AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 166

Cyberstalking

Emma Ogilvie

Victims of stalking suffer dreadfully, and the nature of the response to their plight varies across jurisdictions. To add to traditional forms of stalking, there have been experience of email stalking, Internet stalking and computer stalking. The Australian Institute of Criminology has been a pioneer in the analysis of cyber crime, and this paper adds to that body of knowledge.

This paper examines cyberstalking as an example of a crime that is simultaneously both amenable to, and resistant of, traditional forms of legislation, depending upon the way in which the possibilities of the Internet are exploited. Cyberstalking is analogous to traditional forms of stalking, in that it incorporates persistent behaviours that instil apprehension and fear. However, with the advent of new technologies, traditional stalking has taken on entirely new forms through mediums such as email and the Internet. Cyberstalking dramatically signals the potential of the Internet to facilitate some types of crimes, as well as pointing to the interventions available and likely to prove effective. To date, there is no empirical research to determine the incidence of cyberstalking.

Arguments as to whether Internet-based technologies have created entirely new types of crime requiring equally new legislative and other responses, or provided new expressions of traditional crimes requiring the adaptation of current legislative strategies, are hotly debated by the proponents of both views.

Adam Graycar
Director

September 2000

ISSN 0817-8542
ISBN 0 642 24181 3

Criminology Research Council

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

Stalking and Cyberstalking

Stalking is a relatively recent crime in Australia, with legislative efforts at containment beginning in the mid-1990s. Officially, there are a number of ways in which stalking has been described.

> A constellation of behaviours involving repeated and persistent attempts to impose on another person unwanted communication and / or contact (Mullen et al. 1999, p. 1244).
>
> When one person causes another a degree of fear or trepidation by behaviour which is on the surface innocent but which, when taken in context, assumes a more threatening significance (Goode 1995, p. 24).
>
> The willful, malicious, and repeated following and harassing of another person that threatens his or her safety (Meloy and Gothard 1995, p. 258).

Cyberstalking is analogous to traditional forms of stalking in that it incorporates persistent behaviours that instil apprehension and fear. However, with the advent of new technologies, traditional stalking has taken on entirely new forms through mediums such as email and the Internet. Thus, it becomes cyberstalking. Increasingly, cyberstalking is gaining the attention of the media and the public as the nature of the crime incorporates elements of new technology and threatening behaviours, which symbolise a new form of threat. Unfortunately, we have absolutely no empirical research upon which to estimate the actual incidence of cyberstalking and, indeed, determining the magnitude (or not) of this crime is practically impossible.

It has been argued, however, that such incidents may be more common than traditional forms of stalking. This is because the basic apparatus of the Internet, including free email and chat rooms, facilitate contact with an immense field of potential victims. For example, "a single user can send the same file to hundreds of people in far less time than it would take to telephone or write them" (Masters 1998). The manner in which cyberstalking is conducted, however, is dependent upon the particular use of the Internet being exploited. There are three primary ways in which cyberstalking is conducted.

- **Email Stalking**: Direct communication through email.
- **Internet Stalking**: Global communication through the Internet.
- **Computer Stalking**: Unauthorised control of another person's computer.

Email Stalking

While the most common forms of stalking in the physical world involve telephoning, sending mail, and actual surveillance (Burgess et al. 1997; Mullen et al. 1999; Tjaden 1997), cyberstalking can take many forms. Unsolicited email 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). It is important to note here that sending viruses or telemarketing solicitations alone do not constitute stalking. However, if these communications are repetitively sent in a manner which is designed to intimidate (that is, similar to the manner in which stalkers in the physical world send subscriptions to pornographic magazines), then they may constitute "concerning behaviours" and hence be categorised as stalking.

In many ways, stalking via email represents the closest replication of traditional stalking patterns. Given that the most common forms of stalking behaviour are telephoning and sending mail, the adoption of email by stalkers is not surprising. As a medium, email incorporates the immediacy of a phone call and introduces the degree of separation entailed in a letter. It might be argued that email stalking is actually less invasive than phone calls because the victim can undermine the interaction by deleting, without opening, any suspicious or unsolicited messages. This argument does, however, deny the social meaning of email communication. As with telephone stalking, email harassment constitutes an uninvited and arguably threatening incursion into private space.

As with stalking in the physical world, email stalking can result from an attempt to initiate a relationship, repair a relationship, or threaten and traumatise 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 email 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 Northern America, a university student harassed 5 female students after buying information about them via the net. The student sent over 100 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 an email he sent in 1996 to 59 predominantly Asian students. The anonymous message signed "Asian Hater" and said "I personally will ... find and kill everyone of you ..." (Masters 1998).

What is interesting about these cases is that they all resulted in prosecution of some kind. It is at least arguable that these prosecutions occurred because the harassment closely resembled traditional forms of "postal" stalking. The offenders' email could be traced and their identities be established in much the same way a letter could be traced through the postal system. A majority of these cases did not involve technically complex forms of stalking, and email was simply being used as an alternative form of communication. However, this is not always the case. The free availability of anonymisers and anonymous remailers (which shield the sender's identity and allow the email content to be concealed) provide a high degree of protection for stalkers seeking to cover their tracks more effectively.

Internet Stalking

As with stalking in the physical world, few examples of stalking are confined to one medium. While email stalking may be analogous to traditional stalking in some instances, it is not restricted to this format. Stalkers can more comprehensively use the Internet in order to slander and endanger their victims. In such cases, the cyberstalking takes on a public, rather than a private, dimension.

In one example, a female university lecturer was stalked for some years. Her ex-boyfriend would visit 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 6 months. Her harasser posted notes in a chat room that threatened to rape and kill her, and posted doctored pornographic pictures of her on the net together with personal details (Dean 2000).

What is particularly disturbing about this second form of cyberstalking is that it appears to be the most likely to spill over into "physical 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). As noted by Gilbert (1999):

> In real life, stalkers usually stalk in proximity to their victims—they want the victim to see them and know they are there—they feed on the victim's reaction. On the Net, proximity takes on a new meaning. Obviously, there are important differences between the situation of someone who is regularly within shooting range of her or his stalker and someone who is being stalked from two thousand miles away.

While the previous examples can be viewed as offensive and threatening, they can, nevertheless, be viewed as distinct from "traditional" stalking in that they remain in cyber space. While emotional distress is (appropriately) acknowledged in most criminal sanctions, it is not considered as serious as actual physical threat. Thus, while links between stalking, domestic violence, and femicide have been empirically demonstrated "in real life" (Burgess et al. 1997; Kurt 1995; McFarlane et al. 1999), much cyberstalking remains at the level of inducing emotional distress, fear, and apprehension. However, this is not to say that causing apprehension and fear should not be criminally sanctioned, or that the cyber and the real are somehow inherently or intrinsically disconnected. Cyberstalking can be simply an electronic precursor to real world behaviours.

An example of the blurring lines between cyber and physical stalking 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 on the Internet, 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 News 1999). Needless to say, she received multiple proposals.

Perhaps the most disturbing example of this merging of the cyber world with the physical 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 2 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 girl's place of work and shot her as she got into her car (Romei 1999). Similarly, in an Australian case, an older male stalked a young boy, following him with a camera and placing updates of his activities on his personal website, including descriptions of his (the offender's) paedophilia and of his potential dangerousness to those who threatened him. The offender was charged with stalking (*R v Vose* [1999] VSCA 200).

Computer Stalking

Whilst the first two categories of cyberstalking 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 parts of the Internet 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 the stalker and the victim. In the third category of cyberstalking, 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; rather, it is a 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 on how to use the technologies in this way are available on the Internet. It is likely 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 like discovering that anytime you pick up the phone, a stalker is on-line and in control of your phone. The only way to avoid the stalker is to disconnect the phone completely, and then reconnect with an entirely new number.

Only one specific example of this technique was used in stalking. A woman received a message stating "I'm going to get you", the interloper then opened 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 enable real-time keystroke logging (the recording of every keystroke) and view the computer desktop in real time (Spring 1999). It is not difficult to hypothesise that such mechanisms would appear as highly desirable tools of control and surveillance for those engaging in cyberstalking.

Intervention and Legislation

Given the nature of cyberstalking—specifically its simultaneous resemblance to, and distance from, stalking in the physical world—the opportunities to intervene are varied. There are three primary ways in which cyberstalking can be countered, all of which will have varying degrees of success.

- Personal Protection.
- Technical Fixes.
- Legislation.

Personal Protection

While many may object that personal protection strategies are an infringement upon people's right to travel freely in cyber space, the fact is that personal prevention is taken on a daily basis in the physical world, and the cyber world is no different. Simple strategies such as not providing personal information to strangers are just as, if not more, applicable in cyber space. People who participate in the cyber world will minimise the likelihood of their being stalked by using techniques such as gender neutral and age neutral names. Personal information should not be recorded on the Internet and people should hesitate before filling in electronic forms which request names, age, addresses, together with personal likes and dislikes. Similarly, people can be pro-active before signing on to an ISP provider by researching beforehand on whether there are specific policies prohibiting harassment, abusive behaviours, and cyberstalking.

Technical Fixes

It is also important to note that many of the solutions to cyberstalking are likely to come about through technological fixes, rather than personal or legislative intervention. Personal familiarity with the many "filter" programs available now, both in chat rooms and many email services, allow users to block unwanted messages, or messages received from unknown sources. Whilst anonymous remailers and browsers further reduce the likelihood of potential stalkers being able to identify victims. Most specifically, the third type of stalking described, that carried out through control of a computer, is likely to be easily fixed through a technological "patch" which no longer allows people to access other computers. Already there are programs available on the Internet which scan ranges of IP-addresses for the existence of Back Orifice and / or Netbus servers. There are directions available on how to disarm these intrusions and render Internet users less exposed to the Windows "backdoor" (Norman 1999).

Legislative Responses

In many ways the legislative responses are the most difficult. In theory, there is no reason why current legislation covering stalking should not also cover cyberstalking. While stalking legislation has been drafted differently across the states[1], it is generally defined as acts engaged in on more than one occasion which are intended to cause fear or apprehension. While Victoria and Queensland are the only states to include sending electronic messages to, or otherwise contacting, the victim, elements of the offence for most states cover activities which "could" include stalking. These include such activities as:

- keeping a person under surveillance;
- interfering with property in the possession of the other person, giving or sending offensive material;
- telephoning or otherwise contacting a person;
- acting in a manner that could reasonably be expected to arouse apprehension or fear in the other person; or
- engaging in conduct amounting to intimidation, harassment, or molestation of the other person.

Two possible exceptions here are New South Wales and Western Australia, which have far narrower definitions of what constitutes stalking. Hence, both states identify specific locations such as following or watching places of residence, business, or work which may not include cyberspace. While cyberstalking could be included within "any place that a person frequents for the purposes of any social or leisure activity", the prosecution possibilities seem limited. Other difficulties may occur in South Australia and the Australian Capital Territory, where there is a requirement that offenders intend to cause "serious" apprehension and fear. Thus, the magistrates may dismiss cases of cyberstalking, given the lack of physical proximity between many offenders and victims.

In general, however, cyberstalking should fall within the same domain as the current offence of physical stalking. More specifically, violent email messages could be deemed to be subject to the current (physical) stalking legislation with respect to "intent to cause apprehension or fear". Similarly, assuming control of another person's computer could be deemed to constitute "interfering with property". In saying this, however, cyberstalking has become renowned for the difficulties involved in actually prosecuting it. The simple inclusion of email or Internet communications within the definition of offensive communications would go a long way towards easing current difficulties in prosecution, as has indeed occurred in Northern America.

While the criminalisation of threatening emails would be a reasonably easy fix, it does not overcome the primary difficulties in legislating against cyberstalking, which are the inter-jurisdictional difficulties. While in many ways cyberstalking can be considered analogous to physical world stalking, at other times the Internet needs to be recognised as a completely new medium of communication.

It is at this point that legislating against cyberstalking becomes difficult. In discussing the Internet, we are not always 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, which jurisdiction has responsibility for regulating the cyberstalking? Indeed, this is precisely what occurred in a Victorian case where a charge of stalking was dismissed because the victim lived overseas. Despite the fact that the alleged stalking had been occurring over 6 years, and involved repeated unwanted emails, phonecalls and letters, it was stated that "the [defendant's] actions must have the effect of causing fear or apprehension in the victim, and in this case the victim would have felt any apprehension or fear in Canada." (Magistrate Wakeling cited in Hunt 2000).

This legislative problem is not confined to cyberstalking and, indeed, is one of the primary issues needing to be addressed in most computer-related crimes. While legislators have attempted to provide models for how these difficulties might be addressed (*see* The Model Criminal Code 2000), the possibilities are limited. One option is to follow the American recommendations, which is for states to retain primary jurisdiction over cyberstalking cases, but for federal laws to be written in order to amend existing gaps in legislation so that transmission of communications interstate or internation may be addressed (Report on Cyberstalking 1999). 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", particularly given the substantial costs involved in such exercises. 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.

Conclusion

It can be seen that addressing cyberstalking involves a variety of different approaches, including personal prevention strategies, legislative interventions, and technological solutions to current technological flaws. However, the first step in effectively responding to cyberstalking in particular, and Internet-based crime in general, 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. 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.

Cyberstalking provides an illuminating example of cyber crime. The extent to which cyberstalking can be regulated and responded to by the criminal justice system depends in many respects upon the extent to which it emulates traditional stalking behaviours in the physical world. Cyberstalking conducted through email may well be the easiest to prosecute given its similarity to postal communications. Similarly, intervening in computer stalking may well be better suited to technological fixes, particularly firewalls. However, the exploitation of the Internet to engage in cyberstalking may pose real difficulties in terms of identification and prosecution. The "new" technologies are so different from the old that "the old ways may no longer hold good", and we may need to re-assess our thinking about the nature of the possible intervention strategies. In sum, while some of the traditional strategies will remain applicable in addressing cyberstalking, new and innovative legislative, technical, and investigative countermeasures will almost certainly be necessary.

Notes

[1] For a more detailed overview of stalking legislation, *see* Ogilvie (forthcoming).

REFERENCES

Burgess, A., Baker, T., Greening, D., Hartman, C., Burgess, A., Douglas, J. and Halloran, R. 1997, "Stalking Behaviours Within Domestic Violence", *Journal of Family Violence*, vol. 12, no. 4, pp. 389–403.

CBS News 1999, "An Online Tragedy". http://cbsnews.cbs.com/now/story/0,1597,175556-412,00.shtml

Dean, K. 2000, "The Epidemic of Cyberstalking", Wired News: http://www.wired.com/news/politics/0,1283,35728,00.html

Gilbert, P. 1999, "On Space, Sex and Stalkers", *Women and Performance*, vol. 17, pp. 1–18.

Goode, M. 1995, "Stalking: Crime of the Nineties?", *Criminal Law Journal*, vol. 19, pp. 21–31.

Grabosky, P.N. 2000, "Computer Crime: A Criminological Overview", paper presented at the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna. http://www.aic.gov.au/conferences/other/compcrime/index.html

Hunt, E. 2000, "Stalker Law for Locals", *Herald Sun (Melbourne)*, 25 July 2000, p. 15.

Karp, H. 2000, "Angels Online", *Readers Digest*, pp. 34–40.

Keim, T. 2000, "Cyberstalk Charge Looms", *Courier Mail*, 27 April 2000.

Kurt, J. 1995, "Stalking as a Variant of Domestic Violence", *Bulletin of the American Academy of Psychiatry and Law*, vol. 23, no. 2, pp. 219–30.

Laughren, J. 2000, "Cyberstalking Awareness and Education". http://www.acs.ucalgary.ca/~dabrent/380/webproj/jessica.html

McFarlane, J., Campbell, J.C., Wilt, S., Sachs, C., Ulrich, Y. and Xu, X. 1999, "Stalking and Intimate Partner Femicide", *Homicide Studies*, vol. 3, no. 4, pp. 300–16.

Maharaj, G. 1999, "Chilling Cyberstalking Case Illustrates New Breed of Crime", *Los Angeles Times,* 23 January 1999. http://www.infowar.com/index.shtml? http://www.infowar.com/law/99/law 012799a j.shtml

Masters, B. 1998, "Cracking Down on Email Harassment", *Washington Post*, November 1888. http://www.washingtonpost.com/wp-srv/local/frompost/nov98/email01.html

Meloy, J. and Gothard, S. 1995, "A Demographic and Clinical Comparison of Obsessional Followers and Offenders with Mental Disorders", *American Journal of Psychiatry*, vol. 152, pp. 258–63.

The Model Criminal Code 2000, "Chapter 4: Damage and Computer Offences", *Discussion Paper*, January 2000.

Mullen, P., Pathé, M., Purcell, R. and Stuart, G. 1999, "Study of Stalkers", *American Journal of Psychiatry*, vol. 156, no. 8, pp. 1244–249.

Norman 1999, "Windows Backdoor Programs", *Security Information: Week 11.* http://www.norman.com/corporate/security info/1999 11.htm

Ogilvie, E. (forthcoming), "Legislating, Policing and Prosecuting Stalking Within Australia", *Research and Public Policy Series*, Australian Institute of Criminology, Canberra.

Report on Cyberstalking: A New Challenge for Law Enforcement and Industry 1999, *A report from the Attorney General to the Vice President.* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.html

Romei, S. 1999, "Net Firms Led Killer to Victim", *The Australian*, 4–5 December 1999, pp. 19–22.

Spring, T. 1999, "Hacker Tool Targets Windows NT", *PC World.com* http://www.pcworld.com/pcwtoday/article/0,1510,11662,00.html

Tjaden, P. 1997, "The Crime of Stalking: How Big is the Problem?", *National Institute of Justice: Research Preview*, Office of Justice Programs, United States Department of Justice.

Acknowledgment

This paper is developed out of a larger project "Legislating, Policing and Prosecuting Stalking within Australia", funded by the Criminology Research Council.

Dr Emma Ogilvie is a Post-doctoral Fellow, Criminology Research Council, Australian Institute of Criminology.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.