International Journal of Cyber Criminology
Vol 2 Issue 1 January 2008

Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking

Lynne Roberts[1]
Curtin University of Technology, Australia

Abstract

Cyber-stalking is a crime that transcends national and jurisdictional boundaries. Victims and perpetrators of cyber-stalking may be geographically separated by physical borders (for example, residing in different countries) when the offences occur. This is problematic for investigating the crime, in determining the jurisdiction in which alleged offences have taken place and in which charges may be filed. Legal definitions of stalking (and cyber-stalking) and applicable sentences vary across jurisdictions, if indeed they exist, further muddying the water. This paper provides an overview of the current state of knowledge on cyber-stalking and ends with an examination of the difficulties in investigating and prosecuting cyber-stalkers.

Keywords: Stalking; Cyber Stalking; Victims; Perpetrators;

Introduction

Cyber-crime is emerging as a major international criminological issue. Networked computers provide the media for new types (or variations on old types) of criminal activity to emerge. Cyber-stalking is one such crime enabled by the Internet. In contrast to many 'property' (financial) crimes enabled by the Internet, cyber-stalking represents a crime 'against the person'. This raises new issues for criminology and criminal justice in terms of the 'harms' that can be committed against a person in the absence of the physical presence of the offender. Yet relatively little research has been conducted into cyber-stalking to date. In a recent editorial J. Reid Meloy, a prominent stalking researcher, articulated one of the key future questions for stalking research as "What is the nature of cyber-stalking … ?" (Meloy 2007, p. 6).

This paper provides an overview of the current state of knowledge on cyber-stalking. It begins with a brief overview of what is known about stalking. Building on this knowledge, the concept of cyber-stalking is explored. Developing typologies of cyber-stalking and current estimates of the prevalence of cyber-stalking are provided. Possible relationships between cyber-stalking and off-line stalking are examined to shed light on whether cyber-stalking is simply an extension of off-line stalking behaviours or whether it

[1] Lecturer, School of Psychology, School of Psychology, Kent St, Bentley, Western Australia Email: Lynne.Roberts@Curtin.edu.au

is a new form of deviant/criminal behaviour. The paper ends with an examination of the difficulties in investigating and prosecuting cyber-stalkers.

Stalking

Stalking[2] refers to repeated unwanted intrusive behaviours that result in the victim experiencing fear, physical or psychological harm or emotional distress (Finch, 2001). While the range of possible behaviours included in the stalking spectrum is wide, eight clusters of stalking behaviours have been identified across studies: hyper-intimacy, mediated contacts, interactional contacts, surveillance, invasion, harassment and intimidation, coercion and threat and aggression (Cupach & Spitzberg 2004, cited in Spitzberg & Cupach 2007).

Stalking behaviour has been recorded in early Roman texts through to contemporary literature. Over time, conceptions of possible victims of stalking has widened from 'celebrities' and other public figures to include women harassed by ex-partners and finally to any individual who is subject to repeated intrusive pursuit that causes fear (Finch 2001; Mullen & Pathe 2002; Sheridan & Davies 2004).

Changing conceptions of victims are also reflected in changing conceptions of stalking motivations. 'Celebrity' stalkers were largely seen to have erotomania or morbid infatuations with their victims. With the broadening of victims definitions, stalkers are now seen to vary in their motivations and in their mental state (Mullen & Pathe 2002). Indeed, Kamphius and Emmelkamp (2000) caution that "stalking describes a behavioural problem, not a psychiatric diagnosis per se" (p. 208).

Spitzberg and Cupach (2007) outlined two theoretical frameworks within which stalking behaviours can be understood. First, viewed within an attachment framework, stalkers may exhibit an anxious or pre-occupied attachment style. Second, relational goal pursuit theory posits that individuals who associate the relationship with the victim with the meeting of their higher order goals (e.g. happiness and self-worth) may ruminate and experience negative affect when the relationship is thwarted, potentially motivating ongoing pursuit of the relationship.

More than twenty typologies of stalking have been proposed in the academic literature with three common underlying dimensions: the type of the underlying disorder (physiological, psychological or both), the type and context of the original relationship, and the primary motivation of the stalker (Spitzberg & Cupach 2007). The profusion of typologies suggests that further research is required in this area. As Kamphius and Emmelkamp (2000) commented:

There is a clear need to derive a consensus on a typology of stalkers, with associated diagnostic criteria. At present there is no evidence that one proposed typology is superior to another. The typology eventually agreed upon should have clear implications for treatment. (p. 207)

Stalking prevalence

Most research into stalking has been based on clinical samples of victims or forensic samples of offenders. In order to determine the prevalence of stalking, community samples are required. However, even prevalence estimates from community studies may be

[2] In this paper the term 'stalking' is used to refer to all types of stalking behaviours. The terms 'cyber-stalking' and 'off-line stalking' are used specifically to refer to computer-mediated stalking behaviours and stalking behaviours that are not computer-mediated respectively.

impacted by the definitions of stalking and thresholds used (e.g. the minimum amount of time over which stalking behaviours must persist, the minimum number of episodes required and whether it is a requirement that the behaviours evoke fear; Mullen & Pathe, 2002). Community-based surveys conducted in westernised countries report varying rates of stalking victimisation. In Australia, the 2005 Personal Safety Survey (Australian Bureau of Statistics, 2006) reported 19% of women and 9.1% of men reported ever being stalked (threshold of two or more incidents). In the United Kingdom, the 2004/5 British Crime Survey indicated that 23% of females and 15% of males have been stalked (Finney 2006; using threshold of two or more incidents). In a postal survey of a German city (Dressing, Kuehner & Gass 2005) 11.6% of adult respondents reported ever being stalking (using stricter threshold requirements of a minimum 2 weeks duration, more than one form of intrusive behaviour and the behaviour must have provoked fear).

Based on a meta-analysis of 175 stalking studies, Spitzberg and Cupach (2007) identified that females are significantly more likely to be stalked than males, estimating that 60-80% of victims are females. The majority (79%) of stalkers are known to their victim and are commonly (49%) previous romantic partners. Almost a third (32%) of stalking cases results in physical violence (12% sexual violence).

Effects of stalking

Victims may experience difficulty in knowing when intrusive relationship 'pursuit' behaviours become persistent stalking. Based on an empirical examination of an epidemiological study of stalking in the Australian community, Purcell, Pathe and Mullen (2004a) judged that intrusive behaviours that persist for longer than two weeks meet the threshold for persistent stalking. In almost half (45%) of the cases intrusive behaviours ceased within two weeks. Of the remaining cases, the median length of stalking was six months. There were no raised levels of psychiatric morbidity for victims of brief harassment (less than two weeks) but significantly elevated levels for those exposed to longer periods of harassment.

Spitzberg and Cupach (2007) identified three levels of stalking effects: first, second and third order effects. First order effects are the impacts on the victim and may include impacts on the individual's affective health (fear, anxiety, shame, loss, suicidal ideation, depression, sleep disturbances, impaired psychological well-being) social health (decreased trust, increased alienation and isolation, restricted social activities), resource health (additional security measures, absenteeism from work), cognitive health (maladaptive beliefs, attributions of self-blame, personality adaptation), physical health (physical and sexual violence) or resilience. Stalking may also result in behavioural or general disturbance (Dressing Kuehner & Gass, 2005; Kamphuis Emmelkamp & Bartak, 2003; McEwen Mullen & Purcell, 2007; Purcell Pathe & Mullen, 2002; Spitzberg & Cupach 2007). It is victims who are exposed to protracted periods of stalking who experience the highest rates of psychiatric morbidity, irrespective of the nature of the prior relationship with the perpetrator and the recency of victimisation (Purcell Pathe & Mullen, 2005). The ongoing experience of vulnerability may create more psychological distress than an actual physical assault (McEwen et al 2007). However, Dressing and colleagues (2006) note that while serious individual consequences are reported to result from stalking, the cross-sectional design of most stalking studies do not enable causal interpretations to be made (i.e. Is psychiatric morbidity a vulnerability factor or a consequence of being stalked?). Second order effects are impacts on the individual's social and institutional networks.

Third order effects are direct impacts on network members themselves. For example, network members may themselves be stalked by the perpetrator (Spitzberg & Cupach 2007).

Stalking legislation

Stalking behaviour has progressively been criminalised since the initial stalking legislation was passed in September 1990 in California. This was driven by the 'star stalking' and murder of actress Rebecca Schaeffer by a fan (Mullen & Pathe 2002). Since this first legislation stalking laws have been introduced into most westernized countries including the United States (49 states by end of 1993), Canada (1993), Australia (all states and territories between 1993 and 1995), United Kingdom (1997) and New Zealand (Purcell Pathe & Mullen, 2004b).

While there is a lack of uniformity in anti-stalking legislation across jurisdictions, laws typically contain three essential elements. First, laws specify that the offending behaviour(s) must be repeated, with a minimum contact requirement often specified as two or more occasions. Second, laws typically require that the offender either intends, or could be expected to know, that their conduct would cause mental or physical harm to the victim. The third element is that the victim must experience physical harm or emotional distress or fear for their safety (Purcell et al 2004b). The 'reasonable person' standard may be employed to ensure that conviction is not based solely on an individual victim's vulnerabilities. Dennison and Thomson (2005) argue in favour of conservative stalking laws claiming that both the victim's experience of fear or harm and the perpetrator's intent to cause fear or harm should be subject to the reasonable person standard.

The absence of traditional criminal intent requirements in some legislation makes stalking a 'victim-defined crime' (Mullen & Pathe 2002; Purcell et al 2004b). Repeated inappropriate socially inept behaviours, where each behaviour individually may be legal, taken together may be defined as criminal based on the reaction of the victim. Prior to the introduction of specific stalking legislation, only incidents that on their own met the definition of a criminal offence could be prosecuted, often restricting prosecutions to incidents of physical assault or property damage et al., 2004b).

Cyber-stalking

Cyber-stalking refers to stalking activities conducted in 'cyberspace' using information and communication technologies. Cyber-stalkers may utilise a range of tools and virtual environments including email, chat rooms, bulletin boards, newsgroups, instant messaging and key-logging Trojans. In their study of New York Police Department cyber-stalking cases, D'Ovidio and Doyle (2003) reported the most commonly used methods of cyber-stalking were email (79%) and instant messages (13%). The four main types of cyber-stalking activities reported in a survey were threats, harm to reputation (cyber-smearing), damage to data or equipment and attempts to access confidential information and computer monitoring (Bocij 2003b; Bocij & Sutton 2004; Pittaro 2008).

As with stalking in general, there is no consistently used definition of cyber-stalking in the literature. It should be noted however that the term cyber-stalking is itself not accepted universally. For example, Bahm (2003) argues in favour of the terminology 'the use of technology to stalk' in order to cover current and future forms of technology that can be used in stalking.

Two general typologies of cyber-stalking have been proposed. Ogilvie (2000) developed a typology of cyber-stalking that broadly characterises cyber-stalking according to the media used. Email cyber-stalking (the 'private' dimension) includes unsolicited emails, viruses and spamming. Internet cyber-stalking (the 'public' dimension) includes posting false information, personal information or pictures of the victim on the Internet and slander. Computer cyber-stalking includes the embedding of Trojans (used to log keystrokes or provide remote control of the computer) and unauthorised access to the victims computer. Spence-Diehl (2003) described a typology of cyber-stalking based on the degree of overlap with offline stalking. This typology consists of three categories: cyber-stalking restricted to cyberspace; cyber-stalking that begins in cyberspace but transitions to off-line stalking; and cyber-stalking as one method of stalking utilised in conjunction with other methods of off-line stalking. The two typologies, while developed separately from each other, can be used in conjunction with each other to describe both the relationship with off-line stalking and the type of media used. Each of the categories of stalking proposed by Spence-Diehl can utilise any, or a combination, of the media categories described by Ogilvie.

Other specific categories of cyber-stalking have been proposed. Bocij and McFarlane (2003a) describe third party cyber-stalking as a type of stalking by proxy where the perpetrator incites others to engage in harassing activities on his/her behalf. This may include activities such as placing false advertisements on the Internet using the victim's contact details. Adam (2002) describes the 'pay-off' for third-party cyber-stalkers in terms of

> *"…the original perpetrator becomes a voyeur, someone who invades and transgresses by watching and looking. This further reinforces the power that the perpetrator has over the victim"* (p. 137).

Third party cyber-stalking would appear to be a sub-category of Olgilvie's (2000) Internet cyber-stalking category. Involving third parties in stalking activities is not restricted to cyberspace. Stalking by proxy occurs off-line when the stalker engages others to communicate with, track or contact their victim. The forms this may take include the hiring of private detectives to monitor the victim's movements, ordering or cancelling goods and services, and enlisting the help of friends, family and acquaintances (Mullen Pathe & Purcell, 2000).

Bocij (2003a) proposed a typology of corporate cyber-stalking based upon whether the organisation is the stalker or the victim and the reasons for the stalking behaviour. This typology includes three categories of individuals stalking organisations (motivations of revenge, financial gain and ideological), two categories of organisations stalking individuals (where the organisation is an unknowing accomplice of a stalking employee, and for financial profit) and one of organisations stalking other organisations for competitive reasons. This typology does not fit neatly into more traditional conceptualisations of stalking, where the focus is on the repeated unwanted behaviour of one individual resulting in mental harm, physical harm or emotional distress to another individual. It moves the focus from interpersonal relationships to corporate relationships with its partial focus on financial and competitive gain.

Cyber-Stalking Prevalence

Most surveys of stalking do not allow the disaggregation of cyber-stalking from other stalking behaviours. Typically telephone calls, mail and electronic communication

are combined into a single category (e.g. ABS, 2006). In addition, most stalking surveys do not ask questions about other types of cyber-stalking activities such as the use of Trojans and cyber-smearing. Research to date that provides some indication of the prevalence of cyber-stalking is reviewed below.

Some studies of general stalking have included limited measures of cyber-stalking. Prevalence studies of college students have reported that between a half and a third of college students who report being stalked, report emailing as part of the stalking behaviours (Alexy Burgess Baker & Smoyak, 2005; Fisher Cullen & Turner, 2000). In a study based on the examination of records of 1005 North American stalkers Mohandie, Meloy, McGowan and Williams (2006) reported that a quarter of stalkers used mediated contacts such as letters, packages and email, with only one in twenty using cyberspace as the most frequent form of contact. Other surveys have focussed on cyber-harassment. Surveys of college students have found that between one in ten and a third of students report at least one form of online harassment (Finn 2004; Spitzberg & Hoobler 2002). Bocij and colleagues (Bocij 2003b; Bocij & Sutton 2004) used snowball sampling to obtain a survey sample of 169 Internet users. The results indicated that one in five met the criteria of repeated perpetration dependent upon ICT by one offender that caused distress to the victim. However, the sampling method utilised means that a non-representative sample was obtained.

To date, research specifically addressing cyber-stalking has not included community population-based surveys, limiting the generalisability of research findings. The exact prevalence of cyber-stalking and the percentage of general stalking episodes that contain cyber-stalking elements is still to be determined. As Spitzberg and Hoobler (2002) commented, previous estimates of the proportion of stalking cases that include cyber-stalking elements "represent little more than guesswork and extrapolation" (p. 76).

Relationship between cyber-stalking and off-line stalking

A currently contentious issue in the cyber-stalking literature is whether cyber-stalking is best conceptualised as a new form of deviant/criminal behaviour or as an extension of off-line stalking behaviours.

Bocij and colleagues (Bocij & McFarlane, 2003; Bocij & McFarlane 2003a, b) argue that it is a fallacy to assume that cyber-stalking is simply an extension of stalking. They describe cyber-stalking in terms of a new form of deviant behaviour exploiting new forms of information and communication technologies. In support of their argument they note that cyber-stalkers can pursue victims in other locations without need for physical or geographic proximity and may never have seen (in person or in photograph) or know any personal details (such as the age, gender, or ethnicity) of their victims. Some cyber-stalkers restrict their stalking activities to the Internet and some forms of stalking behaviours such as third party stalking are easier to encourage on-line. Cyber-stalkers can create multiple identities to aid in their stalking activities (Pittaro 2008). Further, they argue that motivations for cyber-stalking can vary from those of stalking and include corporate cyber-stalking for political, profit or competitive advantage. They also point to the distinction between stalking and cyber-stalking made by the public, press and governments.

Alternatively, cyber-stalking behaviours may be viewed as falling broadly within existing conceptualisations of stalking, with information and communication technologies providing new tools or methods for a stalker to use. Central to definitions of both cyber-

stalking and stalking are that persistent unwanted behaviours cause distress to victims. Cyber-stalking activities aimed at engaging the victim (such as repeated emails and instant messages) fit neatly within the 'mediated contacts' cluster of general stalking behaviours (Spitzberg & Cupach 2007) and are analogous to off-line behaviours of repeated and unwanted phone-calls, letters and parcels. Other behaviours such as cyber-surveillance using trojans fall within the surveillance cluster.

The conceptualisation of cyber-stalking as a form of general stalking is also supported by the 'cross-over' between cyber-stalking and off-line stalking. As suggested by Spence-Diehl's (2003) typology of cyber-stalking, while some individuals will restrict their stalking behaviours to cyberspace, others may begin by cyber-stalking their victim but transition to off-line stalking of their victim over time. Others may utilise cyber-stalking in conjunction with off-line stalking.

Cyber-stalking exhibits a marked degree of similarity with other forms of stalking. Rather than a new crime, cyber-stalking represents an old crime modified to take advantage of the affordances of the electronic environment. Over time as Internet use is 'normalised' there are likely to be less distinctions made between stalking and cyber-stalking. While some stalkers will exclusively use off-line or on-line methods of stalking, the majority are likely to use elements of both.

How does 'cyberspace' facilitate stalking activities?

The widespread adoption of the Internet provides individuals with unprecedented access to information about other individuals. The Internet, as a tool for stalking, can be used by stalkers to obtain information about current or potential stalking victims. This may include both information placed in the public domain by the individual (e.g. a personal web page) and information placed on-line without the knowledge or consent of the individual and over which the individual has no control. Identifying information typically available through search engines includes work place details, addresses, telephone numbers and organisations or groups to which an individual may belong. This publicly available information obtainable through searching the Internet may be supplemented through the use of paid on-line information broker search agencies (Tavani 2005). For example, Docusearch.com offers a 'comprehensive background dossier' for $59 that is based on searches of proprietary databases.

Stalkers may use the information obtained from both public and commercial sources on the Internet to aid in stalking their victims off-line. In a well-documented case Amy Boyer, aged 20, was stalked and murdered by Liam Youens. Search facilities, including Docusearch, were used by Youens to obtain information on where Boyer lived and worked and her vehicle details. Youens developed two web-sites. The first presented personal information about Boyer, including a picture of her. The second described in explicit detail Youen's plans to murder Boyer (Tavani 2002; Tavani & Grodzinsky 2002).

The Internet provides a wide range of opportunities for individuals to interact with other people that they might otherwise never meet. This expands the available 'pool' of victims. McGrath and Casey (2002) caution that this may result in increased stalking of 'strangers'. Preliminary research supports this supposition, with more than four out of ten survey respondents in one study not knowing the identity of their cyber-stalker (Bocij 2003b; Bocij & Sutton 2004).

Individuals with even limited technological sophistication can engage in the on-line surveillance of (potential) victims. They may engage in 'pre-surveillance' through

lurking in chat rooms, and may use applications such as 'finger' to determine when a targeted victim is online (Casey, 2004). In addition to providing the stalker with more information about the victim, the surveillance may feed voyeuristic fantasies and increase perceptions of power over the victim. This on-line surveillance is less likely to be detected than physical surveillance (McGrath & Casey 2002).

Many individuals develop a range of relationships on-line ranging from acquaintances to friends and romantic partners (McKenna Green & Gleason, 2002; Parks & Floyd 1996; Parks & Roberts, 1998; Wolak Mitchell & Finkelhor, 2002), experience a sense of community within virtual communities (Roberts Smith & Pollock, 2006) and give and receive emotional support (Whitty 2002). However, interactions on-line predominantly occur in text. The reduced sensory information available in text-based interactions may facilitate fantasy development, transference and a false sense of intimacy (Finn & Banach 2000; McGrath & Casey 2002; Meloy 1998).

In addition, it is easier to misrepresent one-self on-line than in face-to-face interactions and the likelihood of detection of this deception is reduced. Individuals are more likely to misrepresent themselves in online than offline romances, particularly in relation to age and physical attributes (Cornwell & Lundgren, 2001). The rapid expansion and increasing acceptance of on-line dating services may provide a fertile field for the development of one-sided obsessive relationships where individuals engage in deceptive impression management in order to facilitate early attraction (Spitzberg & Cupach forthcoming). In a survey of female customers of three Internet dating sites, 15.7% reported experiencing on-line verbal abuse, 26.9% obscene emails and 8.2% threatening emails (Jerin & Dolinsky 2001).

Cyber-stalkers can use technological means to provide a level of anonymity to their stalking behaviours. Anonymous email re-mailers and web-browsing services can be used to strip identifying information from messages. Stalkers can hide their identity through the use of anonymous and forged emails (Casey 2004). The anonymity provided may reduce social inhibitions, restraints on behaviour and accountability for actions (Bocij & McFarlane 2003a; D'Ovidio & Doyle 2003; McGrath & Casey 2002). The ability to disguise ownership of messages and to destroy evidence combined with the absence of capable guardianship of the Internet means there are limited deterrents to cyber-stalking behaviours online (Bocij & McFarlane 2003a). However, not all cyber-stalkers are technologically sophisticated and some are unaware of measures to keep their communications anonymous (McGrath & Casey 2002).

Cyber-stalking perpetrators

Limited information is known about cyber-stalkers. Research based on cases that have been criminally investigated suggests that cyber-stalkers are predominantly young males who are well-educated and technologically sophisticated (D'Ovidio & Doyle 2003; Lucks, 2004) – matching the profile of early adopters of the Internet. While a preliminary typology of cyber-stalkers has been proposed (McFarlane & Bocij 2003) this was based on a sample of only 24 cyber-stalkers. The studies conducted to date into cyber-stalking perpetrators are limited by their small sample sizes and being drawn from specific populations. As such, the results are best seen as preliminary and may not be generalisable to all cyber-stalkers.

Cyber-stalking Victims

As with perpetrators, limited research has been conducted into the characteristics of victims of cyber-stalking. D'Ovidio and Doyle (2003) examined the characteristics of cyber-stalking victims from 171 closed cases investigated by Computer Investigation and Technology Unit of the New York Police Department. Just over half (52%)of victims were female, a third (35%) were male and the remainder were organisations (8% educational institutions, 5% private corporations and 1% public sector agencies).

Cyber-stalkers may seek 'victims of opportunity', targeting inexperienced Internet users through services such as AOL (Casey, 2004). Novice users report more threats than experienced users (Bocij 2003b; Bocij & Sutton 2004). More competent computer-mediated communication users may be less likely than inexperienced user to become the victims of cyber-stalking (Spitzberg 2006) and experience harassment as less distressful (Bocij 2003b; Bocij & Sutton 2004).

Limited research has detailed the harms experienced by victims of cyber-stalking. In the absence of physical harm and the physical presence of the offender, it is likely that the ongoing threat and experience of vulnerability will create psychological distress. There are no guarantees that an on-line stalker will not, at some stage, transition to stalking their victim(s) off-line. In addition, the harm caused by cyber-smearing (e.g. placing false information about an individual on the Internet) may be greater than harm caused off-line due to the persistence of records on-line and the increased potential audience (Bocij & McFarlane 2003b).

The Internet presents a 'double-edged sword' for stalking victims (Spence-Diehl, 2003). While information and communication technologies provide tools for stalkers to use in stalking their victims, they can also provide the means of information, communication and support for victims and helping professionals. On-line organisations such as WHO@ (Working to Halt Online Abuse: www.haltabuse.org) and Cyberangels (http://www.cyberangels.org/) provide advice and support to cyber-stalking victims.

Working from a feminist perspective, Adam (2002) recommends victims 'reappropriate the gaze' by investigating and tracking their cyber-stalkers online, with the aim of stripping their anonymity. From a different perspective, Bocij (2005) has argued that victims of cyber-stalking may in turn victimize others, and become 'reactive stalkers' themselves. Further research is clearly required into the consequences of stalking victims attempting to take matters into their own hands rather than relying on legal and professional help.

Legislation and criminal investigation

Laws criminalising cyber-stalking provide a form of protection and method of address for victims. Downing (2005) provided three general principles for drafting cyber-crime laws that are of direct relevance to cyber-stalking. First, there needs to be consistency in legislation between cyber and off-line behaviours, so that conduct is criminalized uniformly whether or not the conduct is facilitated by a computer network. Second, laws should be drafted without reference to any specific technology to ensure they do not become quickly outdated. Third, laws need to enable prosecution of offenders across jurisdictions.

The introduction or amendment of legislation to cover cyber-stalking behaviours has been rapid in westernised countries. At the time of writing, forty four states in the US

had stalking and/or harassment legislation that was explicitly inclusive of electronic communication (see http://www.ncsl.org/programs/lis/cip/stalk99.htm). In Australia, some states have, or are in the process of, amending legislation to include cyber-stalking (see, for example, the *Crimes (Stalking) Act 2003* in Victoria). In the United Kingdom, cyber-stalking behaviours are being prosecuted under the *Protection from Harassment Act 1997* (see Seenan, 1999 for details of the first successfully prosecuted case). This rapid adoption of cyber-stalking legislation has led one researcher to comment that "cyber-stalking is well on its way to being criminalized before being empirically examined" (Spence-Diehl 2003: p. 6).

However, the amending of legislation to incorporate cyber-stalking behaviours is far from universal across the world. Cyber-stalking may still be regarded in many jurisdictions as constituting a 'social harm' rather than a criminal offence (Joseph, 2003). Even where legislation exists, it may be problematic to successfully prosecute cyber-stalking as it is difficult to establish a 'credible threat' if a direct threat has not been made or if the stalker and victim live in different jurisdictions. Similarly, Meloy (1998) argued that cyber-stalking alone is unlikely to be prosecuted, but that cyber-stalking in conjunction with other means of pursuit may be.

The criminal investigation of stalking/cyber-stalking poses problems for police as, unlike most crimes, stalking consists of repeated individual behaviours that individually may not constitute criminal offences. Other difficulties facing police are that stalking may be perceived by some as part of a relationship, there is no unique profile of stalkers and it is difficult to predict which stalkers will become violent. Further, police investigations may need to cover multiple jurisdictions. (National Centre for Victims of Crime 2004).

In order to convince authorities to investigate or prosecute cyber-stalking, the onus is often on the victim to produce evidence. Victims of cyber-stalking may find this easier to comply with than victims stalked off-line as electronic communication (e.g. chat room discussions) can be logged and threatening emails saved, providing a form of objective data (Deirmenjian 1999).

Difficulties in investigating cyber-stalking arise in identifying the stalker when they have taken steps to ensure the anonymity of their communications (Joseph, 2003). Cyber-stalkers frequently have greater technical ability than victims and law enforcement agents (Aggarwal Burmester Henry Kermes & Mulholland, 2005). Police may also have difficulty in obtaining information from Internet Service Providers. For example, D'Ovidio and Doyle (2003) noted that in 18% of New York Police Department cyber-stalking cases examined the police were unable to access required records in order to arrest the cyber-stalking suspect.

The need for both law enforcement staff and prosecutors to increase their technical ability and understanding of computer-related crimes has been recognised. In the US, specialized cyber-crime units have been established within or across government departments in addition to FBI computer crime squads. Computer crime prosecutors are employed within each US Attorney's office (Joseph 2003).

Computer solutions have been developed to aid in the investigation and prosecution of cyber-stalking. For example, the Predator and Prey Alert (PAPA) system, consisting of integrated software and hardware modules, can be utilized to capture, record and verify evidence for use in prosecution. It consists of a sessional recorder, a victim module, an agent module and a dispatcher. The system operates by capturing information received by the victim. This can be supplemented by the law enforcement agent remotely

shadowing ongoing interactions with the investigator able to take control of the victim's desktop if required (Aggarwal et al 2005; Aggarwal Henry, Kermes & Mulholland, 2005).

Not all cyber-stalking involves perpetrators and victims from the same jurisdiction. Where victims and perpetrators are located in different jurisdictions investigation and prosecution may be hampered by differences in statutory definitions of stalking. Some jurisdictions may deny or ignore extradition requests (D'Ovidio & Doyle 2003).

There is a lack of clarity over what constitutes jurisdiction in cyberspace. As Brenner and Koops (2004) ask: "is it the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attack? Or all of these at once?" (p. 3). Cyber-crime jurisdictional clauses differ significantly across states and countries. The 'reasonableness standard' suggests that the exercise of jurisdiction requires a close connection with the crime, but this leaves the potential for both negative and positive jurisdiction conflicts. Negative jurisdiction conflicts occur when no jurisdiction claims jurisdiction over a cyber-crime. Positive jurisdiction conflicts occur when more than one jurisdiction claims jurisdiction over the one cyber-crime. While the reasonableness standard dictates the jurisdiction with the closest connection to the crime has priority in prosecuting, it may be difficult to determine who has precedence of jurisdictional claims (Brenner & Koops 2004).

Jurisdictional issues in relation to cyber-stalking are being tested in the courts. An Australian example (cited in Smith Grabosky & Urbas, 2004:52) detailed how a Victorian Magistrate initially dismissed the case of a Melbourne resident who stalked a Canadian actress on the grounds of lack of jurisdiction (based on the harm occurring in Canada rather than Melbourne). At appeal by the Director of Public Prosecution, the Supreme Court determined that although the harm occurred outside of Australia, the criminal conduct was committed within Victoria and the case was therefore within jurisdiction.
While jurisdictional issues result in difficulties in investigating and prosecuting cyber-stalking, these problems are not specific to cyber-stalking but occur with other types of cyber-crime and cross-border crime (D'Ovidio & Doyle 2003; Smith Grabosky & Urbas, 2004).

Conclusion and Future Directions

This paper has presented an overview of cyber-stalking as a form of stalking that takes advantage of the affordances of the electronic environment. There is a need to extend the boundaries of our perceptions of stalking to include current conceptions of cyber-stalking and future methods of stalking that may arise as the proliferation of new information and communication technologies continues. This inclusive approach demands research into the dynamics between on- and off-line stalking and into the prevalence, incidence, duration and effects of stalking conducted within electronic environments.

Cyber-stalking is an interpersonal crime that challenges notions of the requirement for physical proximity for harm to occur. Effective law enforcement and legal responses to cyber-stalking are dependent firstly upon the formulation of laws that recognise both the harms that can result from cyber-stalking and the cross-jurisdictional nature of the crime. These laws need to be supported through co-operation between jurisdictions and the continued training of law enforcement and legal officers to increase their technological sophistication and understanding of cyber-stalking behaviours.

References

Adam, A. (2002). Cyberstalking and Internet pornography: Gender and the gaze. *Ethics and Information Technology, 4*, 133-142.

Aggarwal, S., Burmester, M., Henry, P., Kermes, L., & Mulholland, J. (2005). Anti-Cyberstalking: The Predator and Prey Alert (PAPA) System. *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, (SADFE '05)*, 195-205.

Aggarwal, S., Henry, P., Kermes, L., & Mulholland, J. (2005). Evidence handling in proactive cyberstalking investigations: the PAPA approach. *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, (SADFE '05)*, 165- 176.

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention , 5*(3), 279-289.

Australian Bureau of Statistics. (2006). *Personal Safety Survey Australia: 2005 (Reissue).* Canberra: Commonwealth of Australia.

Bahm, T (2003). Eliminating "cyber-confusion". *Stalking Resource Centre Newsletter, 3*(2), 2. Retrieved April 15, 2007 from http://www.ncvc.org/src/AGP.Net/Components/DocumentViewer/Download.aspx nz?DocumentID=33500

Bocij, P. (2003a). Corporate cyberstalking: An invitation to build theory. *First Monday,* 7(11). Retrieved April 15, 2007 from http://firstmonday.org/issues/issue7_11/bocij/index.html.

Bocij, P. (2003b). Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. *First Monday, 8*(10). Retrieved April 15, 2007 from http://firstmonday.org/issues/issue8_10/bocij/index.html

Bocij, P. (2005). Reactive stalking: A new perspective on victimisation. *The British Journal of Forensic Practice,* 7, 23-34.

Bocij, P., Bocij, H. & McFarlane, L. (2003). Cyberstalking: A case study of serial harassment in the UK. *The British Journal f Forensic Practice, 5*(2), 25-32.

Bocij, P. & McFarlane, L. (2003a). Cyberstalking: The technology of hate. *The Police Journal, 76*, 204-221.

Bocij, P. & McFarlane, L. (2003b). Seven fallacies about cyberstalking. *Prison Service Journal, 149*, 37-42.

Bocij, P. & Sutton, M. (2004). Victims of cyberstalking: Piloting a web-based survey method and examining tentative findings. *Journal of Society and Information, 1*(2). Retrieved April 15, 2007 from http://josi.spaceless.com/.

Brenner, S W., & Koops, B-J. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law, 15*(1), 1-46.

Casey, E. (2004*). Digital evidence and computer crime: Forensic science, computers and the Internet* (2nd ed). London: Elsevier Academic Press.

Cornwell, B., & Lundgren, D. C. (2001). Love on the Internet: Involvement and misrepresentation in romantic relationships in cyberspace vs. realspace. *Computers in Human Behavior, 17*, 197-211.

D'Ovidio, R. & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin, 72*(3), 10-17.

Deirmenjian, J. M. (1999). Stalking in cyberspace. *Journal of American Academy of Psychiatry and Law, 27*(3), 407-413.

Dennison, S. M., & Thomson, D. M. (2005). Criticisms or plaudits for stalking laws? What psycholegal research tells us about proscribing stalking. *Psychology, Public Policy & Law, 11*(3), 384-406.

Downing, R. W. (2005). Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime. *Columbia Journal of Transnational Law, 43*, 705- 762

Dressing, H., Kuehner, C., & Gass, P. (2005). Lifetime prevalence and impact of stalking in a European population. *British Journal of Psychiatry, 187*, 168-172.

Finch, E. (2001). *The criminalization of stalking: Constructing the problem and evaluating the solution*. London: Cavendish.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468-483.

Finn, J., & Banach, M. (2000). Victimization online: The down side of seeking human services for women on the Internet. *CyberPsychology & Behavior, 3*(2), 243-254.

Finney, A. (2006) *Domestic violence, sexual assault and stalking: Findings from the 2004/05 British Crime Survey*. Home Office Online Report 12/06. London: Home Office. Retrieved April 15, 2007 from http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr1206.pdf

Fisher, B. S., Cullen, F. T., & Turner, M. G. (2000). *The sexual victimization of college women*. National Institute of Justice and Bureau of Justice Statistics Research Report: NCJ 182369. Retrieved April 15, 2007 from http://www.ncjrs.gov/pdffiles1/nij/182369.pdf

Jerin, R., & Dolinsky, B. (2001). You've got mail! You don't want it: Cyber-victimization and on-line dating. *Journal of Criminal Justice and Popular Culture*, 9(1). Retrieved April 15, 2007 from http://www.albany.edu/scj/jcjpc/vol9is1/jerin.html

Joseph, J. (2003). Cyberstalking: An international perspective. In J Yewkes (Ed.), *Dot.cons: Crime, deviance and identity on the Internet* (pp. 105-125). Cullompton: Willan.

Kamphius, J. H., & Emmelkamp, P. M. G. (2000). Stalking — a contemporary challenge for forensic and clinical psychiatry. *British Journal of Psychiatry, 176*, 206-209.

Kamphius, J. H., Emmelkamp, P. M. G., & Bartak, A. (2003). Individual differences in post-traumatic stress following post-intimate stalking: Stalking severity and psychosocial variables. *British Journal of Clinical Psychology, 42*, 145-156.

Lucks, B. D. (2004). *Cyberstalking: Identifying and examining electronic crime in cyberspace*. Unpublished doctoral dissertation, Alliant International University, San Diego, CA.

McEwan, T., Mullen, P. E., & Purcell, R. (2007). Identifying risk factors in stalking: A review of current research. *International Journal of Law and Psychiatry, 30*, 1-9.

McFarlane, L. & Bocij, P. (2003). An Exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday, 8-9*. Retrieved April 15, 2007 from http://www.firstmonday.org/issues/issue8_9/mcfarlane/index.html

McGrath, M. G., & Casey, E. (2002). Forensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace. *Journal of the American Academy of Psychiatry and the Law, 30(1),* 81-94.

McKenna, K. Y. A., Green, A. S., & Gleason, M. E. J. (2002). Relationship formation on the Internet: What's the big attraction? *Journal of Social Issues, 58*(1), 9-31.

Meloy, J. R. (1998). The psychology of stalking. In J. R. Meloy (Ed.) *The Psychology of Stalking: Clinical and Forensic Perspectives* (pp.1-23). San Diego: Academic Press.

Meloy, J. R. (2007). Stalking: The state of the science. *Criminal Behaviour & Mental Health, 17*, 1-7.

Mohandie, K., Meloy, R., McGowan, M. G., & Williams, J. (2006). The RECON typology of stalking: Reliability and validity based upon a large sample of North American stalkers. *Journal of Forensic Sciences, 51*, 147-155.

Mullen, P., Pathe, M., & Purcell. R. (2000). Stalkers and their victims. Cambridge: Cambridge University Press.

Mullen, P.E., & Pathe, M. (2002). Stalking. In M. Tonry (Ed), *Crime and Justice: A Review of Research, Volume 29* (pp.273-318). Chicago: University of Chicago Press.

National Centre for Victims of Crime (2004). *Stalking. Problem-oriented guides for police problem-specific guides Series No 22*. US Department of Justice. Retrieved April 15, 2007 from http://www.cops.usdoj.gov/mime/open.pdf?Item=1042.

Ogilvie, E. (2000). Cyberstalking. *Trends & Issues in Crime and Criminal Justice, No 166*. Canberra: Australian Institute of Criminology.

Parks, M. R., & Floyd, K. (1996). Making friends in cyberspace. *Journal of Communication, 46*, 80-97.

Parks, M. R., & Roberts, L. D. (1998). 'Making MOOsic': The development of personal relationships on-line and a comparison to their off-line counterparts. *Journal of Social & Personal Relationships, 15,* 517-537.

Pittaro, M. L. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, *1*(2), 180–197. Retrieved September 1, 2008, from http://ccrimejournal.brinkster.net/pittaroijccvol1is2.htm

Purcell, R., Pathe, M., & Mullen, P. E. (2002). The prevalence and nature of stalking in the Australian community. *Australian and New Zealand Journal of Psychiatry, 36*, 114-120.

Purcell, R., Pathe, M., & Mullen, P. E. (2004a). Editorial: When do repeated intrusions become stalking? *The Journal of Forensic Psychiatry & Psychology, 15*(4), 571-583.

Purcell, R., Pathe, M., & Mullen, P. E. (2004b). Stalking: Defining and prosecuting a new category of offending. *International Journal of Law and Psychiatry, 27*, 157-169.

Purcell, R., Pathe, M., & Mullen, P. E. (2005). Association between stalking victimization and psychiatric morbidity in a random community sample. *British Journal of Psychiatry, 187*, 416-420.

Roberts, L. D., Smith, L. M., & Pollock, C. M. (2006). Psychological sense of community in virtual communities. In S. Dasgupta (Ed.). *Encyclopedia of Virtual Communities and Technologies* (pp. 390-396). Hershey, PA: Idea Group Inc.

Seenan, G. (1999, October 16). Three months' jail for internet stalker. *The Guardian* (p. 9).

Sheridan, L. & Davies, G. (2004). Stalking and harassment. In J. R. Adler (Ed.), *Forensic Psychology: Concepts, debates and practice* (pp. 197-211). Cullompton: Willan.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.

Spence-Diehl, E. (2003). Stalking and technology: The double-edged sword. *Journal of Technology in Human Services, 22*(1), 5-18.

Spitzberg, B. H. (2006). Preliminary development of a model and measure of computer-mediated communication (CMC) competence. *Journal of Computer-Mediated Communication, 11*, 629-666.

Spitzberg, B. H., & Cupach, W. R. (forthcoming 2007). Cyber-stalking as (mis)matchmaking. In M. T. Whitty, A. Baker, & J. Inman (Eds.). *Online matchmaking* (pp. 127-146). Basingstoke: Palgrave Macmillan.

Spitzberg, B. H., & Cupach, W. R. (2007). The state of the art of stalking: Taking stock of the emerging literature. *Aggression and Violent Behavior, 12*, 64-86.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71-92.

Tavani, H. T. (2002). The uniqueness debate in computer ethics: What exactly is at issues, and why does it matter? *Ethics and Information Technology, 4*, 37-54.

Tavani, H. T. (2005). Search engines, personal information and the problem of privacy in public. *International Review of Information Ethics, 3*, 39-45.

Tavani, H. T., & Grodzinsky, F. S. (2002). Cyberstalking, personal privacy, and moral responsibility. *Ethics and Information Technology, 4*, 123-132.

Whitty, M. T. (2002). Liar, liar! An examination of how open, supportive and honest people are in chat rooms. *Computers in Human Behavior, 18*, 343-352.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2002). Close online relationships in a national sample of adolescents. *Adolescence, 37*(47), 441-455.