THE INTERNET AND CYBERSTALKING

Dr Emma Ogilvie
Criminology Research Council / Australian Institute of Criminology

*Paper presented at the Stalking: Criminal Justice Responses Conference convened by the Australian Institute of Criminology and held in Sydney 7-8 December 2000*
Introduction

“Cyber crime” has increasingly moved to the foreground in examinations of 21st century criminality. Arguments as to whether Internet-based technologies have created entirely new types of crime requiring equally new legislative and other responses, or simply provided for new expressions of traditional crimes requiring the adaptation of current legislative strategies, are hotly debated by the proponents of both views. At the heart of this dispute is the more important question of whether or not it is possible to regulate the Internet to anything like the same extent other communication media are controlled.

This paper focuses upon cyberstalking because in this way it becomes possible to discern what is special about criminality that takes advantage of the unique possibilities offered by the Internet. Cyberstalking is analogous to traditional forms of stalking in that it incorporates persistent behaviours that instil apprehension and fear. However, because by definition cyberstalking takes place in a ‘virtual’ environment, it draws our attention to what is distinct about the world of the Internet and the way it incorporates dimensions never envisaged by those seeking to control behaviour though legislation.

Cyberstalking

Cyberstalking thus entails the same general characteristics as traditional stalking, but in being transposed into the virtual environment it is fundamentally transformed. The nature of this transformation is dependent upon what particular aspects of the Internet are exploited. The Internet is used by both those with an interest in efficient exercises of “traditional” criminality as well as those attuned to the possibilities of altogether new forms of criminality (Grabosky, 2000). In both instances, we need to understand what the Internet actually ‘is’ if we wish to determine the potential for criminality it entails. At present, our attempts to protect the wider community from cyber crimes are hindered by a failure on the part of policy makers to appreciate that the Internet offers access to domains beyond the reach of traditional legislative frameworks.

This means that before understanding the nature of cyberstalking, we need to first understand the nature of the Internet.

At a superficial level, the Internet is conceptually very simple. All that is happening is we have a means of efficiently transferring digitised data. There are three major ways in which these data exchanges can be categorised.

Categorising the Internet

- **Category One: The Internet as a medium of convenience** Data may be transferred directly from sender to a nominated and “willing” recipient. Person to person email communications are the most obvious example of this type of data exchange.

- **Category Two: The Internet as a Medium of Control.** Data may be exchanged in an interaction involving an unwilling and/or unknowing party being manipulated by a usually unknown and effectively invisible external party. Exploitation of the “back door” into the Windows operating system in order to take over control of another computer connected to the Internet is the obvious example of this second type of data exchange.

- **Category Three: The Internet as a medium of “range” enhancement** Data may be electronically positioned in such a way that any number of data “seekers” may locate and obtain it. Web sites that are “hit” by “net-surfers” are the obvious example of this third type of data exchange. Other examples include Internet Relay Chat (IRC), Multiple-User Dungeons (MUDs) and Multiple Object-Oriented domains (MOOs).
Each of these three types of data exchange mechanisms constitutes a particular form of ‘virtual’ social interaction that may or may not accompany an interaction ‘in real life’ (IRL). In drawing the concepts of virtual events versus IRL events, we are obviously drawing upon the language of the Internet itself. Some might argue that the distinction between the virtual world of cyber space and the more substantial IRL world is false or misleading, in that in both cyberstalking and IRL stalking, real people are communicating whether it be by computer connections, telephone, letters, face to face contacts, or whatever. However, the extent to which (virtual) cyber interactions both resonate with (IRL) pre-Internet endeavors and are amenable to regulation, is far from uniform. The cyber/IRL distinction is therefore useful for clarifying the difference between cyber crimes that are extensions of traditional criminal behaviours, and cyber crimes that are wholly distinct from traditional forms of criminality. Use of the Internet to distribute illegal pornography for example, is a good example of a cyber crime that closely resembles the “real” world. Digitised images are transferred on a commercial basis between providers and purchasers. Essentially, all that is occurring is that the Internet is providing a convenient new forum for a particular aspect of the “hidden” or “black” economy (as well as the legitimate trade in legal images). Digital data are transferred instead of pictures in brown paper envelopes. In contrast, the distribution of digitised music via ‘MP3’ files across networks such as NAPSTER (and more especially, ‘Freenet’) represents the development of ‘virtual communities’ that not only threaten notions of copyright and intellectual capital, but also redefine what the Internet ‘is’ in ways that were never anticipated. Between these two extremes, there are activities such as cyberstalking, which owe something to the real world and something to the virtual world. In thinking about cyberstalking in terms of the three categories of cyber interaction we can obtain a sense of how the movement from IRL crime to virtual crime may entail a shift from the controllable to the uncontrollable. Cyberstalking provides an especially illustrative example of this shift because of the way it can occur as an instance of each of the three types of cyber interaction.

**Category One: The Internet as a medium of convenience**

Unsolicited e-mail is one of the most common forms of harassment, including hate, obscene, or threatening mail. Other forms of harassment include sending the victim viruses or high volumes of electronic junk mail (spamming). In many ways, stalking via e-mail represents the closest parallel of traditional IRL stalking patterns. Given that the most common forms of stalking behaviour are telephoning and sending mail (Burgess et al, 1997; Mullen et al, 1999; Tjaden, 1997), the adoption of e-mail by stalkers is not surprising. As a medium, e-mail incorporates the immediacy of a phone call, but also introduces the degree of separation inherent in a letter.

As with IRL stalking, e-mail stalking can result from an attempt to initiate a relationship, repair a relationship or threaten and scare a person. Interestingly though, those cases which have been prosecuted have tended to fall into the latter category. For example, in the first case to be prosecuted in Queensland, a woman received e-mail correspondence that began amicably, but then became more threatening once she sought to end the communications. She ultimately received death threats from the offender and threats to “have [her] pack-raped, videotaped and uploaded on the Internet” (Keim, 2000).

In another case brought to court in the United States, a University student harassed five female students after buying information about them via the net. The student sent over one hundred messages including death threats, graphic sexual descriptions and references to their daily activities (Grabosky, 2000). Similarly, in California, a university student was charged in connection with a 1996 e-mail he sent to 59 predominantly Asian students. The anonymous message signed “Asian Hater,” said, “I personally will ... find and kill everyone of you…” (Masters, 1998).

---

1 It is important to note here that sending viruses or telemarketing solicitations are not in and of themselves indicative of stalking. However, if these communications are repetitively sent in a manner which is designed to intimidate (ie: similar to the manner in which IRL stalkers send subscriptions to pornographic magazines), than they may constitute “concerning behaviours” and hence be included as stalking.
What is interesting about these cases is that they all resulted in prosecution of some kind (although while the latter two were charged under stalking, the Queensland case was charged under illegal use of a telecommunications device). It is at least arguable that these prosecutions occurred because the harassment closely resembled traditional forms of “postal” stalking. The offenders e-mail could be traced and their identities established in much the same way a letter could be traced through the postal system. The majority of these cases did not involve technically complex forms of stalking, and e-mail was simply being utilised as a more convenient form of letter writing. This is not always the case however, and the free availability of anonymizers and anonymous re-mailers (which shield the senders identity and allow the e-mail content to be concealed – and can be accessed free of charge on the Internet) provide a high degree of protection for stalkers seeking to cover their tracks more effectively.

Category Two: The Internet as a Medium of Control

Whilst the first category of cyber stalking can “spill over” into real world interactions, the “distancing” quality of the cyber component of the interaction is nevertheless a defining feature of the interaction. If there is no movement into the real world, targets of the harassment are still able to buffer themselves from exposure to the stalker by avoiding those parts of the Internet being used by the stalker. The necessity to do this is of course an intrusion upon the rights of the individual, but it is at least a strategy that can be employed to obtain a degree of distance between stalker and victim. In the second category of cyber stalking, this defensive strategy is undermined by the stalker. In essence, the stalker exploits the workings of the Internet and the Windows operating system in order to assume control over the computer of the targeted victim.

It is probably not widely recognised that an individual Windows based computer connected to the Internet can be identified and connected to by another computer connected to the Internet. This “connection” is not the “link” via a third party characterising typical Internet interactions but rather is a direct computer to computer connection allowing the interloper to exercise control over the computer of the target. At present, a reasonably high degree of computer “savvy” is required to undertake this form of exploitation of the Internet and the Windows operating system. However, and inevitably, instructions as to how to use the technologies in this way are available on the Internet, and it is not unlikely that progressively easier “scripts” for the exercise will be made freely available for anyone so inclined to download.

In practice what this means is that individual computer users have a vastly reduced buffer between themselves and the stalker. A cyber stalker can communicate directly with their target as soon as the target computer connects in any way to the Internet. The stalker can assume control of the victim’s computer and the only defensive option for the victim is to disconnect and relinquish their current Internet “address”. The situation is rather like discovering that anytime you pick up the phone a stalker is on-line and in control of your phone, with the only way to avoid them being to disconnect the phone completely and then reconnect with an entirely new number.

Only one specific example was found of this technique being utilised in stalking, where a woman received a message stating “I’m going to get you” - followed by the interloper opening the woman’s CD rom drive in order to prove he had control of her computer (Karp, 2000). More recent versions of this technology claim to be able to allow real-time keystroke logging (the recording of every keystroke) and a view of the computer desktop in real time (Spring, 1999). It is not difficult to imagine that such a facility will appear an appealing possibility for those interested in cyber stalking.
Category Three: The Internet as a medium of “range” enhancement

Like IRL forms of harassment and stalking, few examples of stalking are confined to simply one medium. While e-mail stalking may be analogous to traditional stalking in some instances, it is not restricted to this format. Stalkers can more comprehensively utilise the Internet in order to slander and endanger their victims. In such cases, the cyberstalking takes on a public rather than private dimension.

In one example, a female University lecturer was stalked for a period of some years. Her ex boyfriend would habit her usual chat sites and then follow her from site to site, recording where she went. He also posted false information about her in various chat sites including both those she habited and pornography sites that he visited. Finally he hunted down and distributed semi-pornographic photographs of her as a young girl across the net (Gilbert, 1999). In another example a woman was stalked for a period of six months. Her harasser posted notes in a chat room that threatened to rape and kill her, and also posted doctored pornographic pictures of her on the net together with personal details (Dean, 2000).

What is particularly disturbing about this second form of cyber stalking is that it appears to be the most likely to spill over into “real space”. In these instances cyberstalking is accompanied by traditional stalking behaviours such as threatening phone calls, vandalism of property, threatening mail and physical attacks (Laughren, 2000).

An example of the blurring of the lines between cyber and the real involved a Los Angeles security guard whose romantic advances were rejected by a 28-year-old woman. In response, he impersonated her in chat rooms, and, pretending to be her, posted the woman’s name, address and phone number, claiming that she was looking for men who would provide substance to her rape fantasies. The result of these postings was that the woman was “repeatedly awakened in the middle of the night by men banging on her front door, shouting that they were there to rape her” (Maharaj, 1999). Similarly, an author was stalked by a publishing company who, among other techniques such as spamming, also placed her name, home address and home phone number on the web, with an advertisement saying that she “would be available for sex anytime, day or night” (CBS, 1999). Needless to say, she received multiple proposals.

Perhaps the most disturbing example of this merging of the cyber world with the real world involved a young male who hunted down a female ex classmate, who he believed had “humiliated” him at high school. The young man maintained a web site for a period of nearly two years dedicated to describing the girl, providing updates on her, and outlining his plans for her. He discovered her social security number, licence-plate number and place of employment (interestingly enough via Internet people finder companies). He then detailed his plans to kill the girl on a website. Only 41 minutes after his final website update, he drove to the girls place of work and shot her as she got into her car (Romei, 1999).

IRL Implications

When we understand the Internet as a composite medium potentially incorporating three quite different types of data exchange interactions, the problematic nature of Internet-based crimes quickly becomes apparent. Cyber crimes can in some instances closely resemble real world crimes but in other instances are so virtual that their connection with the real world is tenuous and constantly shifting.

Cyberstalking provides an illuminating example of what it means to be faced with fertile new ground in which crime can flourish untroubled by effective surveillance and control. The extent to which cyberstalking can be routinely regulated and responded to by the criminal justice system
depends upon the extent to which it occurs as an articulation of the first of the three highlighted types of interaction. Control of the second type of interaction may prove to be achievable via technological ‘fixes’ of one sort or another, but exploitation of the third type of interaction takes us into entirely foreign territory where “the old ways no longer hold good”.

The person to person (or organisation to organisation) communications identified as the first type of exchange, are conceptually not so very different from old-fashioned postal communications and can in all likelihood be regulated by extensions to current legislative initiatives, as has indeed been undertaken in the United States. Email correspondence may be kept as “evidence” of a concerning act and current stalking legislation should theoretically allow for e-mail to be considered a threatening communication. The more predatory second type of exchange may be highly problematic but it is not unreasonable to expect a technical fix that renders Internet users less exposed to the Windows “backdoor” (Norman, 1999). Conceptually, this second form of interaction simply represents a new expression of the “old crime” of misappropriation. Whilst apprehension of the perpetrator of such a crime may or may not prove to be possible, defining such activities as “illegal” would not be difficult.

The third type of data exchange mechanism however is quite different from the other two types and presents serious challenges to both pre-Internet conceptions of social interactions based upon data exchanges, and any attempts to regulate such interactions. In a further “twist”, this third type of interaction is increasingly opening up possibilities for the evolution of new forms of the other two types of data exchanges. Internet developments such as NAPSTER, Freenet and Gnutella permit data exchanges in such a way that they can no longer be readily understood in terms of concepts that pre-date the Internet and are increasingly resistant to notions of control that pre-date the Internet. Users of networks such as Freenet become members of virtual communities whose internal communications are extraordinarily difficult if not impossible to either monitor or regulate. In the future, this avenue for communication might well come to include highly invasive and predatory e-mail type communications that would be essentially immune to any attempts at control.

In examining this third form of interaction, the Internet needs to be recognised as a new medium of communication rather than the “latest version” of the old mediums. In discussing the Internet we are not discussing traditional criminal contexts. Instead, we are faced with substantial challenges to legislative and regulatory controls that rely upon clearly definable jurisdictional contexts and clearly definable behaviours. If a stalker in California uses an Internet Service Provider in Nevada to connect to an anonymiser in Latvia to target a victim in Australia what jurisdiction has responsibility for regulating the cyberstalking? Even assuming it is possible to resolve these new jurisdictional problems it is far from clear that anything could be done to actually “bring the cyberstalker to justice”. At least as far as the Internet is concerned, the “stalker” is after all nothing more than a digital address. While such addresses may be traced, they may also be continually hidden, shifted, and altered.

Whilst it can be argued that some cyber crimes are no different from real world crimes in as much as they reflect the same range of offensive and dangerous behaviours, it also needs to be acknowledged that the Internet can magnify, distort and ignore the attributes of the real world in ways we urgently need to address.

The first step in effectively responding to Internet based crime in general and cyberstalking in particular, is to ensure our understanding of the Internet is derived from a realistic appreciation of the nature of the new technologies themselves rather than being rooted in a pre-Internet conception of information exchange mechanisms. Whether we like it or not, the future will be a foreign country and we may have to do some things differently there.

---

2 It should be noted that this legislative problem is not specific to stalking and while the jurisdictional issues are difficult, legislators are attempting to address them. See The Model Criminal Code (2000).
References


