Stalking in Cyberspace

John M. Deirmenjian, MD

The Internet has revolutionized communication on a global level while creating a medium for stalking. Cyberstalking has emerged as a new form of stalking behavior. While 10 states have passed laws against electronic harassment, there has been great debate about whether electronic stalking constitutes criminal behavior or whether a perpetrator is entitled First Amendment protection. In the psychiatric literature to date, there are no studies of cyberstalking. This article focuses on relevant cases of stalking on the Internet. Specific legal issues associated with cyberstalking, such as boundary laws and freedom of speech, are examined. The psychological profile of the cyberstalker, as well as methods of intervention, are discussed.

The Internet is an international computer network that has pioneered a new medium for communication known as cyberspace. By the year 2000, it is estimated that 40 million people in the United States alone will be sending 60 billion electronic messages annually.1

Cyberspace law is developing as a multidisciplinary specialty that encompasses all cases, statutes, and constitutional provisions that impact persons and institutions in cyberspace. The distinct components of cyberspace law include jurisdiction, freedom of expression, intellectual property, privacy, safety, equity, and electronic commerce.2

Safety issues of cyberspace law include crimes such as cyberstalking. Other cyberspace crimes such as computer hacking, child pornography, pedophilia, and hate crimes are often mistaken for cyberstalking in the popular literature and the media.

Cyberstalking refers to harassment on the Internet using various modes of transmission such as electronic mail (e-mail), chat rooms, newsgroups, mail exploders, and the World Wide Web. Cyberstalkers can obtain personal information about their victims, such as home addresses or phone numbers. After obtaining this personal information, cyberstalkers then have the ability to meet their victims in person. CyberAngels, an affiliate of the Guardian Angels, offers an online description of the stalking phenomenon on the Internet, which includes the following: malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, directed toward an individual, disregarded warnings to stop, harassment, and threat.3

Dr. Deirmenjian is a Forensic Psychiatry Fellow in the Dept. of Psychiatry, Case Western Reserve University School of Medicine, Cleveland, OH, and a Rappeport Fellow of the American Academy of Psychiatry and the Law. This paper was presented at the 29th Annual Meeting of the American Academy of Psychiatry and the Law, New Orleans, LA, October 22, 1998. Address correspondence to: John M. Deirmenjian, MD, Forensic Psychiatry, University Hospitals, 11100 Euclid Ave., Cleveland, OH 44106. E-mail: jdeirmen@earthlink.net.
Four basic motivations for stalking on the Internet include sexual harassment, love obsession, hate/revenge vendettas, and power/ego trips.\textsuperscript{4}

This article will introduce cyberstalking as a phenomenon and present specific cases of Internet harassment.

**Relevant Cases**

**Stalking on the Internet.** Case 1 Andrew Archambeau was charged with the misdemeanor of stalking a school teacher whom he had met on a video dating service.\textsuperscript{5} After five days, the teacher realized that she was not interested in pursuing a relationship. Archambeau, however, persisted and sent her (the teacher) approximately 20 e-mail messages. When the e-mails were traced to Archambeau, he responded that his "caller ID" showed that someone from her area was ringing and hanging up and that he perceived it as her shy manner of expressing interest. She denied the claim and went to the police after he left a message on her answering machine saying that he had watched her leaving work. He argued that pursuing his romantic interest via e-mail was nonthreatening, because e-mail messages can be ignored by the recipient. However, Michigan’s anti-stalking law prohibits nonconsensual contact via electronic communications.\textsuperscript{6}

Archambeau pleaded no contest to the charges and was sentenced to a year’s probation and ordered to undergo a psychiatric evaluation.\textsuperscript{7}

Case 2 Cynthia Armistead-Smathers of Georgia received obscene e-mails from the account of Richard Hillyard.\textsuperscript{8} She then began receiving messages sent through an anonymous remailer (an online service that masks the sender’s identity). The messages included phrases, such as “You’d better watch your back,” “Let’s get it on bitch,” and “I’m your worst nightmare.” After Hillyard’s Internet service provider canceled his account, Armistead-Smathers began receiving messages from the Centers for Disease Control and Prevention in Atlanta where Hillyard worked. She then received thousands of messages from men who had seen a posting of a nude woman (presumed to be Armistead-Smathers), which listed her e-mail address and offered prostitution during the Olympics. Out of fear, she moved three times that year, changed her phone number frequently, and began to carry a licensed concealed weapon. The police informed her that there was little they could do, until she received an anonymous message from someone saying that he had followed her 5-year-old daughter and her from the post office box to their home. Hillyard was charged with stalking and later acknowledged getting into an online argument with Armistead-Smathers but denied sending the messages.\textsuperscript{8}

Case 3 Jayne Hitchcock filed a $10 million lawsuit against the Woodside Literary Agency (Woodside) of New York claiming defamation and harassment.\textsuperscript{8} She had answered an e-mail advertisement posted by the agency. In its response, Woodside asked Hitchcock for a monetary fee and additional payments before it would represent her. The up-front fees raised her suspicion because legitimate agents generally earn their money
after selling an author’s work. So Hitchcock (as well as other suspicious writers), through posting in Internet newsgroups, informed other writers about possible fraudulence. She claims that the company targeted her for retaliation, defaming her in its ads and subjecting her to a barrage of assaults. Among the incidents cited in Hitchcock’s legal complaint: e-mail accounts used by Hitchcock, her literary agent, and her employer (the University of Maryland) were flooded with messages (mail bombing); and inflammatory messages were posted in newsgroups under Hitchcock’s name. A sexually oriented posting made under Hitchcock’s name included her address and phone number, which led to a series of unusual phone calls, unsolicited magazine subscriptions, and at least one suspicious package that contained incense. Although Hitchcock contacted the local police and the FBI, it was unclear how the author could prove her allegations because no actual threat had been made against her. It would also prove difficult to track the tormentors who had altered their e-mail account information to conceal their identity. The Jayne Hitchcock legal fund was established, and Jayne Hitchcock testified before a Maryland subcommittee on behalf of a bill to punish instigators of e-mail harassment in the state of Maryland.8, 9

Case 4 Robert and Teresa Maynard, who helped found Internet America, Dallas’s largest Internet access provider, discovered harassing messages posted on an Internet newsgroup.10 Most of the messages closed with the same poem: “Lord grant me the serenity to accept the things I cannot change... and the wisdom to hide the bodies of the people I had to kill.” The messages ranged from claiming Teresa Maynard as being unfaithful to one message in which the harasser stated, “I have a .45.” Kevin Massey, a 30-year-old computer consultant with a criminal record for burglary and weapons possession, was identified as the harasser. Massey claimed that he was responding to online attacks initiated by Maynard and his employers. However, Massey called himself “The Cyberstalker” and even lobbied to be a guest on Howard Stern’s radio show.

Case 5 In the United States’ first successful prosecution of a hate crime on the Internet, Richard Machado, a former student at the University of California, Irvine, was convicted of violating the civil rights of 59 mostly Asian students by sending threatening e-mail messages (signed “Asian hater”).11, 12 His message stated, “I personally will make it my [life’s work] to find and kill everyone [sic] of you personally. OK. That’s how determined I am. Do you hear me?” He threatened to kill them if they did not withdraw their enrollment from school. Initially, a jury was deadlocked nine to three in favor of acquittal. After serving a year in jail and undergoing a second trial, he was fined $1,000 and was given one year of probation, which prohibited his use of the university computer laboratories.10, 11 His attorney argued that the threat was a “classic flame” (online slang for an angry message that is more annoying than harmful). However, many disturbed recipients of the e-mail message were prepared to arm themselves with pepper spray, became suspicious of
Case 6  Jake Baker, a student at the University of Michigan, was arrested by FBI agents on February 9, 1995 and charged with “transmitting threats across state lines” to a pseudonymous Arthur Gonda. The charge came about after it was discovered that Baker had posted an erotic fantasy on the Internet in which he raped and tortured a character with the same name as one of Baker’s real-life classmates. The charges were later revised to making a “threat to injure another person,” but in the meantime Baker had been suspended from the university, and his story had made headlines around the world. Baker was eventually acquitted, in part because his story was determined to be self-expression and did not constitute a threat.

Discussion
Stalking is defined as the willful, malicious, and repeated following and harassing of another person that threatens his or her safety. Meloy and Gothard report that stalkers (also known as obsessional followers) are likely to be older, more intelligent, and better educated than other offenders with mental disorders. One federal study revealed that approximately one million women and 370,000 men are stalked each year. One of every 12 women claims to have been stalked at some point in her life. Meloy profiles the majority of stalkers as males who are likely to have prior criminal or Axis I mental disorders, such as drug or alcohol history, mood disorders, or schizophrenia. Meloy and Gothard found that 85 percent of their sample qualified for a personality disorder diagnosis, including antisocial, schizoid, borderline, avoidant, paranoid, and personality disorder not otherwise specified. They noted, however, that in comparison with a random group of mentally disordered offenders, obsessional followers more frequently have a Cluster B diagnosis other than antisocial personality disorder. However, paranoid personality disorder (Cluster A) and dependent personality disorder (Cluster C) have also been identified.

The psychological profile of the cyberstalker reveals a sophisticated perpetrator (i.e., one who is computer literate and is often financially able to support subscriptions to online services). The typical cyberstalker is the emotionally disturbed loner who seeks attention and companionship in cyberspace and often becomes obsessed with someone he met in a chat room. After obtaining personal information about the acquaintance, the stalker may seek a close, often smothering relationship. If spurned, the stalker launches a campaign of cyberspace harassment, which can extend from online to physical harassment if the stalker has obtained personal information about his victim. The stalker can experience significant attachment issues and transference as a result of electronic communication. The cyberstalker projects narcissistic linking fantasies upon victims, especially in the absence of sensory perceptions. The pursuit by a cyberstalker tends to have an obsessional, angry nature, usually as a result of rejection. In contrast, sexual predators have a sexualized, deceptive pursuit.

Cyberstalking provides the perpetrator
Stalking in Cyberspace

with anonymity and the opportunity to conceal gender and identity and to use multiple anonymous remailers, as well as the ability to gain computer access in public domains. For example, Richard Hillyard used computers at his place of employment, which would make a direct link to him more difficult. Moreover, the lack of vocal intonation and facial expression in electronic communication can affect the recipient's impression of the seriousness of a threat. In cyberstalking, the evidence in proving a credible threat is based upon the interpretation of the written word. Exclamations, repetition of phrases, and the use of boldface print can provide clues regarding the seriousness and emotions of the sender. Electronic communication provides objective data, whereas harassment via the telephone and following are usually based upon subjective reports by the victim or witnesses. The lack of social constraints connected with cyberstalking means that social anxiety, which typically serves to inhibit aggressive behavior, is nonexistent. However, some people consider communication on the Internet as safe, without social inhibitions, and protected against personal embarrassment or communicable diseases. While the Internet has been thought to provide a therapeutic outlet for anxieties that would otherwise be suppressed, others believe that fantasy can serve as a precursor to threat, such as in the Jake Baker case.

Global communications on the Internet raise the issue of borders in cyberspace where there are no physical boundaries. Cyberspace must be governed by a new set of rules. While protected by the First Amendment, activities in cyberspace must abide by state and federal legislation. The absence of geographic borders in cyberspace makes the application of territorial legal doctrine difficult. On a global level, the issue of borders becomes even more convoluted. Even if a new set of laws were created for cyberspace, the enactment of such laws, often in foreign countries, would be nearly impossible. For example, it was impossible to find “Arthur Gonda,” the Canadian recipient of Jake Baker’s messages. It has been difficult enough for authorities to act upon threats of cyberstalking locally, much less on an international level. In addition, there may be a greater burden of proof imposed upon an accuser to prove that there is imminent danger or threat. However, illegal activities, such as the distribution of child pornography, may be easier to apprehend. If a certain behavior is legal in one country and not in another, it must be determined which laws apply.

The evolution of the Internet has brought forth an ongoing debate on whether constitutional law, such as freedom of speech, applies to the Internet, and if so, to what extent should the government impose regulations on online activities. The free speech issues resulting from the development of the cyberspace medium include anonymity, accountability, defamation, discrimination, harassment, obscenity, and liability of online services and Internet service providers. The Communications Decency Act of 1996 made it a crime to make “indecent” or “patently offensive” material available to minors over the Internet. In June 1997, in a landmark ruling, the Supreme
Court struck down the Communications Decency Act, ruling that constitutional free speech protections apply just as much to online systems as to books and newspapers.24

To date, only 10 of the 50 states (Alabama, Alaska, Arizona, Connecticut, Delaware, Michigan, Maryland, Oklahoma, New York, and Wyoming) have enacted laws against computer harassment. While laws exist against telephone harassment where the motive is to annoy, threaten, or alarm another person, the difficulty with computer harassment lies in convincing local authorities that such cases are worthy of investigation.25, 26 Often, the difficulty appears to be that to merit the time and resources of the police, an imminent danger or threat must be present. Thus, the victim must provide proof or evidence that a crime has been committed. For example, in the Machado and Hillyard cases, it was the responsibility of the prosecution to prove the presence of a credible threat. It is clear in those two cases that the victims demonstrated fear for their safety to the extent that they altered their living circumstances and daily activities. In the Jovanovic case, the accused was not perceived to be a threat until the alleged encounter took place. Finally, Jake Baker was eventually acquitted because he was not found to be a credible threat. Some police departments are now forming threat assessment units specialized in cyberstalking to facilitate the investigation of these crimes. For example, in Will County, IL, a special Internet prosecution unit was formed for prosecuting all Internet-related crimes within the county. In addition, police officers are being given specialized training to monitor Internet newsgroups for the purpose of apprehending cyberspace criminals. Will County has also made an extensive effort to educate the public about Internet crimes.26

Organizations such as Women Halting Online Abuse (WHOA) and CyberAngels have formed to educate the community about online harassment and to protect individuals from cyberstalkers. CyberAngels is a network of volunteer sleuths that watches the information superhighway and investigates more than 10,000 harassment complaints a year.27 CyberAngels, which started in June 1995, has more than 1,200 members in 32 countries, creating a global “neighborhood watch” for cyberspace.28 Its director, Colin “Gabriel” Hatcher reports that cyberstalkers can be violent, paranoid, often with poor social skills, malicious, and obsessed with the object of their hatred.3

CyberAngels distributes a pamphlet entitled “Cyberstalking and Internet Online Harassment” that offers suggestions for preventing and dealing with cyberstalkers. In the pamphlet, Hatcher advises the reader to choose online user names with care and to avoid feminine names, which will immediately draw people seeking targets. Instead, he suggests choosing gender-neutral names and advises against giving out personal information such as home addresses, school names, workplaces, or phone numbers. He recommends ignoring online harassment at first notice to avoid a “flame war,” following which further hate mail and other forms of electronic harassment can ensue. If harassment continues, he
suggests sending one polite written warning without showing fear or anger or making threats. He also recommends logging all evidence from the start and saving all relevant e-mail, which may be collected for evidence if stalking persists and the police are involved.3

Conclusions

A new form of stalking has emerged, known as cyberstalking. To date, no studies in the psychiatric literature have examined cases of cyberstalking. In this article, six cases of cyberstalking are presented. The psychological profile of the cyberstalker, in its rudimentary form, is discussed. In addition, controversial legal issues such as boundary laws and First Amendment rights are identified, surrounding the application of the Internet to existing laws. Finally, there is a brief look at current modes of intervention, ranging from community organizations to state laws. Cyberstalking currently remains an open area for future investigation.

References

1. Anna Bevilacqua, Electronic harassment (last modified May 2, 1997). (http://www.wings.buffalo.edu/complaw/complawpapers)
3. Gabriel Hatcher, What is cyberstalking? (http://www.cyberangels.org)
7. Associated Press: E-mail stalker sentencing likely will influence future cases. The Detroit News home page, Mar 23, 1996
25. Reiter L: Stamp out e-mail harassment. The Record, May 5, 1998, p L09
28. O'Connor C: Women battle online stalking; harassment threats in cyberspace seem to be increasing experts say. Dallas Morning News, Oct 12, 1996, p 1A