BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

Cyberstalking: Tackling Harassment on the Internet

Louise Ellison, Lecturer in Law, University of Reading,

Introduction

The problem of on-line harassment has received considerable and, in many cases sensationalised, press coverage in recent years. These reports suggest that women who use the Internet instantly risk becoming the target of a cyberstalker and finding themselves the victim of a campaign of electronic abuse. Disturbing pronouncements as to the nature and impact of harassment on-line have become commonplace. Some commentators have gone as far as to state that on-line harassment is already killing free speech on the Internet, in particular the free speech of women. Women are engaging in self censorship, it is claimed, in order to avoid harassment and are, as a result, being further marginalised in cyberspace. In February 1999, the Vice President of the United States, Al Gore, called for a fight against cyberstalking stating that the Internet had inadvertently become a sinister new avenue for carrying out violence against women. This paper examines the phenomenon of cyberstalking and highlights the danger that largely exaggerated fears regarding on-line harassment may ultimately have serious and negative repercussions for privacy and freedom of speech on the Internet.

What is on-line harassment?

Harassment on the Internet can take a variety of guises. 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. It may involve electronic sabotage, in the form of 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 cyberstalker impersonating his or her victim on-line and sending abusive e-mails or fraudulent spams in the victim's name. 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.

Unsurprisingly, it is the more dramatic cases of on-line harassment which have grabbed the media headlines. One such case is that of Cynthia Armistead of Atlanta, who received threatening and obscene e-mail messages from her cyberstalker as well as harassing telephone calls. Her harasser posted phoney advertisements to a USENET discussion group offering Armistead's services as a prostitute and providing her home address and telephone number which led to more obscene e-mail messages and telephone calls. Jayne Hitchcock posted a warning on the Internet about a New York literary agency asking for $225 to review her book. She was then "mail bombed" with more than 200 e-mail missives. Her name, telephone number and address appeared on racist and sex newsgroups inviting men to call her or come to her home day or night. In January 1999, Gary Dellapenta, a 50 year old security guard from Los Angeles, was arrested and charged under California's 'cyberstalking' laws. Dellapenta allegedly posted messages in AOL chat rooms that appeared to come

from his victim, a 28 year old woman. The messages claimed that the woman had an unfulfilled sexual fantasy of being raped and included her name, address and telephone number. Six men visited the woman's apartment in response to the messages and the woman also received dozens of telephone calls from men. Dellapenta has pleaded not guilty of the charge and is currently on bail.

It is not only women who are the targets of offensive and threatening electronic messages. There have been a number of well publicised cases involving death threats sent via the Internet. In 1998, the first US federal case involving hate e-mail resulted in the conviction of Richard Machado. Machado had sent derogatory e-mail messages to Asian students at the University of California, in which he threatened to kill them. He was convicted on one civil rights charge and sentenced to time served. In another case, Kingman Quon of California was accused of e- mailing death threats to Hispanic professors, students and officials across the country. In January 1999, he pleaded guilty to seven misdemeanour counts of interfering with federally protected rights, specifically threatening to use force against his victims with the intent to intimidate or interfere with them because of their national origin or ethnic background.

While undoubtedly distressing for the victims involved in these cases, there is no evidence to suggest that persistent campaigns of on-line harassment which involve death threats or escalate into 'real life' stalking are commonplace. Media generated concerns about harassment on-line cloud the fact that it is only a small minority of users who engage in illegal activity such as cyberstalking and that harassment on-line more commonly takes the form of unwanted, sexually explicit invitations or occasional offensive, annoying and abusive messages. As Brail notes, " most forms of harassment are mere annoyances, desperate men looking for sex in the electronic ether and hitting on anything vaguely female."

Do characteristics of CMC encourage harassment?

Concern surrounding on-line harassment has also been fuelled by the claims of some commentators that characteristics peculiar to the Internet and to computer-mediated communications ('CMCs') make the medium particularly attractive to the stalker and harasser. These claims are examined below.

Although the nature of CMC and its societal and behavioural effects have been the subject of much research it is, as Walther notes, "still debated, tested, and not very well understood when one examines the literature on the subject." It has, however, been suggested that CMC differs in many ways from traditional communication technologies. One striking and highly valued feature of CMC is its general potential for pseudonymity. Pseudonymity on the Internet can be achieved by simply forging or "spoofing" an e-mail header so as to create an on-line digital persona. In CMC the gender, race, age and physical appearance of others is not immediately evident. It is for the user to decide what information she or he will or will not reveal in Internet communications. This gives users greater control over self-representation. For example, researchers of human behaviour on CMC systems observe that identity manipulation is commonplace in CMC. Users often create alternative personae for their on-line interactions with others that bare little resemblance to their real life identities. The comparative anonymity of CMCs, it is claimed, means that users tend to be less inhibited in their on-line interactions with others. It is commonly asserted that that people will write, or more accurately type, things in electronic communications that they would not ordinarily say or write in 'real life'. For example, it is claimed that e-mail users are often more blunt and direct in their communications and are less concerned with the possible impact their speech may have. The words they choose, it is suggested, are more harsh or crude than those used in other contexts.

Disinhibtion among CMC users has also been attributed to a lack of regulating feedback in electronic communications. There is no body language, no change in tone of voice or facial expression in

CMC. There are only letters, numbers and symbols. Reid claims that this lack of social context cues obscures the boundaries that would generally separate acceptable and unacceptable forms of behaviour. According to Reid, this can lead to extremes of behaviour on-line including hostility and aggression.

It is also suggested that people attach less significance and weight to their electronic correspondence. Electronic messages are often regarded as casual and transitory and are, it is alleged, less reflective as a result. This is in part due to the fact that people assume that their one-to-one messages are private and will be seen only by the recipient and because users are often unaware that most e-mail systems can create a complete record of a communication.

Harassment on-line has also been linked to sex differences in computer-mediated communications. While research in this area has only recently begun, a number of researchers have already argued that men tend to be more adversarial in their on-line interactions and use intimidation tactics to dominate and control on-line discourse. Susan Herring is one such researcher who claims that men are more belligerent on-line and more likely to use angry and abusive language. The practice of flaming is given as example. Flames are highly aggressive, sarcastic, vulgar, or critical responses sent to a user. The general acceptance of flaming on-line is reflected in rules of nettiquette: rules regarding appropriate behaviour on-line. Virgina Shea, author of *Netiquette*, explains that although flames often get out of hand, they have a purpose in the ecology of cyberspace. Flames are aimed at teaching someone something or stopping them from doing something. While conceding that flame messages often use more brute force than is strictly necessary, Shea maintains, that that is half the fun. It has been argued that these rules, which have been developed largely by men, have a definite male bias and fail to acknowledge that women often find this type of interaction intimidating. For example, Dale Spender, author of *Nattering on the Net,* likens net rules to those governing a boxing match "[n]o hitting below the belt, no fighting dirty; may the best man win." Most netiquette statements acknowledge that the going can get rough but, according to Spender, the answer is invariably, that if you can't take the heat, stay out of the kitchen.

Tackling harassment on-line

Legal Regulation

In the United States concerns that existing laws are inadequate to deal with on-line harassment has led to calls for specific cyberstalking legislation. A number of US states now have specific cyberstalking statutes. The first US State to include on-line communications in its statutes against stalking was the state of Michigan in 1993. Other states which have anti-stalking laws that include electronic harassment include Arizona, Alaska, Connecticut, New York, Oklahoma, and Wyoming.

In contrast, in the UK existing laws are sufficiently flexible to encompass on-line stalking and e-mail harassment. A person sending offensive or threatening messages may, for example, commit an offence under the Telecommunications Act 1984 section 43 which 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. 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. It creates two criminal offences, the summary offence of criminal harassment and an indictable offence involving fear of violence. 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.

Harassment includes alarm and distress but these terms are not defined in the Act; they 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 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.

The use of these laws will, however, 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

The Internet presents law enforcement bodies with unique problems. These pertain mainly to the 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 that a potential offender may not be within the jurisdiction where an offence is committed. Anonymous use of the Internet also promises to create challenges for law enforcement authorities. True anonymity on-line is 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 allocating an "anonymous ID". The most sophisticated re-mailer technology is called MixMaster which uses public key cryptography, granting unprecedented anonymity to users who wish to communicate in complete privacy. By chaining together several re-mailers a user could create a trail so complex that it would be impossible to follow. 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. Opponents of anonymity argue that it threatens civility and accountability on-line. Those who call for such restrictions 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. Free speech is facilitated by anonymity on line. It allows human rights activists, political and religious dissidents, and whistle blowers throughout the world to engage in confidential communications free from intrusion. Anonymity is also important for on-line discussions and newsgroups dealing with sensitive issues such as sexual abuse, domestic violence and alcoholism. Users seeking access to information on AIDS, for example, or seeking guidance from the Samaritans clearly benefit from remaining anonymous. Anonymity can also facilitate the protection of privacy on the Internet. On-line users can currently use web based services such as the Anonymizer to surf the web anonymously thus enabling them to evade surveillance and monitoring of their activities on the Internet. The importance of anonymity both to free speech and privacy on the Internet should not be underestimated and the need to protect these freedoms should shape any future regulatory initiatives.

Non-legal solutions

Ignore it

Some advocates of free speech on the Internet have been quick to urge against legislative or regulatory solutions and to advise women simply to ignore on-line harassment. These commentators present harassment as an inescapable, if regrettable feature of life on-line. Jensen, for example, argues that women should take a "sticks and stones" approach to abusive and offensive e-mail messages. However, such a view assumes that 'minor' incidents of harassment do not have a real and significant impact on women users. Advising women simply to put up with the more mundane everyday instances of on-line harassment fails to acknowledge that this type of 'dripping tap harassment' may well cause some women to curb their activity on-line. Simply ignoring the problem, or asking individual women to handle on-line harassment at a personal level, it is submitted, is not a satisfactory solution.

Anti-harassment policies

The development and introduction of voluntary anti-harassment policies has been advocated as another means of tackling harassment on-line. For example, the Web site Women Halting On-line Abuse ('WHOA'), launched in 1997, aims to educate the Internet community about on-line harassment and to formulate voluntary policies that system administrators can adopt in order to create harassment-free environments. Samples of possible policies that administrators may wish to adopt are provided on the WHOA site which also contains a list of "safe sites" which have an observable anti-harassment policy that is enforced. ChaTciRCuiT, is one of the sites listed and its Chat Policy for their IRC Chat site states that the "use of speech as a means to hurt others, such as threats, harassment, racism, or obscenity will not be permitted." TalkCity, another site listed by WHOA, has adopted a similar policy simply stating that expressions of bigotry, hatred, harassment or abuse" will not be tolerated. It is unlikely that anti-harassment policies alone will be effective in tackling Internet harassment, however, they may serve to raise awareness and are likely to stimulate debate within the Internet community.

Women-only cyber spaces

The development of women-only forums has been suggested as a way to counteract sexual harassment. Women are already creating their own cyber spaces, through the creation of web sites, newsgroups and chat channels dedicated to areas of interest to women. Women'space and Virtual Sisterhood are examples of electronic resources for women on-line. These sites are however also open to both men and women users. The merits of separatism are questionable and given the ease with which electronic personas can be spoofed on the Internet, segregation in on-line forums could prove impossible to control. Defending women-only forums, Spender argues that while separatism is not necessarily what women want for their discussions, until gender equality becomes a reality in a wide variety of settings, women need both access to the public nets and some safe forums for their conversations.

Self-Protection

Self-protection is arguably the least problematic solution to stalking and harassment on the Internet. The education of users is the first step towards self-protection. There are many web sites and books which provide information for self-protection from cyberstalkers for on-line users. In general, women are advised, where possible, to adopt either a male or gender neutral user name. It is recommended that personal information divulged on-line be kept to a minimum. To guard against on-line impersonation, users are also advised to use strong encryption programmes such as the Pretty

Good Privacy ("PGP") to ensure complete private communications. New and innovative software programmes which enable users to control the information they receive are also being developed. 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. In the future, advanced filtering systems which recognise insulting e-mail may also be available.

Conclusion

In highlighting the issues surrounding cyberstalking this paper has sought to question the appropriateness of various means of tackling Internet harassment. The limitations of legal regulation have been identified and so too have the potential costs in terms of fundamental freedoms. This paper suggests that there are more suitable ways in which users can both empower and protect themselves from on-line harassment such as through practical solutions at a personal level. This favouring of self-regulatory solutions is also in line with developments elsewhere where legal regulation at a national level is recognised increasingly as futile and also undesirable.