, 1989).

41 In October 1996, a Texas District judge issued the one of the first restraining orders to an on-line stalker which was itself delivered by e-mail and posted in newsgroups. Kevin Massey, was accused of the on-line harassment of Teresa Maynard, cofounder the ISP, Internet America. The temporary restraining order was granted following allegations that Massey had made 'vulgar' posting to newsgroups which referred to Maynard and sent 'lewd' and 'insulting' e-mail messages. See "In Harassment Case, Judge Issues Injunction via the Net," *The New York Times* 17 October 1997.

telecommunications system[42] 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 so designated by the Secretary of State and is not confined to British Telecom's telephone system.[43] The Act therefore potentially covers the sending of offensive e-mail messages in some instances.[44] 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.[45] So, whether the Act applies to e-mail harassment will depend upon the telecommunications network used, but the Act is not limited to voice communications.

The Protection from Harassment Act 1997 may also be invoked in cases of on-line harassment. This Act provides a combination of civil and criminal measures to deal with stalking.[46] It creates two criminal offences, the summary offence of criminal harassment[47] and an indictable offence involving fear of violence.[48] 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.[49] 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. 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.[50] Breach of such an order carries a potential sentence of five years imprisonment. Harassment includes alarm and distress.[51] Harassment, alarm and distress are not defined in the Act. 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 e-mails or the posting of offensive material would constitute an offence under section 2 of the Act as

---

42 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, electro-magnetic, 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....."

43 Telecommunication Act 1984 s.9(1). See also House of Commons, Home Affairs Committee, First Report on Computer Pornography, (1993-94 H.C. 126) Appendix: 2 Memorandum by the Crown Prosecution Service, at 27 para. 66.

44 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. See Manchester, C., "CJPOA 1994: Obscenity, Pornography and Videos" [1995] *Crim. L.R.* 123 at 127.

45 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. See Walker, C.P., "Criminal Libel," in Milmo, P., & Rogers, W.V.H., *Gatley on Libel and Slander*, (1998, London: Sweet & Maxwell) at 22.17.

46 See for example Gibbons, S., "Freedom from Fear of Stalking," (1998) 6(1)*European Journal on Criminal Policy and Research* 133-141.

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

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

49 "Conduct" includes speech (s. 7(4)) and "course of conduct" is defined as conduct on at least two occasion (s.7 (3)).

50 S.5

51 S.7(2)

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. According to Home Office Minister Alun Michael, there have been 504 prosecutions under section 2 of the 1997 Act, which have resulted in 247 convictions.[52] None of these prosecutions were Internet related and the majority dealt with neighbourhood nuisance issues rather than stalking activity.[53]

Although existing UK laws may potentially provide better protection from on-line harassment than that afforded, for example, by US anti-stalking legislation, the use of these laws will be necessarily limited to relatively straightforward cases of an identifiable offender sending obscene, offensive or threatening e-mails within the UK. This is because of the unique enforcement problems involved in the legal regulation of the Internet. The Protection from Harassment Act 1997 may not, for example, avail the victim of on-line harassment when the offender is outside the UK or if the offender chooses to remain anonymous.

Enforcement Problems

"Even with the most carefully crafted legislation, enforcing a law in a virtual community creates unique problems never before faced by law enforcement agencies."[54]

These problems pertain mainly to international aspects of the Internet. It is a medium that can be accessed by anyone throughout the globe with a computer and modem. This means, as explained below, that a potential offender may not be within the jurisdiction where an offence is committed. Anonymous use of the Internet, though beneficial in many instances, also promises to create challenges for law enforcement authorities.

The International Stalker

The Internet is a global medium regardless of frontiers, and this creates new possibilities for the so-called cyber-stalker. Cheap and easy access to the Internet means that distance is no obstacle to the cyber-stalker. A user in the UK may be stalked by someone on the other side of the world by the click of a mouse. The Internet is not a "lawless place",[55] but there are difficulties in applying laws that are made for specific nation states and this would be also true of applying national harassment and stalking laws to the Internet.

For example, under section 43 of the Telecommunications Act 1984, an offence is not committed where a telecommunication system located outside the jurisdiction is used to send offensive materials into UK.[56] Even if the 1984 Act covered telecommunication systems located outside the jurisdiction, there would have been difficulties for prosecuting a foreign cyber-stalker. First, the act of the cyber-stalker might not constitute an offence within the

---

52 In addition, 171 cautions have been recorded provisionally for the offence. See House of Commons Written Answers, Protection from Harassment Act, col. 298 18 June, 1998.

53 See for example the cases of *Huntingdon Life Sciences Ltd v Curtin*, The Times, December 11, 1997; *McGlennan v McKinnon*, 1998 S.L.T. 494.

54 Jensen, B., "Cyberstalking: Crime, Enforcement and Personal Responsibility in the On-line World," <http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm>.

55 See Reidenberg, J.R, "Governing Networks and Cyberspace Rule-Making" (1996) 45 *Emory Law Journal* 911.

56 House of Commons, Home Affairs Committee: First Report on Computer Pornography, (1993-94 H.C. 126) Appendix: 2 Memorandum by the Crown Prosecution Service at 27 para. 67 and 68.

country of origin; and even if it did so there may be problems of extradition. There would also be problems in cross-border policing.

The UK Government recently dealt with the problem of cross-border policing in the context of transnational child abuse with the Sexual Offences (Conspiracy & Incitement) Act 1996. The Act deals with British sex offenders abroad, and section 2 of the 1996 Act makes it an offence to incite another person to commit certain sexual acts against children abroad. The scope of incitement for the purposes of section 2 extends to the use of Internet, and any incitement will be deemed to take place in the UK if the message is received in the UK.[57] The same principles could apply if the 1997 Protection from Harassment Act were to be extended to British offenders who live abroad. This would only be a limited and partial solution, however, to the problem of international stalkers. In addition, recent criticism from police officers of the 1996 Act casts doubts upon the effectiveness of this kind of extra-territorial legislation.[58]

The Anonymous Stalker

Internet technology creates possibilities for anonymous communications and hence for anonymous cyberstalking. The identity of a cyber-stalker may, therefore, not be revealed or found. The fluidity of identity on the Internet has been described as one of its chief attractions.[59] The Internet facilitates experimentation with different identities. Users may adopt an on-line persona which bears little, if any, resemblance to his or her real identity. Pseudonymity is achieved by simply forging or "spoofing" an e-mail header so as to create an on-line digital persona. For example, Alice can create a new persona for her on-line participation in Usenet discussion groups with an e-mail address such as Billy-Kid@compuserve.com rather than using her real e-mail address, alice@compuserve.com. Impersonation of other users may also be possible by faking the header of an e-mail message to make it appear as if it originates from the victim's account. Anonymity on the Internet can be achieved by using an anonymous re-mailer. Re-mailers are computer services which cloak the identity of users who send messages through them by stripping all identifying information from an e-mail and assigning a random replacement header. The most sophisticated re-mailer technology is called MixMaster[60] which uses public key cryptography, granting unprecedented anonymity to users who wish to communicate in complete privacy. A user who chains together several re-mailers could send communications safe in the knowledge that the trail created would be so complex that it would be impossible to follow.[61] According to Ball, true anonymous re-mailers maintain no database of addresses:

---

57 See also the Sex Offenders Act 1997 s.7 which deals with sexual offences committed outside the UK. See Alldridge, P., "Sexual Offences (Conspiracy and Incitement) Act 1996, Sex Offenders Act 1997," [1997] *Crim. L.R.* 655.

58 No prosecution has been achieved under this law within the UK since its enactment. See Burrell, I., "Child-sex tourists escape UK law," *The Independent*, July 13, 1998.

59 See Wacks, R., "Privacy in Cyberspace: Personal Information, Free Speech, and the Internet" in Birks, P. (ed.), *Privacy and Loyalty*, (Oxford: Clarendon Press, 1997) at p.93.

60 Lance Cottrel, Mixmaster FAQ, <http://www.obscura.com/~loki/re-mailer/mixmaster-faq.html>.

61 Some re-mailers keep a record of the original e-mail address and thus senders are traceable. See Detweiler, L., "Identity, Privacy and Anonymity on the Internet" (1993) at <http://www.rewi.hu-berlin.de/Datenschutz/Netze/privint.html>; Greenberg, S., "Threats, Harassment and Hate On-line: Recent Developments" (1997) 6 *Boston Public Interest Journal* 673; Froomkin, M., "Anonymity and its Enmities" (1995) *Journal of Online Law* art. 4

"When messages are resent from a truly anonymous re-mailer, the header information is set either to a deliberately misleading address, or to randomly generated characters. There is no record of the connection between the sending address and the destination address. For greater security, many users program messages to pass through five to twenty re-mailers before the message arrives at its final destination. This technique, known as chaining, assures greater security than sending through a single re-mailer. Even if some re-mailers keep secret records of their transactions, a single honest re-mailing system will protect the user. One disadvantage is that unless the sender has identified herself in the body of the message, the recipient has no way to reply to an anonymously sent message."[62]

The ease with which users can send anonymous messages would render legal regulation of on-line harassment a difficult, if not impossible, task. Tracing a cyber-stalker may prove an insurmountable obstacle to any legal action when the electronic footprints which users leave behind are effectively eliminated by re-mailer technology.

Given these enforcement problems, some commentators have called for the prohibition of anonymous communications while others have called for restrictions to be placed on anonymity.[63] Opponents of anonymity argue that it facilitates illegal or reprehensible conduct and allows perpetrators to evade the consequences of their actions.[64] Arguments based on the social psychology of anonymity have been used.[65] Anonymity, it is alleged, lowers social inhibitions and encourages anti-social behaviour and aggression.[66] People will say and do things on the Internet, it is maintained, that they would never seriously entertain doing in real life.[67] Those who call for the prohibition of anonymous remailers or other restrictions on on-line anonymity may, however, fail to recognise the cost of such action to the on-line community in terms of fundamental freedoms. Placing restrictions upon anonymity on-line would have serious negative repercussions for freedom of expression and privacy on the Internet, as shall now be described.[68]

Freedom of Speech

"Freedom of speech and privacy are frequently conceived as rights or interests of the individual, and as rights or interests of the community as a whole."[69]

Free speech can be facilitated by anonymity on-line. It allows human rights activists, political dissidents, and whistle blowers throughout the world to engage in confidential communications free from intrusion.[70] It is also essential for political discussion and some special subject interest groups who deal with sensitive issues. Users seeking access to

---

62 See Affidavit of Witness Patrick Ball in ACLU v. Miller, January, 1997, <http://www.aclu.org/issues/cyber/censor/gapbaffidavit.html>.

63 Kabay, M., "Anonymity and Pseudonymity in Cyberspace: Deindivduation, Incivility and Lawlessness Versus Freedom and Privacy," Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research, March 1998.

64 Detweiler, L., (1993), *op. cit.*

65 Bell, V., and de la Rue, D., "*Gender Harassment on the Internet,"* <http://www.gsu.edu/~lawppw/lawand.papers/harass.html>

66 Kabay, M., (1998), *op. cit.*

67 Greenberg, S., (1997), *op. cit.*

68 Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, (Cmnd. 1102, London: HMSO, 1990) para. 3.12, p 7.

69 Wacks, R., (1997) *op cit*. at p.103

70 See Banisar, D., "Bug Off! A Primer on Electronic Surveillance for Human Rights Organizations," (1995) *International Privacy Bulletin*, October.

information on AIDS, for example, or seeking guidance from the Samaritans clearly benefit from remaining anonymous. One of the best-known anonymous re-mailers on the Internet, anon.penet.fi, was offered for more than three years by Johann Helsingius.[71] Among its users were Amnesty International, the Samaritans,[72] and the West Mercia Police who used it as the basis of their "Crimestoppers" scheme. Anonymity also allows users to by-pass class, race and gender stereotypes. As one commentator states, "I may have a good idea you will not consider if you know my name. Or I may individually fear retaliation if my identity is revealed. Anonymity is therefore good, because it encourages greater diversity of speech."[73]

In the United States, attempts to control anonymity on the Internet have been ruled unconstitutional.[74] In *ACLU v. Miller*,[75] the Federal District Court agreed with the ACLU, that a recent Georgia statute is unconstitutionally vague and over-broad because it bars on-line users from using pseudonyms or communicating anonymously over the Internet. Judge Shoob noted that Georgia's law, "sweeps innocent, protected speech within its scope." "The Court recognised that anonymity is the passport for entry into cyberspace for many persons," according to Gerald Weber, Legal Director of the ACLU of Georgia. "Without anonymity, victims of domestic violence, persons in Alcoholics Anonymous, people with AIDS and so many others would fear using the Internet to seek information and support."[76]

There is no express constitutional guarantee for freedom of speech in Britain because of the absence of a comprehensive Bill of Rights. Although the European Convention on Human Rights, which protects the freedom of expression in Article 10, does bind the UK in international law as an external bill of rights, it has not been directly implemented in the national laws. This situation is however set to change following the introduction of the Human Rights Bill 1997-98[77] which will incorporate the ECHR into the UK legal systems. Article 10 of the ECHR states that:

> 1.Everyone has the right to freedom of expression. This right should include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers...
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of health or morals, for the

---

71 See Dyson, E., *Release 2.0: A Design for Living in the Digital Age*, (London: Viking, 1997) at p.236; Wallace, J., and Mangan, M., (1996) *op. cit*. See also The Church of Scientology vs. anon.penet.fi pages at <http://www.xs4all.nl/~kspaink/rnewman/anon/penet.html>.

72 The Samaritans now use another anonymous remailer service (samaritans@anon.twwells.com). See <http://www.samaritans.org.uk/sams.html/contact2.html>.

73 See Wallace, J., "Mrs. McIntyre in Cyberspace: Some thoughts on anonymity," *The Ethical Spectacle*, May 1997 at < http://www.spectacle.org/597/mcintyre.html>.

74 *NAACP v. Alabama ex rel. Patterson* 357 U.S. 449 (1958) and more recently *McIntyre v. Ohio Elections Commission* , 514 U.S. 334 (1995); 115 S.Ct. 1511, (1995).. See Branscomb, A., "Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces," [1995] 104 *Yale L.J.* 1639, at p.1642.

75 See *American Civil Liberties Union of Georgia v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997) (preliminary injunction), permanent injunction entered, 1997 U.S. Dist. LEXIS 14972 (Aug. 7, 1997).

76 ACLU Press Release, "ACLU Wins First-Ever Challenge to a State Internet Censorship Law in Georgia," June 20, 1997, <http://www.aclu.org/news/n062097b.html>.

77 1997-98 H.C. No.219. See House of Commons Library Research Paper, *The Human Rights Bill [HL], Bill 119 of 1997/98: Some constitutional and legislative aspects* (No: 98/27, 1998).

protection of the reputation or rights of others, for preventing the disclosure if information received in confidence, or for maintaining the authority and impartiality of the judiciary."

The importance of anonymity as a facilitator of free speech has been affirmed by the European Court of Human Rights in *Goodwin v UK*.[78] The Court recognised that the press has a vital watchdog role in a healthy democratic society and that this function could be undermined if journalists are not reasonably allowed to keep confidential the sources of their information. In this case, the Court concluded that the application of the law of contempt to a recalcitrant journalist was not necessary where the subject of the damaging story had already obtained an injunction against publication. It is not clear that the same level of protection of anonymity would be afforded by the European Court to the idle gossip of non-press speakers such as is common on the Internet,[79] but anonymous "political speech" would deserve higher protection.[80]Moreover, there may also be instances where Internet postings may lead to persecution if the identity of the individual is known.[81] The Supreme Court in *NAACP v. Alabama ex rel. Patterson*[82] stated that "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association"[83]. However, the lead it has given in regard to "public" speech is important and is not yet reflected by the English courts, as illustrated by the later case of *Camelot v Centaur Communications* in which the Court of Appeal demanded disclosure in circumstances not dissimilar to *Goodwin*.[84] Hopefully, the Human Rights Act, when passed, will prompt some re-evaluation by the judges of the importance to free speech of anonymity.

Anonymity and Privacy

Anonymity, apart from facilitating free speech, can also facilitate the protection of privacy on the Internet. Many users are unaware that every time they surf the Internet, information about the web sites they have visited is logged and stored. The Center for Democracy and Technology ("CDT") has an on-line demonstration entitled "Who's Watching You and What are You Telling Them?"[85] which allows users to view their personal on-line biography. CDT's web site notes that:

"Many people surf the web under the illusion that their actions are private and anonymous. Unfortunately, there is more information collected about you than you might think. Every

---

78 Appl.no.17488/90, Ser. A vol.??, (??)(1996) 22 EHRR 123. See further *X v. Morgan-Grampian* [1990] 2 W.L.R. 1000; Palmer, S., "Protecting journalists' sources" [1992] P.L. 61; Cram, I., "When the interests of justice outweigh freedom of expression" [1992] M.L.R. 400.

79 See also the support for disclosure on grounds of private and family life in *Gaskin v UK*, Appl.no.??, Ser.A vol.160, (??)(1989) 12 EHRR 36.

80 See *McIntyre v. Ohio Elections Commission* 115 S.Ct. 1511, (1995). The Supreme Court stated that: "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment" and "the anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment."

81 See the written evidence submitted by the Christian Action Research and Education (CARE) to the House of Lords, Select Committee on Science and Technology, Fifth Report on "Information Society: Agenda for Action in the UK", (1995-96 H.L. 77, London: HMSO) at p.187.

82 357 U.S. 449 (1958).

83 *Ibid* at 462.

84 [1998] 2 W.L.R. 379.

85 See <http://www.13x.com/cgi-bin/cdt/snoop.pl>.

time you visit a site, you leave a calling card that reveals where you're coming from, what kind of computer you have, and many other details. Most sites keep logs of all visitors."

There are Internet-based marketing organisations who build comprehensive profiles of users and then sell on the information. With the right equipment, a user's e-mail address together with files viewed and other detailed information can be obtained by web systems even though no information is supplied directly to a web site. The Electronic Privacy Information Center ("EPIC") reviewed 100 of the most frequently visited web sites on the Internet in the summer of 1997. EPIC found that few web sites have explicit privacy policies (only 17 of their sample), and none of the top 100 web sites met basic standards for privacy protection. [86] On-line users can currently use web based services such as the Anonymizer to surf the web anonymously.[87] The Anonymizer shields a user's personal information from the other web sites that he or she visits. On visiting the Anonymizer web site a user is assigned an anonymous identity and is thus able to surf the web without revealing his or her true identity.

Anonymity enables users to prevent surveillance and monitoring of their activities on the Internet not only from commercial companies but also from government intrusion. In Britain, the DTI Consultation Paper, "Licensing of Trusted Third Parties for the Provision of Encryption Services",[88] which may have been expected to address privacy and anonymity on the Internet, devoted no space to the issue. [89] The Internet Watch Foundation (formerly known as Safety-Net),[90] endorsed by the UK Government, sees anonymity on the Internet as a danger, proposing that:[91]

"... [A]nonymous servers that operate in the UK [should] record details of identity and make this available to the Police, when needed, under Section 28 (3) of the Data Protection Act (which deals with the disclosure of information for the purpose of prevention of crime)."

A key aspect of the Safety-Net approach is making users take responsibility for material they post on the Internet; stressing the importance of being able to trace the originators of child pornography and other illegal material.[92] For this purpose, the Safety-Net document proposed that the Internet Service Providers should not provide their users with

---

86 See Electronic Privacy Information Center report, "Surfer Beware: Personal Privacy and the Internet," Washington, DC, June 1997 at <http://www.epic.org/reports/surfer-beware.html>.

87 See <http://www.anonymizer.com/>.

88 Department of Trade and Industry, Consultation Paper, "Licensing of Trusted Third Parties for the Provision of Encryption Services," March 1997, <http://www.dti.gov.uk/pubs/>. This followed up the earlier "Paper On Regulatory Intent Concerning Use Of Encryption On Public Networks," June 10, 1996, <http://dtiinfo1.dti.gov.uk/cii/encrypt/>. See Akdeniz, Y., et. al., "Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals," (1997) 2 *The Journal of Information, Law and Technology*; Akdeniz, Y., "UK Government Encryption Policy," [1997] *Web JCLI* 1; Akdeniz, Y., and Walker, C., "UK Government policy on encryption: trust is the key?" (1998) 3 Journal of Civil Liberties 110.

89 See Akdeniz, Y., "No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights," (1998) *Web JCLI* 1.

90 The Internet Watch Foundation ("IWF"), was announced on September 23, 1996. IWF has an e-mail, telephone and fax hotline so that on-line users are able to report materials related to child pornography and other obscene materials. See the Safety-Net proposal, "Rating, Reporting, Responsibility, For Child Pornography & Illegal Material on the Internet" adopted and recommended by the Executive Committee of -Internet Services Providers Association, ("ISPA"), London Internet Exchange, ("LINX") and the IWF at <http://dtiinfo1.dti.gov.uk/safety-net/r3.htm>.

91 Safety-Net proposal 1996, para 30.

92 See DTI, "Rating, Reporting, Responsibility, For Child Pornography & Illegal Material on the Internet," September 1996, at http://dtiinfo1.dti.gov.uk/safety-net/r3.htm para 29-30.

anonymous accounts. ISPs must ensure that they know who all their customers are. This approach is in contrast with European Union initiatives. The benefits of anonymity on-line were recognised at the recent "Global Information Networks, Ministerial Conference," in Bonn, in July 1997. At the Bonn Ministerial Conference, the Ministers declared that:

"Ministers recognise the principle that where the user can choose to remain anonymous off-line, that choice should also be available on-line. Ministers urge industry to implement technical means for ensuring privacy and protecting personal data on the Global Information Networks, such as anonymous browsing, e-mail and payment facilities."[93]

An express right to privacy in UK law will be granted for the first time once the Human Rights Bill is passed and comes into force. Article 8 of the European Convention on Human Rights demands "respect for ...private and family life...home and ...correspondence", and this undoubtedly requires a greater recognition of the value of privacy than has hitherto been forthcoming from English judges or Parliament.[94] In particular, it will be noted that Article 8 expressly protects "correspondence", and this has been applied by the European Court of Human Rights to curtail unregulated police access to telephone conversations as well as other forms of electronic surveillance.[95] "Correspondence" on the Internet is deserving of at least an equal degree of protection, though whether the importance of anonymity on the Internet both to free speech and to privacy will ultimately be recognised and, in turn, influence the shape of future regulatory initiatives remains to be seen.

Non-legal Solutions

This article has highlighted the limitations of legal regulation of on-line harassment in cases which involve anonymous and international cyber-stalkers. These limitations in legal regulation are, to some extent, compensated for by the availability of non-legal solutions to on-line harassment. A number of more suitable ways in which users can both empower and protect themselves from on-line harassment are discussed below.

Self-Protection

The education of users is the first step towards self-protection from Internet harassment. There are many web sites and books which provide information for self-protection from cyber-stalkers for on-line users.[96] In general, women are advised, where

---

93 See the "Bonn Declaration" at http://www2.echo.lu/bonn/final.html.

94 See House of Commons Library Research Paper, The Human Rights Bill [HL], Bill 119 of 1997/98: Privacy and the Press, No: 98/25 (London: 1998); Lord Bingham, "Should there be a law to protect rights of personal privacy?" [1996] *EHRLR* 250.

95 See *Malone v. U.K.* (Application no. 8691/79, Judgment of Court Ser. A. vol. 82, (1984); *Halford v UK*, Appl. no. 20605/92, (1997) *The Times* 3 July; Carter, PB, "Evidence obtained by the use of a covert listening device" (1997) 113 LQR 467.

96 For example see Women Halting Online Abuse <http://whoa.femail.com/>, CyberAngels at <http://www.cyberangels.org/stalking/index.html>. Cnet News.Com special, "Cyberstalkers: What to do if you are harassed or stalked," July 1997, <http://www.cnet.com/Content/Features/Dlife/Dark/ss01c.html>; Online Harassment Resources at <http://www.io.com/~barton/harassment.html>; Women, Take Back the Net!: An Online Guide to Reporting E-Harrassment at <http://www.virtual.net/Projects/Take-Back-the-Net/>. Information on real life stalking can be found in Stalking Victims' Sanctuary at <http://www.ccon.com/stalkvictim/> and at the US National Victim Center's Helpful Guide for Stalking Victims, <http://www.nvc.org/ddir/info44.htm>. See also Gelman, R.B., et. al., *Protecting Yourself Online : The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*, (New York: HarperCollins, 1998), Sherman, A., *Cybergrrl! A Woman's Guide to the World Wide Web*, (USA: Ballantine, 1998)

possible, to adopt either a male or gender neutral user name. Passwords, it is advised, should ideally be a meaningless combination of letters and numbers and changed frequently. Passwords should never be given out and should never be sent out via simple e-mail messages as these are the equivalent of sending traditional "postcards" via snail mail. It is recommended that personal information divulged on-line be kept to a minimum. Users should regularly check their on-line profile (finger files) or biography to see what information is available to a potential stalker. To guard against on-line impersonation, users are also advised to use strong encryption programmes such as the Pretty Good Privacy ("PGP")[97] to ensure complete private communications. Strong encryption can provide confidentiality, integrity and authenticity of the information transferred via on-line communications. Strong encryption and use of such software as PGP is the only solution for having truly private communications over the Internet. Using strong encryption would put your electronic "postcard" in a secure envelope and seal it.

A number of self-appointed Internet patrollers have been involved in tracking the senders of offensive e-mail messages. Among the organisations offering assistance in tracking down stalkers are CyberAngels,[98] a branch of the New York based Guardian Angels, Cybertrackers,[99] and Women Halting On-line Abuse ("WHOA").[100] Once the perpetrator is identified, a message through e-mail calling for an end to the harassing behaviour is sent out to the perpetrator. These self-policing activities may help in some instances but their overall effectiveness remains to be determined.

Role of the Internet Service Providers

Access to the Internet is possible through Internet Service Providers ("ISPs"). An individual who receives unwanted e-mail or finds that offensive information about them has been posted on the Internet should contact the offender's ISP who may eliminate his or her account. As mentioned above, the ISPs in Britain do not provide their customers with anonymous accounts, and every single Internet user through the British ISPs or ISPs that provide services within Britain should have identifiable customers. These precautions may assist the police in cases in which they are trying to find the identity of a cyber-stalker who may be accessing the Internet and conducting his or her cyber-stalking activities through a British ISP. These precautions may not be of help in cases in which the offender is untraceable, e.g. when he or she uses anonymous re-mailers or where the cyberstalker is not a customer of the ISP in question or has posted messages from outside the jurisdiction.

Some of these issues were discussed in a recent US defamation case involving America Online, *Kenneth M. Zeran v. America Online, Inc*.[101] On April 25, 1995, six days after 168 people were killed in the Oklahoma City bombing, an unidentified America Online user posted an advertisement on one of AOL's bulletin boards for "Naughty Oklahoma" T-shirts and bumper stickers, all of which contained offensive slogans. The advertisements asked interested parties to contact "Ken" and gave Kenneth Zeran's telephone number in Seattle, Washington. Death threats to Zeran started immediately after the initial postings. Zeran, who was not at all responsible for the postings and did not even have an AOL account,

---

97 See <http://www.pgp.com>.
98 See <http://www.cyberangels.org/>.
99 See <http://www.alyssa.com/cyber.htm>.
100 See <http://whoa.femail.com/>.
101 See U.S. District Court, E.D. Virginia, 958 F.Supp. (1997); U.S Court of Appeals, 4th Circuit, CA-96-1564-A, 129 F.2d 327 (1997); U.S. Supreme Court, Cert. Pet. 97-1488, denied.

decided to sue AOL, arguing that the company had unreasonably delayed in removing the defamatory messages and had failed to screen for similar postings thereafter.

A District Court found that section 230 of the Communications Decency Act 1996,[102] which "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user," barred Zeran's suit. This was also confirmed by the US Court of Appeals.[103] The court further stated that tort-based lawsuits would have an "obvious chilling effect" on the Internet and on Internet Service Providers. As a result, the controversial CDA 1996[104] now offers more protection to ISPs than any other media but falls short of granting "common carrier" status enjoyed by telephone companies. This may even go too far: according to David Sobel of EPIC, "there should be some degree of accountability on the part of online services as there is for other forms of media."[105]

Software

New and innovative software programmes which enable users to control the information they receive are being developed.[106] There are, for example, technical means by which users may block unwanted communications. Tools available include 'kill' files and bozo files which delete incoming e-mail messages from individuals specified by the user, and such tools are included with most of the available e-mail software packages. There is also specially designed software to filter or block unwanted e-mail messages. These tools such as CyberSitter[107] and Netnanny[108] are designed mainly to block the access of children to sexually explicit web sites and newsgroups, but they can be used to filter out and block e-mail communications. Some of this software can also filter words through the incoming and outgoing e-mail messages. The mandatory use of such software, especially at access level, by libraries and ISPs is criticised[109] within the US because the decisions taken to block certain web sites are arbitrary and within the discretion of the private companies that develop these systems.[110] They are also defective since most of them block such web sites as the Middlesex County Club or the Mars Explorer while trying to block the word "sex" or they block web sites by looking at the keywords in the meta-tags offered by the individual html files.[111] But these tools may be of some use to victims of cyber-stalkers to filter out unwanted messages. In the future, advanced filtering systems which recognise insulting e-mail may also be available.

---

102 47 USC s.223.

103 *Kenneth M. Zeran v. America Online, Inc*, U.S Court of Appeals, 4th Circuit, CA-96-1564-A, 129 F.2d 327 (1997).

104 See also *ACLU v Reno* (117 S. Ct. 2329 (1997).

105 Kornblum, J., "Supreme Court backs AOL," *Cnet News.Com*, June 22, 1998.

106 Spertus, E., "Social and Technical Means for Fighting Online Harassment," (Presented at Virtue and Virtuality: Gender, Law, and Cyberspace - - MIT Artificial Intelligence Laboratory, May 5, 1996) <http://www.ai.mit.edu/people/ellens/Gender/glc/>.

107 See <http://www.solidaok.com/>.

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

109 See the ACLU complaint in Mainstream Loudoun, et al., v. Board of Trustees of the Loudoun County Library and others, Case No. 97-2049-A, at <http://www.aclu.org/court/loudoncocomplaint.html>. See also Judge Brinkema's Opinion in the Loudoun Blocking Software Case at <http://www.techlawjournal.com/courts/loudon/80407mem.htm>.

110 See American Civil Liberties Union, "Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet," August 1997, at <http://www.aclu.org/issues/cyber/burning.html>; Cyber-Rights & Cyber-Liberties (UK), "Who Watches the Watchmen: Internet Content Rating Systems, and privatised censorship," November 1997, at <http://www.leeds.ac.uk/law/pgs/yaman/watchmen.htm>.

111 See generally Electronic Privacy Information Center, "Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet," Washington, December 1997, at <http://www2.epic.org/reports/filter-report.html>.

Conclusion

This article has sought to highlight the issues surrounding legal regulation of the Internet in relation to on-line harassment. It is suggested that ".. the Internet is in its infancy and lawmakers should exercise caution in attempting to regulate this new technology whose potential none of us can fully comprehend."[112] The most famous attempt at legal regulation of the Internet was the US Communications Decency Act of 1996 which attempted to limit the availability of "indecent speech" on the Internet.[113] Judge Dalzell in *ACLU v Reno* stated that:

"As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from government intrusion. Just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects."[114]

The indecency provisions of the CDA were struck down by the US Supreme Court in the summer of 1997, and this was also seen as an end to regulatory initiatives by single nation-states. We are now witnessing a move towards self-regulatory solutions especially for Internet content regulation.[115] There are also many initiatives at a supra-national European level[116] and elsewhere which again suggest that legal regulation of the Internet at a national level is futile and also undesirable. The House of Lords Select Committee on Science and Technology in its paper, *Information Society*[117] stated that where "government intervention is needed, it is also clear that as much as possible should be agreed internationally" and that "there are issues here which must be resolved internationally, to ensure that the defence and law enforcement agencies of national governments are not emasculated by the growth of the Information Society."[118] According to a recent House of Commons Select Committee on Culture Report, "The Multi-Media Revolution," international initiatives will have an important impact on national Internet regulation, but at the same time "the question is whether such attempts at regulation can be anything more than optimistically indicative rather than genuinely effective."[119] This does not mean that laws cannot be applied to the Internet and that individuals cannot be protected from so called cyber-crimes. It means that a new multi-layered governance approach will be necessary. The new governance will involve both public and private bodies at both national and supranational level. New self-regulatory solutions will also be sought. In this new way of thinking "self" may both mean as an individual solution

---

112 Greenberg, S., (1997) *op cit.*

113 See *ACLU, et al. v. Janet Reno*, 929 F Supp 824 (1996), and *ACLU v Reno*, 117 S. Ct. 2329 (1997).

114 Per Judge Dozzell, *ACLU, et al. v. Janet Reno*, 929 F Supp 824 (1996) at p.883.

115 See House of Lords, Select Committee on Science and Technology, Information Society: Agenda for Action in the UK (1995-96 H.L. 77), para.5.50 and also Minister for Science Energy and Industry, John Battle: "HMG strategy for the Internet", 18 March 1998 at <http://www.dti.gov/Minspeech/btlspch3.htm>.

116 See Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Action Plan on promoting safe use of the Internet, November 1997. See also Akdeniz, Y., "The European Union and illegal and harmful content on the Internet," (1998) 3 *Journal of Civil Liberties* 31.

117 House of Lords, Select Committee on Science and Technology, Information Society: Agenda for Action in the UK (1995-96 H.L. 77). See also the Government's Response, (Cm.3450, London: HMSO, 1996).

118 *Ibid* paragraph 5.45.

119 House of Commons Select Committee on Culture, "The Multi-Media Revolution - Volume I," (1997-98 HC 520-I) para.108. See also the Government Response to "The Multimedia Revolution," (HC520-1), July 1998. See also Cyber-Rights & Cyber-Liberties (UK) Report: "Who Watches the Watchmen: Part II - Accountability & Effective Self-Regulation in the Information Age," September 1998 at <http://www.cyber-rights.org/watchmen-ii.htm>.

(e.g. individual protection from cyber-crimes such as cyber-stalking), or as a more collective solution (e.g. codes of conduct for ISPs or the introduction of hotlines and user organisations).

The moral panics that the Internet has witnessed regarding on-line activity, largely the result of misreporting by the media, cloud the fact that it is only a small minority of users who engage in illegal activity such as cyberstalking and only a small portion of the Internet contains illegal content:[120]

"The peccadilloes of the few, however, should not be permitted to override the beneficial uses of these computer-mediated communications systems. They are only a small portion of what is actually happening."

The beneficial uses of the Internet far outweigh its abuses and the few problems created by the use of the Internet by a small proportion of the Internet community should be dealt with through self-regulatory solutions at both private and public levels together with the improvement of good practices for Internet usage.

[120] Branscomb, A., (1995) *op. cit.* at p.1677.