Cyberstalking: A New Challenge for Criminal Law

Paul Bocij, Mark Griffiths and Leroy McFarlane

Cyberstalking has recently emerged as a new and growing problem and is an area that will probably receive a higher profile within criminal law as more cases reach court (see Griffiths, 1999; Griffiths, Rogers and Sparrow, 1998; Bojic and McFarlane, 2002a; 2002b). For the purposes of this article we define cyberstalking as the use of information and communications technology (in particular the Internet) in order to harass individuals. Such harassment may include actions such as the transmission of offensive e-mail messages, identity theft and damage to data or equipment. Whilst a more comprehensive definition has been presented elsewhere (Bocij and McFarlane, 2002), it is hoped that the definition here is sufficient for those unfamiliar with this field.

The stereotypical stalker conjures up images of someone harassing a victim who is the object of their affection. However, not all stalking incidents are motivated by unrequited love. Stalking can also be motivated by hate, a need for revenge, a need for power and/or racism. Similarly, cyberstalking can involve acts that begin with the issuing of threats and end in physical assault. We also make distinctions between conventional stalking and cyberstalking. Whilst some may view cyberstalking as an extension of conventional stalking, we believe cyberstalking should be regarded as an entirely new form of deviant behaviour.

It is not surprising that cyberstalking is sometimes thought of as a trivial problem. A number of writers and researchers have suggested that cyberstalking and associated activities are of little genuine concern. Koch (2000), for example, goes as far as accusing those interested in cyberstalking as promoting hysteria over a problem that may be minuscule or even imaginary. The impression gained is that cyberstalking represents a relatively small problem where victims seldom suffer any real harm. Whilst there are no genuinely reliable statistics that can be used to determine how common cyberstalking incidents are, a great deal of evidence is available to show that cyberstalking is a significant and growing problem (Griffiths *et al,* 1998). For instance, CyberAngels (a well-known Internet safety organization) receives some 500 complaints of cyberstalking each day, of which up to 100 represent legitimate cases (Dean, 2000). Another Internet safety organization (Working to Halt Online Abuse) reports receiving an average of 100 cases per week (WHOA, 2001).

To highlight the types of cyberstalking behaviours that take place and some of the major issues facing criminal law, we briefly examine four high profile cases of cyberstalking (adapted from Bocij and MacFarlane, 2002b).

Case Study 1: Amy Boyer

Amy Boyer was a 20-year-old student in her final year of a dental hygiene course. Amy was widely regarded as a well-liked and highly motivated young lady, as evidenced by the fact that she was supporting her studies by working two part-time jobs. In October 1999, Liam Youens committed suicide shortly after he had shot 20-year-old Amy Boyer as she left work. While investigating the murder a number of disturbing facts emerged. Youens had (i) unbeknown to Amy, been following her movements for more than four years, (ii) obtained confidential information about Amy from various Internet services including her Social Security number and her work address, (iii) kept a diary detailing his long obsession about Amy on his web site and how he had been watching her for years, and (iv) outlined his plan to murder Amy on

his web site. The written detailed plan was carried out exactly as described.

Case Study 2: Kerry Kujawa

Kerry Kujawa, a male student at Texas A&M University, was found murdered after family and friends had filed a missing person's report. Subsequent investigation found that Kujawa had developed a relationship with a young woman named 'Kelly McCauley' on the Internet. However, 'McCauley' was in fact a 31-year-old male called Kenny Wayne Lockwood. Kujawa eventually arranged to meet 'McCauley' at a face-to-face meeting (April 7, 2000). The investigation found that the murderer Lockwood had invented the personality of 'Kelly McCauley' as a way to meet with young men. To 'entice' young men, Lockwood pretended he was a woman in a destructive relationship and needed someone to help her. To add to the deception, Lockwood sent photographs of an attractive young woman to his potential victims. Lockwood met Kujawa at the agreed time and place but then pretended to be McCauley's brother in order to allay suspicions. He later killed him and then pretended that Kujawa was still alive by posting Internet messages pretending to be Kujawa.

Case Study 3: The Boehle family

The US-based Boehle family underwent a campaign of harassment that lasted for two-and-a-half years. The family began to receive late-night telephone calls from different men asking to speak to their 9-year-old daughter. They contacted the police who simply advised them to change their telephone number and keep their daughter inside the house. Dissatisfied with the police, the child's father, decided to investigate further and suspected the calls were being organised by a neighbour with whom he had argued on several occasions. Eventually, he found out that his neighbour had been using the Internet to post messages about his daughter. The neighbour made it appear that the daughter was soliciting sex from strangers by including the family telephone number. The neighbour had begun a campaign of harassment because of some trivial incidents (eg, the daughter had chalked the word 'hello' near the neighbour's drive). Following his arrest, the neighbour was convicted of transmitting obscene material. This was treated as a misdemeanour and he received a $750 fine.

Case Study 4: John Robinson

Serial killer John Robinson was tried in June 2000 for the murder of five women he was alleged to have contacted via the Internet, hiding the dead bodies in barrels in his garden. Using the alias of 'Slavemaster', Robinson contacted women who might be willing to act as "sex slaves" for him. The women were encouraged to meet Robinson through various inducements (eg, promises of a well-paid job). The notion that a serial killer may have operated via the Internet is, understandably, one that has resulted in a great deal of public anxiety.

Implications for the Legal Profession

These four case studies highlight many important issues where cyberstalking occurs. The Internet allows many activities to be made with almost perfect anonymity (eg, inquiries about confidential information, e-mail postings using aliases or other identities). These activities require very little effort and can be done without the person having to leave their home or workplace. It is unlikely that without such anonymity, that the protagonists would have engaged in their behaviour offline.

John Robinson's case also demonstrates the relative ease with which the Internet can be used to locate victims. Robinson was 56 years old and not considered attractive. His case demonstrates the ease with which an individual can construct a new, more attractive identity in order to entice potential victims. Similarly, the case of Kerry Kujawa demonstrates how easy it is for an individual to mask their identity to pursue a victim. Kujawa's murderer clearly invested time and effort in constructing the 'Kelly McCauley' identity, even going as far as inventing a 'history' that he felt would be attractive to the young males he was pursuing as potential victims. Such incidents of new Internet identities may not be as isolated as they may first seem. In the UK, for example, the first case involving a man who assumed a false identity in order to stalk a young girl was heard in October 2000 (Vickers, 2000). In this case, Patrick Green, a 33-year-old man from Buckinghamshire, used the identity of a 15-year-old boy in order to meet young girls in chat rooms. After developing a relationship with a victim, Green would arrange to meet her so that he could entice her back to his home for sex.

The Boehle case highlights how little provocation was needed in order for the neighbour to organise a prolonged campaign of harassment. It also demonstrates the relative ease with which Internet messages were able to be posted on behalf of the child. There also appeared to be a lack of concern shown by the police to the family's distress. This may have been due to a lack of understanding concerning computer-related crime but this should not be seen as an excuse. It also appears that the neighbour's punishment of a fine was not particularly severe and is unlikely to deter others from pursuing a similar course of action. Finally, the fear felt by the family should not be underestimated. Deborah Boehle, the child's mother, said in a subsequent media interview that "Even though he never touched my daughter… he literally led millions of paedophiles to her."

Conclusions

Unfortunately, the term "cyberstalking" carries a number of unspoken assumptions that sometimes work against the interests of victims, researchers and other interested parties. To begin with, the term implies that this form of behaviour takes place entirely online, within the virtual world of the Internet. However, all too often, the behaviour spills over into offline reality. The fear that a victim feels is real and may persist long after the computer is switched off. Similarly, if an individual chooses to pursue his victim in real life, the consequences can come to haunt an entire family for a lifetime.

This article has presented a number of examples that demonstrate some of the different ways in which victims suffer genuine and significant harm. Each of the examples cited are genuine, and show how this form of harassment causes victims a great deal of genuine anxiety and fear. In other cases, it has been shown that cyberstalking may

eventually result in a violent attack against a victim or even murder.

Finally, all of the cases described within this article contain an implicit assumption that cyberstalkers are individuals. However, there is some evidence to suggest that harassment carried out via the Internet sometimes involves small groups of people working together and sometimes involves business organizations. The case of Jayne Hitchcock provides a good example of what has come to be termed "corporate cyberstalking". Hitchcock's experience is well documented, having been featured heavily in the media. Hitchcock's case concerns her allegation that she has been harassed by the Woodside Literary Agency since 1996. Since the case is ongoing and is the subject of a legal action, it is considered inappropriate to comment further. However, it should be noted that the allegations made against the literary agency involve many of the activities commonly associated with cyberstalking, such as identity theft and various forms of information warfare (such as e-mail bombing).

At present, there are many problems concerning the concept of cyberstalking within the criminal law system. For instance:

- Some legislation does not set out in detail what is meant by harassment. Instead, harassment is defined in terms of how a reasonable person might construe a given course of action.
- Much of the legislation adopted within the United States requires that the harassment must be carried out with the intention of causing the victim to feel fear or distress. However, it is possible for harassment to occur without this intention being present. In addition, the threat of physical violence may be of less relevance to victims of cyberstalking than other actions, such as threats to humiliate or embarrass a victim.
- Some US legislation defines harassment in terms of "unconsented contact". With regard to cyberstalking, the notion that victims must protest against the way they are being treated is unreasonable since it may not be possible for them to contact the harasser.
- No current legislation allows for the possibility that harassment perpetrated via the Internet may involve small groups of people or business organizations.
- Existing definitions fail to deal with many of the activities associated with cyberstalking, such as real-time monitoring.
- Existing definitions of cyberstalking tend to be derived from definitions of physical stalking. As a result, there is a lack of emphasis on behaviours that are of more importance to victims of cyberstalking.
- Some definitions of stalking suggest that a threshold should be set on the number of incidents that must occur before a certain course of behaviour is treated as stalking. Such thresholds are of little relevance to cyberstalking.
- All legal definitions assume that the victims of stalking are individuals. There is evidence to suggest that cyberstalking sometimes involves small groups of people, such as individual families.

With all of these issues in mind, we offer a formal definition of cyberstalking for discussion and examination. Cyberstalking therefore constitutes a group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology to harass one or more individuals. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, the solicitation of minors for sexual purposes and confrontation. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress.

We end by re-iterating that cyberstalking is a growing problem that transcends international boundaries. Whilst not quite the "epidemic" described by the media, the problem is a significant one that requires further study and discussion by all those in the criminal law system. The victims of cyberstalking incidents should not be ignored and the harm suffered by these individuals must not be trivialized.

References

Paul Bocij and Mark Griffiths are lecturers at Nottingham Trent University;
Leroy McFarlane is ….…. at HMP Nottingham.