



PEER-REVIEWED JOURNAL ON THE INTERNET

Corporate Cyberstalking: An Invitation to Build Theory

by Paul Bocij

Abstract

Corporate Cyberstalking: An Invitation to Build Theory by Paul Bocij

Cyberstalking describes a relatively new form of stalking behaviour where technology is used as the medium of harassment. The term corporate cyberstalking is often used to describe incidents that involve organisations, such as companies and government departments. This paper uses a number of case studies in order to propose a typology of corporate cyberstalking. It is suggested that incidents involving corporate cyberstalking can be divided into two broad groups, depending on whether or not the organisation acts as a stalker or as a victim. Examining the motivations behind corporate cyberstalking allows these groups to be subdivided further. The motives behind corporate cyberstalking can range from a desire for revenge against an employer to cyberterrorism. The paper also briefly discusses definitions of stalking and cyberstalking, concluding with a revised definition of cyberstalking that is more in keeping with the material discussed.

Contents

[Introduction](#)

[What Is Corporate Cyberstalking?](#)

[Categories of Corporate Cyberstalking](#)

[Conclusion](#)

Introduction

Most people are familiar with the concept of stalking thanks to a small number of high profile cases involving celebrities, such as Madonna and Rebecca Schaeffer (Fremouw et al., 1997). Cyberstalking, however, is a relatively new term that has been coined to describe a new form of stalking behaviour where technology is used as the medium of harassment. Comparatively little is known about cyberstalking although some countries are beginning to recognise that it is a growing and serious problem. For instance, *Stalking and Harassment*, one of a series of Research Notes published on behalf of The Scottish Parliament in August 2000, stated: "Stalking, including cyberstalking, is a much bigger problem... than previously assumed and should be treated as a major criminal justice problem and public health concern."

We can distinguish between stalking and cyberstalking by taking a brief look at how each is defined. Two of the best-known definitions of stalking are offered by Meloy and Mullen et al. Meloy [1] describes stalking in terms of obsessional following, defining it as "... an abnormal or long term pattern of threat or harassment directed toward a specific individual." He goes on to define a pattern of harassment as "... more than one overt act of unwanted pursuit of the victim that was perceived by the victim as being harassing." Although Mullen, Pathé and Purcell [2] support Meloy's definition, they also offer their own: "... a constellation of behaviours in which one individual inflicts on another repeated unwanted intrusions and communications." Intrusions are characterised as "... following, loitering nearby, maintaining surveillance and making approaches."

Although some view cyberstalking as nothing more than a variation on conventional stalking, others have argued that cyberstalking should be seen as an entirely new phenomenon (for example, Ogilvie, 2000). This view is supported by two main arguments. Firstly, it can be argued that advances in technology bring new opportunities for crime and other forms of deviant behaviour (for example, Smith 1998). This seems reasonable with regard to cyberstalking since it is clear that this kind of stalking relies on the availability of services and technologies that simply did not exist a few decades ago. Secondly, the behaviours associated with cyberstalking tend to be different to those associated with conventional stalking. For instance, a report from the U.S. Attorney General to the Vice President entitled *Cyberstalking: A New Challenge for Law Enforcement and Industry* lists a number of significant differences between cyberstalking and what the report calls "offline stalking".

Some of these differences are highlighted within a definition of cyberstalking offered by Bocij and McFarlane (2002):

"A group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology (ICT) 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."

As this definition shows, cyberstalking may sometimes involve harassment carried out by an organisation. Such behaviour is often termed corporate cyberstalking. This paper discusses the nature of corporate cyberstalking and puts forward three basic arguments for examination and discussion. Firstly, it is argued that corporate cyberstalking can involve organisations as both the perpetrators and the victims of harassment. Secondly, it is suggested that it is possible to identify specific types of corporate cyberstalking. It is possible to distinguish specific categories of corporate cyberstalking by examining factors such as the motivation behind the harassment. Finally, the motivations behind corporate cyberstalking incidents can be very different to those commonly associated with offline stalking and cyberstalking. For instance, many corporate cyberstalking incidents involve attempts to gain some form of financial benefit.



What Is Corporate Cyberstalking?

Many people associate corporate cyberstalking with the notion of a company - usually represented by a single employee or manager - setting out to harass an individual. Indeed, the first cyberstalking case to make international headlines was that of Jayne Hitchcock, a person who claims to have been stalked by the Woodside Literary Agency for several years (see, for example, Rock, 2000, for a brief description of this case). Since Hitchcock's case is well known and is described in some depth on her own Web site, it will not be discussed further here [3]. It is important to note, however, that this kind of incident normally involves a senior figure in the organisation making a conscious decision to divert company resources towards a campaign of harassment. What distinguishes this kind of stalking from other types of corporate cyberstalking is that the manager's actions are almost always based on personal reasons, such as a grudge against a former intimate.

Occasionally, an organisation may be an unwitting accomplice to a cyberstalker rather than an active and willing participant. There have been numerous cases, for example, where employees have used company e-mail facilities to harass other members of staff. In one case, for instance, a network administrator was dismissed for harassing a clerk. Undeterred, the administrator broke into the company's systems and continued his campaign of harassment. In addition to sending embarrassing e-mail messages about the clerk around the firm, he stole sensitive company information and even gave the clerk a \$130,000 pay rise [4].

It is worth pointing out that the resources of charities, local authorities and other not-for-profit organisations are also open to abuse by some individuals. For instance, it is alleged that a research student at Glasgow University abused Internet and e-mail facilities when he began to correspond with paedophiles [5].

It is also worth pointing out that organisations may sometimes hold some of the responsibility for incidents where company resources are directed towards harassing others. This is because it can be argued that organisations have a duty to ensure that resources are used appropriately. Even when legislation does not impose such a duty, it seems difficult to claim that companies have no professional or moral responsibility to protect the public. Of course, there are also very sound business reasons to ensure that organisational resources are not abused in the ways described here.

It can be argued that some organisations use cyberstalking as a way of controlling some of the information posted to the Internet. As an example, recent years have seen many companies use SLAPPs (Strategic Lawsuits Against Public Participation) to prevent individuals from publishing various kinds of information on the Internet, such as complaints. The Civil Liberties Monitoring Project suggests that SLAPPs can be used "... to intimidate activists into silence by filing meritless lawsuits against them ... for such torts as slander or intentional interference with business advantage" (Kirk, 1998). Some well-known cases regarding SLAPPs include the Electronic Frontier Foundation (EFF) and its support of a parody concerning a favourite children's character named Barney™ [6], Carla Virga and Terminix [7], and some of the numerous disputes concerning Scientology [8].

Although the use of SLAPPs is perfectly legal in many countries, there may be circumstances where their use exposes an organisation to civil or criminal legal action. For instance, many companies "follow" their critics around the Internet, keeping a close watch on Web sites, bulletin boards and chat rooms for any material that criticises the company. Sometimes, especially in the case of Web sites, a company may wish to act against a particularly vocal critic and an unusual cat-and-mouse situation may arise. In such a scenario, an individual establishes a Web site containing criticisms of a company. When the company becomes aware of the site, a complaint or legal threat is made to the service provider so that the critic's site is taken down. The owner is then forced to move to another service provider and the cycle begins again. If the complaints made to service providers are unfounded, the company might face civil action (e.g. for libel) or even criminal charges (e.g. harassment). The Geocities case study given later provides a good example of the kind of cat-and-mouse game described here.

Each of the examples given so far has described an incident where an organisation has become involved in harassing an individual. There are, however, many occasions where an organisation can become a victim of harassment.

A typical example of this type of corporate cyberstalking will usually involve one or more individuals targeting a specific company for financial gain or in order to exact revenge against a former employer. Often, these cases involve individuals posting false or defamatory information to various sites on the Internet, such as chat rooms. This is sometimes known as "bashing" or "cyber-smearing" (Smith, 2000). This kind of behaviour can be directly compared to a type of offline stalker known as the resentful stalker. According to Mullen, Pathé and Purcell [9], the behaviour of such people involves "... esponding to a perceived insult or injury by actions aimed not just at revenge but at vindication." In outlining a typology of cyberstalkers, McFarlane and Bocij (in press) propose a category known as the "vengeful stalker" which is similar to the resentful stalker described by Mullen, Pathé and Purcell.

Cyber-smearing is a serious matter since the damage caused is often more serious than if the information were contained in a letter or even a newspaper article. In the former case, the potential audience to the information is very limited. In the latter, a retraction can be printed quickly and easily. It is argued that it is almost impossible to retract a message posted to a chat room or discussion board. Usually, the information contained within the message becomes persistent, meaning that it remains easily accessible for the foreseeable future, increasing the harm done to the company over time. It is also worth noting that the potential audience for a message posted on the Internet is far larger than the circulation of any newspaper in the world.

False or defamatory information is often posted to financial chat rooms and message boards in order to perpetrate online stock fraud. The most common method, known as "pump and dump", usually involves the perpetrator buying large quantities of a given company's stock. The fraudster then artificially increases the value of a company's stock by posting rumours such as "news" of a potential take-over. As soon as the value of the stock rises, the fraudster sells his shares at a large profit. Occasionally, a fraudster may artificially decrease the value of a stock so that shares can be bought at a bargain price, to be resold once the stock recovers.

The harm caused by this form of cyberstalking must not be underestimated. As explained earlier, the damage caused to an organisation's public image is often severe and long-lasting. However, the financial losses that accompany online stock fraud can sometimes harm an entire industry, let alone an individual company. For instance, in August 2000, Mark Jakob, a 23-year-old former student, released a body of false information concerning Emulex. Within an hour the company's stock had fallen in value by \$2.5 billion but Jakob had realised a personal profit of \$240,000 (Berenson, 2000). Fearful that Emulex indicated a problem within the sector, panicked investors began selling shares in other companies, causing shares in Brocade and Qlogic to fall in value too (Grice and Ard, 2000).

Occasionally, an organisation may use cyberstalking as a competitive strategy. Lopez (1999), for example, describes a legal action started by Amway against Procter & Gamble. In this case, it was alleged that Procter & Gamble had sponsored a Web site that encouraged complaints against Amway. According to Lopez, it is alleged that the site featured negative news stories, personal testimonials and even confidential documents belonging to Amway. Such behaviour is directly comparable to behaviour termed "stalking by proxy", where a stalker recruits other people, whether witting or unwitting, to assist in his activities [10].

Individuals may sometimes pursue an organisation in order to further a social or political goal. At one level, a person might use the Internet as a means of making a peaceful protest against a government's policy. At another, more direct action may be taken in order to force compliance from a company or government. For instance, Vatis (2001) provides several detailed examples of recent cyberterrorism incidents, including clashes involving India and Pakistan, Israel and the Palestinians, and NATO and Serbia in Kosovo.

Although most cyberterrorism is aimed at government agencies, it is worth remembering that businesses and non-commercial organisations may also make tempting targets for cyberterrorists. For instance, a company might be attacked because it has links to the defence industry. As an example, *Information Week* (17 September 2001) reports that AT&T and Lucent Technologies were threatened by pro-Palestinian hackers in November 2001. Public services, such as hospitals, are also vulnerable because of the wide scale disruption and public alarm that an attack might cause.



Categories of Corporate Cyberstalking

As suggested earlier, cases involving corporate cyberstalking can be divided into two broad categories: incidents where an organisation acts as a stalker and incidents where an organisation becomes a victim of stalking. It is also possible to group corporate cyberstalking incidents together by examining the motives behind the harassment. As discussed in the previous section, the motives behind corporate cyberstalking can range from a desire for revenge against an employer to cyberterrorism.

Keeping all of this in mind, it is now possible to propose a tentative typology of corporate cyberstalking. Such a typology is summarised by [Table 1](#).

Table 1: A proposed typology of corporate cyberstalking incidents

Stalker/Victim	Category Name	Description

Individual/Organisation	Vengeful	The individual wishes to exact some form of revenge against the organisation e.g. cyber-smearing.
Individual /Organisation	Individual Gain	The individual is seeking some form of benefit e.g. financial gain obtained via stock fraud.
Individual/Organisation	Ideological	The individual acts in support of beliefs e.g. cyberterrorism and hacktivism.
Organisation/Individual	Unwitting	The organisation is unaware of the actions of an employee and is an unknowing accomplice.
Organisation/Individual	For Profit	The organisation seeks to realise some form of (business) benefit by its actions, e.g. silencing critics using SLAPP. The victim is normally an individual.
Organisation/Individual	Competitive	The organisation seeks to improve its competitive position. The victim is another organisation.

The coloured part of the table represents categories of corporate cyberstalking where an organisation becomes a victim. Category names have been used as a simple way of identifying and describing a given category. These names also help to make clear the differences between categories.

A number of examples have already been provided in support of the points made by this paper. However, it is felt that some additional examples will help to clarify and illustrate each of the categories described within the proposed typology. The following six case studies have been selected to highlight the seriousness and diversity of corporate cyberstalking incidents.

Case 1: (Vengeful) Clancy Systems International

In September 2000, Clancy Systems International took the unusual step of commencing legal action against to discover the identities of some unknown individuals who were posting defamatory statements on various chat rooms, including the Raging Bull Message Board [11].

In November 2001, judgement was awarded against an individual who had been stalking the company via the Internet for two years. This individual was accused of a number of acts including: posting false statements, posting defamatory statements, making threats to company employees, making threats to other users of a chat room and hacking into the company's chat site in order to copy information which could be distorted and then posted to public chat sites [12].

In addition to awarding Clancy Systems International damages, the individual was permanently banned from posting messages to the Raging Bull Message Board or any other board that discusses the company.

Case 2: (Individual Gain) NEI Web World

In January 2001, Arash Aziz-Golshani and Hootan Melamed were both jailed for manipulating the stock of a printing company called NEI Web World (Hyman, 2001). Over a period of time, the duo purchased thousands of shares in the company at between 5 and 13 cents each. They then posted numerous messages to bulletin boards that exaggerated the value of the company. When the company's stock climbed to \$15 per share, they sold their holdings at a profit of \$350,000. However, as soon as it was realised that the rumours circulated by the pair were false, the shares immediately fell in value by 25 per cent, causing other investors to suffer losses [13].

Case 3: (Ideological) Electrohippies

In December 1999, a group called the Electrohippies organised what they described as a "virtual sit-in" at the World Trade Organisation's Web site (Cassel, 2000). It is estimated that more than 450,000 participants took part in a massive denial of service (DoS) attack that overloaded the WTO's Web site for hours at a time on a number of occasions [14].

The group's protest was organised via its Web site [15], where participants were given instructions on when, where and how to act. In addition to DoS attacks, the group also attacked the WTO's e-mail system. A message on the group's Web site stated "So far we've demonstrated that the WTO's public information system is not immune from public pressure. Now we move to their private information system - their email."

Whilst some have described the actions of the Electrohippies and similar groups as cyberterrorism, the term hacktivism has also been used. Hacktivism is often described as political activism carried out via the Internet or, more simply, as hacking in order to spread socially conscious messages (Kirby, 2002).

Case 4: (Unwitting) A Serial Cyberstalker

A detailed account of the following case study is provided by Bocij, Bocij and McFarlane (in press).

Mr. Smith harassed a number of women via e-mail and Internet chat rooms. Victims would be selected by searching the personal profiles that many people submit to various services, such as ICQ. Mr Smith appeared to select victims who were single and lived relatively close to him.

Mr. Smith adopted several distinct identities when communicating with his victims. These identities would be used to minimise the possibility of being caught once he began to conduct a sustained campaign of harassment against his victims. This harassment would take a number of different forms, including sending abusive e-mail messages, placing surveillance software on the victim's computer, following the victim and making threats that implied he would assault the victim in her own home.

Mr. Smith was eventually caught when he deviated from his usual pattern of behaviour and selected a married woman as a victim. The woman's husband was a consultant with expertise in computer security. This man was able to trace Mr. Smith's name, address and place of employment. It was found that Mr. Smith was a network administrator for a relatively large local company and had been using his employer's facilities in order to stalk his victims. This included:

- making use of company software packages, such as route planning software and a database containing a register of electors, to find personal information about victims;
- establishing numerous false e-mail accounts; and,
- intercepting e-mail messages meant for senior management, deleting them and then impersonating managers in replies.

Once notified of Mr. Smith's activities, senior management were quick to offer a guarantee that the matter would be dealt with. However, it does not appear that the police were informed of Mr. Smith's actions and he does not appear to have been dismissed from his post.

Case 5: (For Profit) Zeman and Geocities

A detailed account of Zeman's allegations concerning the behaviour of Geocities can be found at <http://www.angelfire.com/mo/geocensored>.

Mark Zeman alleges that Geocities, a free Web space provider, actively pursues those who criticise the company on their Web sites. His personal Web site states: "GeoCities has followed critics around the Web, tracked them down, threatened, and otherwise harassed them and their ISPs and Web hosts. GeoCities has in the past threatened legal action against those that dare host any critic."

Zeman's allegations against Geocities come in three separate parts. Firstly, he argues Geocities follows its critics around the Internet and issues legal threats against any ISP unwise enough to host a Web site containing criticisms of the company. Secondly, although no explicit accusation is made, Zeman appears to suggest that his Web site has been deliberately banned by several software packages that are used to filter Web content (sometimes known as censorware). Finally, Zeman claims to have received various legal threats from Geocities based around copyright infringement and trademark infringement. According to Zeman, all of these actions make it difficult for people to exercise the right to free speech because they are effectively being censored by Geocities.

Zeman claims that there are many Web sites that contain criticisms of other free Web space providers, but very few that criticise Geocities. This, he suggests, is evidence that shows Geocities has adopted a policy of (legal) harassment against its critics. He also claims that he is not the only one to have been censored by Geocities. His Web site lists a number of Web rings (groups of related Web sites) and individual Web sites devoted to those claimed to have been censored by Geocities.

Case 6: (Competitive) Microsoft and the Halloween papers

The Web site of the Open Source Initiative describes a series of documents produced by Microsoft employees that outline how the company planned to deal with competition from open source software, such as Linux (an operating system) and Mozilla (a Web browser) [16]. The first document was named "Halloween" because of the date it was leaked. Over a period of a year, six Halloween documents were leaked, each containing information that was embarrassing to Microsoft for one reason or another.

The first memorandum was produced by a Microsoft software engineer. This document suggested that Microsoft could deal with competition from open source software (OSS) by subverting common standards. The engineer, Vinod Valloppillil, stated in his report "By extending these protocols and developing new protocols, we can deny OSS projects entry into the market" (Ricciuti, 1998). The memo also stated that Microsoft's usual FUD tactic would be unlikely to work in the case of products like Linux. FUD stands for "fear, uncertainty and doubt".

The last of the Halloween documents dragged the highly respected Gartner group into the argument. According to the Open Source Initiative, Gartner published a series of five articles that criticised Linux and predicted that its popularity would decline once Windows 2000 became more established. The press

responded to these reports by publishing numerous articles suggesting that Linux was doomed to failure. However, Eric Raymond of the Open Source Initiative claims that there is evidence to show that Microsoft wrote and published the articles on Gartner's Web site.

If one accepts the allegations made by the Open Source Initiative, then Microsoft were responsible for harassing the developers of Linux and other open source software for more than a year.




Conclusion

The definition of cyberstalking - provided at the beginning of this paper - recognises that an organisation may sometimes harass one or more individuals. However, although it is felt that the majority of the definition described earlier remains valid, it is felt that a modification is needed to recognise the fact that an organisation can sometimes become the *victim* of cyberstalking. Some additional minor changes are also needed to make the definition a little easier to read. With this in mind, it is suggested that the definition should be amended as follows:

"A group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology to harass another individual, group of individuals or organisation. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, damage to data or equipment, identity theft, data theft, computer monitoring, the solicitation of minors for sexual purposes and any form of aggression. 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."

The recognition that organisations may sometimes become victims of cyberstalking allows us to place corporate cyberstalking incidents within two broad groups. These groups consist of incidents where an organisation acts as a stalker and incidents where an organisation becomes a victim of stalking. By examining some of the motivations that underlie corporate cyberstalking incidents, it is possible to subdivide these groups further. The typology proposed by this paper suggests that there can be a diverse range of motives behind corporate cyberstalking. Some of these motives operate at an individual level and can be very personal, for example a person may act upon a desire for revenge against a former employer. At the organisational level, motives tend to be impersonal and are motivated by a desire to achieve some form of business benefit, for example an organisation may use cyberstalking as a means of gaining a competitive edge against a rival.

The more serious examples given within this paper have shown that corporate cyberstalking may represent a serious threat to society. In addition to the harm suffered by individuals, we must also consider the wider danger posed by acts such as online stock fraud and cyberterrorism. It is hoped that the development of a typology of corporate cyberstalking will help to encourage discussion and stimulate further research. Such research is necessary if we are to develop effective responses to the different forms of cyberstalking behaviour described here. 

About the Author

Paul Bocij is a former university lecturer who now works as a professional writer and consultant. As a writer, he has produced or contributed to more than twenty books, including a number of academic texts. He is one of the authors of *Business Information Systems*, the U.K.'s best-selling IS textbook, and also helped to develop an accompanying Internet course that is now used across the U.K. In addition, he is also the author of numerous articles, magazine columns, academic papers, training guides and other materials related to information systems and information technology. He is an active researcher and his research interests are largely concerned with the impact of technology on society, with a particular emphasis on deviant forms of behaviour, such as harassment. At present, he is a doctoral student at Nottingham Trent University studying the impact of cyberstalking on victims. In his work as an independent consultant, he regularly advises individuals and organisations on a wide range of issues related to computer security. He has also been involved with several cases of cyberstalking and has helped a number of people to deal with harassment perpetrated via the Internet.

E-mail: mail@pbocij.demon.co.uk

Acknowledgments

The author acknowledges the intellectual property of others. All trademarks, patents and registered designs are acknowledged as being the property of their respective owners.

Notes

1. Meloy, 1998, pp. 2-3.
2. Mullen, Pathé, and Purcell, 2000, p. 7.

3. The case of Jayne Hitchcock is described in detail at her own Internet site at <http://members.tripod.com/~cyberstalked/index.html>.
4. Source: "Cyberstalking rears its head in the workplace," *MSNBC*, 24 April 2001.
5. Martin, 2001 and *The Scotsman* (10 September 2001).
6. The EFF's formal response to allegations made by the Lyons Partnership with regard to the use of the Barney character can be viewed at http://www.eff.org/Privacy/SLAPP/IP_SLAPP/20010706_eff_barney_response.html. Additional information regarding the dispute is also available at the site.
7. Virga's account of her experience with the company is contained within her protest site at <http://www.syix.com/emu/index.htm>.
8. A detailed account of incidents involving alleged harassment perpetrated by supporters of Scientology can be found at <http://www.factnet.org/briefing.htm#1>.
9. Mullen, Pathé and Purcell, 2000, pp. 76-77.
10. Mullen, Pathé and Purcell, 2000, p. 173.
11. Source: *Business Wire*, 1 November 2001.
12. *Ibid.*
13. *Ibid.*
14. *Ibid.*
15. Electrohippies maintain a Web site at <http://www.fraw.org.uk>.
16. The Open Source Initiative Web site is located at <http://www.opensource.org>.

References

- "Clancy Systems International, Inc. Gets Court Judgement Against Basher," *Business Wire* (1 November 2001), at <http://globalarchive.ft.com/globalarchive/article.html?id=011101010105&query=internet+stalking>.
- "Cyberstalking rears its head in the workplace," *MSNBC* (24 April 2001), at <http://zdnet.com.com/2100-11-529416.html@legacy=zdn>.
- "University investigates PhD student's Internet links with convicted paedophiles," *The Scotsman* (10 September 2001), at <http://globalarchive.ft.com/globalarchive/article.html?id=010910004151&query=internet+paedophile>.
- A. Berenson, 2000. "Investigators Arrest a Suspect in Stock Manipulation Case," *New York Times* (1 September), at <http://www.nytimes.com/library/financial/090100emulex-plunge.html>.
- P. Bocij, H. Bocij and L. McFarlane, in press. "Cyberstalking: a case study concerning serial harassment in the U.K."
- P. Bocij and L. McFarlane, 2002. "Online harassment: towards a definition of cyberstalking," *Prison Service Journal*, number 139 (February), HM Prison Service, London.
- D. Cassel, 2000. "Hacktivism in the Cyberstreets," *AlterNet.org*, at <http://www.alternet.org/story.html@StoryID=9223>.
- J. Fremouw, D. Westrup D and J. Pennypacker, 1997. "Stalking on Campus: The prevalence and strategies for coping with stalking," *Journal of Forensic Science*, volume 42, number 4, pp. 666-669.
- C. Grice and S. Ard, 2000. "Hoax briefly shaves \$2.5 billion off Emulex's market cap," *CNET News.com* (25 August), at <http://news.cnet.com/news/0-1004-200-2611957.html>.
- G. Hulme and M. Garvey, 2001. "Terror Attack Brings Renewed Emphasis On Security," *InformationWeek.com* (17 September), at <http://www.informationweek.com/story/IWK20010916S0013>.
- G. Hyman, 2001. "Two Beverly Hills Men Sentenced for Securities Fraud," *INT Media Group* (24 January), at http://siliconvalley.internet.com/news/article.php/5321_568551.
- C. Kirby, 2002. "Hacking With a Conscience Is a New Trend," *San Francisco Chronicle* (20 November), http://www.sfgate.com/cgi-bin/article.cgi@file=2Fchronicle_2Farchive_2F2000_2F11_2F20_2FBU121645.DTL.
- E. Kirk, 1998. "Slapped? Slapp Back," *Civil Liberties Monitoring Project Newsletter* (Spring), at <http://www.civilliberties.org/spring98slapp.html>.
- R. Lopez, 1999. "Corporate Strategies for Addressing Internet 'Complaint' Sites," Thelen Reid & Priest LLP (August), at http://www.constructionweblinks.com/Resources/Industry_Reports_Newsletters/August_1999/august_1999.html.

- L. Martin, 2001. "Inquiry into student's child sex research," *The Herald* (10 September), at <http://globalarchive.ft.com/globalarchive/article.html?id=010910007694&query=internet+paedophile>.
- L. McFarlane and P. Bocij, in press. "An exploration of predatory behaviour in cyberspace: towards a typology of cyberstalkers."
- J. Meloy, 1998. "The Psychology of Stalking," In: J. Meloy (editor). *The Psychology of Stalking: Clinical and Forensic Perspectives*. London: Academic Press.
- P. Mullen, M. Pathé and R. Purcell, 2000. *Stalkers and their victims*. Cambridge: Cambridge University Press.
- E. Ogilvie, 2000. "Cyberstalking," *Trends and Issues in Criminal Justice*, number 166 (September), Australian Institute of Criminology, at <http://www.aic.gov.au/publications/tandi/tandi166.html>.
- M. Ricciuti, 1998. "Memo angers open source advocates," *CNET News.com* (4 November), at <http://news.com.com/2100-1001-217522.html?legacy=cnet>.
- A. Rock, 2000. "Stalkers Online (Cyberstalking)," *Ladies Home Journal* (March), at http://www.findarticles.com/cf_0/m1127/3_117/59643364/p1/article.jhtml?term=internet+stalking.
- Scottish Parliament. Information Centre, 2000. "Stalking and Harassment," *Research Note*, RN 00-58 (10 August), at http://www.scottish.parliament.uk/whats_happening/research/pdf_res_notes/rn00-58.pdf.
- A. Smith, 2002. "Stock shenanigans: The cybersmear," *U.S. News & World Report* (28 August), at <http://www.usnews.com/usnews/nycu/tech/articles/000828/nycu/stocks.htm>.
- R. Smith, 1998. "Criminal exploitation of new technologies," *Trends and Issues in Criminal Justice*, number 93 (July), Australian Institute of Criminology, at <http://www.aic.gov.au/publications/tandi/tandi93.html>.
- U.S. Department of Justice, 1999. "Cyberstalking: A New Challenge for Law Enforcement and Industry," *A Report from the Attorney General to the Vice President* (August), at <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>.
- M.A. Vatis, 2001. "Cyber Attacks During The War On Terrorism: A Predictive Analysis," a report published by Institute For Security Technology Studies, Dartmouth College (22 September), at http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf.

Editorial history

Paper received 14 September 2002; accepted 25 October 2002.

Contents **Index**

Copyright ©2002, First Monday

Copyright ©2002, Paul Bocij

Corporate Cyberstalking: An Invitation to Build Theory by Paul Bocij
First Monday, volume 7, number 11 (November 2002),
URL: http://firstmonday.org/issues/issue7_11/bocij/index.html