CyberAge Stalking

By Barbara Fullerton

Barbara Fullerton is Manager of Library Services, Locke Liddell & Sapp LLP
Barbara has an M.L.I.S. from Emporia State University, Emporia, KS, a paralegal certificate, and a B.A. in mass communications.

Published December 22, 2003


These are words that define the characteristics and behaviors of a traditional stalker who “violates individual privacy and pursues unwanted attention of another.” In Black’s Law Dictionary, 2nd Pocket Edition, stalking is defined as “the act or an instance of following another by stealth or the offense of following or loitering near another, often surreptitiously, with the purpose of annoying or harassing that person or committing a further crime such as assault or battery” (2nd Pocket Edition, p. 660.). In similar feelings, a stalker’s behavior can cause a reasonable person to fear and lose control of their everyday routines. This fear is that key emotion stalkers like to impart to their victims.

Recent studies and research have shown that more men than women stalk, and that stalking exists with other forms of violence that can include threats and malicious intent of obsessive intrusions. Men have been victims of stalking “relationships,” but this article will focus on men stalking women with a new tool: the computer. This type of stalking is known as cyberstalking.

Cyberstalking refers to the use of the Internet, email or other electronic communication devices employed to stalk another person. Black’s Law Dictionary defines cyberstalking as “the act of threatening, harassing or annoying someone through multiple e-mail messages, as though the Internet, esp. with the intent of placing the recipient in fear that an illegal act or an injury will be inflicted on the recipient or a member of the recipient’s family or household.” (2nd Pocket Edition, p. 169). To understand the psychology of cyberstalking, we must first learn about stalking in the more traditional sense, before the world of computers changed stalking methods.

Most stalkers believe that male dominance equals female submissiveness. These acts can be physical, visual, verbal, or sexual in nature, and can be seen as a threat, invasion or assault that hurts or degrades or takes away an individual’s control. In the world before the use of the Internet, stalking research was still in its infancy, and there were no real statistics. In the mid 1990s, the National Violence Against Women Prevention Research Center conducted a survey of 8,000 women and 8,000 men in the U.S. From this survey, the results revealed that 78% of the victims of stalking were female and 87% of the perpetrators were male (Davis, 2002, p.165). The study also showed that the stalker was usually a friend, family member, ex-husband, co-worker, ex-boyfriend, or someone the victim had known.
There are some differences in stalkers. The single obsessed stalkers are most common and most violent. They want to dominate their possession. Intimacy seeking stalkers see their victims as their “true love” and believe their love is received to establish a relationship. Incompetent stalkers are aware that their advances and affection are not received but perceived that their efforts will be rewarded and lead to intimacy. Resentful stalkers frighten and threaten their victims and choose victims at random. Predatory stalkers take pride in their power with the intent to sexually assault their victims. And they like to get to know their victims (Davis, 2001, p. 167).

Internet

The computer has opened a door to many possibilities for these new stalkers. The Internet, as an easy accessible and affordable tool, opens new avenues for the “traditional stalker.” Cyberstalkers can choose a complete stranger, someone who meets a particular requirement. For example: a domain name can attract a stalker; a classmate who hides in the shadows of school and admires someone from afar but has no contact with the chosen victim (the Amy Boyer case); viewing a discussion in cyberspace; locating negative context in a chat room or in a discussion group; lurking around the USENET lists; liking or disliking the writing style of a person; finding a photo on the web; etc. Motivations of such stalkers include feelings of hostility and anger, jealousy, sensitivity to rejection, obsession, feeling of possession, and revenge. All these negative attitudes and the variety of Internet applications have made it more difficult to analyze and/or detect a stalker and his violent intentions.

In cyberstalking, there is no direct physical contact, but the victim feels the violence of the act and can bear long-term scars, both emotional and psychological. These scars can include paranoia, high-anxiety, panic attacks, chronic sleep disturbances, weight fluctuations and persistent nausea, increased usage of alcohol or cigarette, headaches, and depression (Pathe & Mullen, 1997).

Internet Service Providers (ISPs), email, web pages, websites, search engines, images, listservs, Instant Chat Relay (IRCs) are all cyberstalking tools. As Internet usage increased, it is not known if people realize what online stalking was or if it was recognized as a crime. One of the most famous cases that brought cyberstalking into the public’s eye was the Jayne Hitchcock incident. Her story brought cyberstalking to the attention of lawmakers and she and others helped rewrite state stalking laws. Her harassment began online via discussion groups and emails and then lead to physical stalking of her and her family in the real world.

Another example of a victim was Cynthia Armistead of Atlanta, Georgia. She and her daughter began receiving threatening and obscene messages and phone calls from her stalker in 1996. He posted phony advertisements on the USENET offering her services as a prostitute and provided her address and phone number. She moved and changed her address. Then she was stalked physically. Her stalker continued to email her. Finally he was caught and brought to trial. The stalker could not be prosecuted because Georgia had no laws regarding cyberstalking, but the stalker, Richard Hillyard, was charged with the “traditional” stalking laws and found not guilty.

In 1998 Dwayne Comfort, a former USD student, sent over 100 threatening, harassing, terrorizing and sexually explicit emails to five different victims. He used personal information about them and intimidated them to the point of obsession. He was able to avoid detection for 10 months. Also in that same year, Richard Machado emailed “death threat” messages to 59 students, mostly Asian Americans attending the University of California. Machado threatened, “to find and kill every one of you personally.” He was convicted on a civil rights charge and sentenced to a year in prison with time served. Machado was also expelled for poor academic performance. At the trial, he testified he had sent the messages out of boredom and to provoke a response. He denied any intention to follow up on his threats. His case was the first civil rights charge for crime committed on a computer.

It was New Hampshire in the late 1990s. Liam Youens fell in love with his fellow eighth grader Amy Boyer and obsessed her from afar and online. She had no idea she was being stalked. Liam stalked her for two years and created a website dedicated to her. He chronicled his daily obsession about her and published it on the website, as well as the ways he would kill her. Liam
obtained Amy’s social security number via an online database, found her place of employment, and as she was getting into her car, he shot her in the head and then killed himself. Because of this incident, and the easy accessibility to obtain social security numbers, the U.S. legislation passed the Social Security Number Protection Act of 2000. (The Social Security Number Privacy and Identity Theft Prevention Act of 2003 was introduced in the 2003 legislation to prevent misuse and identity theft of these account numbers.) It is now a civil and criminal offense to sell or purchase a number except for legitimate purposes. The online database brokers were also found liable for their role in Amy’s death. The New Hampshire Supreme Court has held that information brokers and private investigators can be liable for the harms caused by selling personal information.

About this time, then-Vice President Al Gore realized there was a rise in online stalking and commissioned the U.S. Justice Department Report on Cyberstalking. From the 1999 study, it was reported that more than 1 in 12 women (8.2 million) will be stalked or have been stalked, and 50% of the cases will not be reported. Stalking victims are usually between the ages of 18-26, and stalkers usually have a prior criminal history or a personality disorder. Cyberstalkers now may be younger, more intelligent and better educated than other criminals. They are described as fairly lonely, isolated, highly intelligent, impulsive, cunning, resourceful, understand how to be anonymous, and know computers. They love cyberspace because there are no face-to-face meetings.

Anonymity has another trait that is important in cyberstalking: pseudonymity. The Internet and ISPs allow users to create a fake name as their identity. One can fake gender, age, race and physical appearance. It is up to the user to decide how to control personal information that is released on the Internet. Another reason to use cyberspace is real-time vs. virtual time communications. Email users are more blunt and direct in their communications and less concerned with what possible impact their speech or chosen words may have on another person. Email has no body language, no tone of voice, and no facial expressions. Most often people do not realize that emails are not private and that email systems can create a complete record of transactions. And what about cookies? Cookies or data text files are stored on a user’s hard drive. When visiting certain sites, one can track the habits of the users by accessing the cookies. Most surfers do not know how their information is gathered and used. Now many commercial and non-profit websites will tell the user what they do with the collected cookies. But this information is not in “plain sight” and one has to hunt for the policy.

On the Internet, cyberstalkers can sometimes reach an anonymous identity by using a tool called Anonymizer or MixMaster. Using one of these applications can wipe out someone’s electronic identification information and reallocate it to an anonymous ID. These re-mailers can also use public key cryptography so there is a complete privacy for the user. By chaining together a few of these re-mailers, the user can create a complicated trail for law enforcement and others to track. There are several individuals and groups who would like to call for a prohibition of these re-mailers. But the First Amendment and privacy issues play a part in why these applications are still available to the public. Free speech can be facilitated by anonymous online usage, which allows human rights activities, political and religious speeches and whistleblowers to engage in confidential communications (Wallace, 1999). For example, Anonymizer was used in 1999 to launch the Kosovo Privacy Project to provide free and confidential web browsing and email to people in that region. Other Internet tools that are utilized to taunt their cyber victims include: spoofing (forging headers), spamming, sniffing, chat rooms, and news groups (Wall, 2001, p. 147).

Laws

First Amendment

As in defining harassment in a cyberstalking case, what do the courts consider the line between a genuine threat and a nuisance when considering the First Amendment? (Wall, 2001, p. 6) One such famous case is the Jake Baker case in United States vs. Alkhabaz. Baker created and published stories about rape-torture and posted them to discussion groups on the Internet. In one of his stories, he named the victim as one of his fellow female students. During the time he wrote his stories, Baker had not stalked this fellow student or contacted her. He said he used her name because it rhymed with other words in his stories. This caused the confusion among many students who knew the female student and thought the stories were about her. While these stories were
initially about violence, the courts looked at Baker’s right to freedom of speech. This brought in a new perspective on cyberstalking. Courts must look at the First Amendment in all stalking cases and the level of harassment involved in each case. The courts ruled in his favor, and his words were protected under the First Amendment. The court found that he had the right to freedom of speech and the email messages were not a credible threat. But some say the law did not take action to protect the female listed in his stories. It was a violation of the woman’s character but the courts did not address the slander against her, nor did they address her privacy rights.

Anti-stalking statutes need to be relatively broad to be effective and carefully formulated and enforced so as not to impinge upon speech that is protected by the First Amendment.

“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.”

Stalkers may claim the First Amendment as a defense to any state law but the First Amendment does not protect true threats. And the United States Supreme Court realized that true threats might be criminalized without violating the First Amendment. The First Amendment lets the public give free speech in a public forum and the Internet is considered a public forum or an important tool for the expression of free speech. For example the Communications Decency Act of 1996 was regarded by many as a dangerous first step in censorship of the Internet by the federal government, and it was ruled that the Communications Decency Act is an unconstitutional infringement of speech (Reno v. American Civil Liberties Union, 521 U.S. 844, 850-52, 870 (1997); American Civil Liberties Union v. Reno, 31 F.Supp.2d 473, 476, 493 (E.D. Pa. 1999). But the courts have also recognized some parts of the Internet are private. Thus, privacy laws are broken as stalkers find information about their victims online and are repetitive in their online harassment and conduct attitude.

State

Most stalker cases are prosecuted at the state and local level, so it is up to each state to provide language that will protect potential victims. Most often, first time offenders are given lenient fines or punishments. Some state laws need to be changed to offer more severe punishments. All 50 states have stalking laws, and about 42 states now have laws that include electronic communications as a harassment tool or in some way relate to cyberstalking. States that do not have laws yet are: Utah, New Jersey, New Mexico, Idaho, Nebraska, and DC. In 1993, Michigan was the first state to pass a stalking law that included the words electronic harassment. It has been a challenge for the states to find a balance between a law that involves “expressive conduct and speech which is protected under the First Amendment,” and laws that protect victims and forbid harassment and provide privacy.

Another problem is the accused may not be in the same jurisdiction as the victim, or where the offense occurred. But in these instances, states have broadened their jurisdiction rules to help address cybercrimes that are not part of their harassment laws, like jurisdiction. In their jurisdiction laws, courts can look at where the stalking began, various sites the messages may have passed, and the physical location of the stalker.

Federal

There is also a gap in the federal law. In 1996, the U.S. passed the Interstate Stalking Act (18 US 2261A). It is a crime for any person to travel across state lines with intent to injure or harass another person. For example: Keith Kosiewicz intended to extort money from a San Diego Corporation. He sent threatening emails from Illinois, which also violated 18 USC 875 (b) (the anti-stalking federal law). No one answered his emails so Keith traveled to the corporation and was arrested by the police. According to 18 USC 875 (c) most stalking statues require specific intent on the part of the defendant to install fear and a threat to its victim. 18 U.S.C. § 2261A was originally enacted on September 23, 1996. In November 2000, the federal statute was amended as part of the Violence Against Women Act (VAWA) of 2000 (P.L. 106-386). This act extends the federal stalking statute to stalking that occurs by mail, telephone or Internet. VAMA 2000 is aimed to engage the courts in the effort against domestic violence, sexual assault, and stalking by making the courts
eligible to receive funds (STOP grants and Grants to Encourage Arrests) for training court personnel and state and federal court judges. And training is essentially what is needed for cyberstalking cases.

Many law enforcement officers are not trained to handle cyberstalkers. Sometimes complaints or reports are not taken seriously. Some officers are not computer literate and/or departments are not equipped with the right software to track cyberstalkers’ footsteps.

**How to Stop Cyberstalking**

There are some ways to help stop cyberstalking: self-regulatory, ignore the stalking, and self-protection. Self-regulatory and self-protection practices can include turning off the computer, changing your email address a few times a year, or dropping out of discussion groups. All are not solid ways to deal with an online stalker. One can contact their Internet Service Provider if they have found offensive information about themselves. The ISP may eliminate the accused account. But policies by the ISPs addressing electronic harassment often are difficult to locate. Most policies are not clear and do not have understandable procedures. ISPs need to cooperate fully with the law agencies and to develop training and enforce their policies. WHOA, the organization founded by Jayne Hitchcock, was established to educate the Internet community about online harassment and help ISPs formulate policies that system administrators can adopt to create a harassment free environment. Online abusive acts do affect actual lives whether they are verbal abuse vs. online text abuse.

**How to handle a stalker**

Here are some things to follow:

- Use another email address via Hotmail or Yahoo when visiting chatrooms, blogs, newsgroups
- Limit your personal email address to only friends and family
- Use a gender-neutral user name
- Use illogical patterns for your password
- Use a good IRC program for chat (MIRC)
- Locate ISPs with acceptable use policies
- Use a re-mailers to post to Usenet groups
- Assume all communications are public
- Change your password frequently
- Never leave your computer logged on
- Avoid 800 or 900 numbers
- Request privacy policies
- Do not create an online biography
- If you own your own domain name, create multiple mailboxes and use the main one only for friends and family
- Do not offer your real name to strangers
- Do not get caught up in feeling of guilt over not being nice online
- Ego search. Search your name on the search engines to see if anything “weird” pops up.

**If you are being stalked**

- Send a message to the offender. Make it a clear warning that contact is unwanted. Cease all communications and keep a copy of all messages.
- File a compliant with the offenders’ ISP provider
- Filter messages
- Get help from WHOA or NCVC or CyberAngels
• File an harassment report at the police department
• Save all messages
• Save all recorded messages
• Keep all copies out of the house (Stalkers are known to break in and steal things.)

Conclusion

Cyberstalking is an old behavior with a new tool: the Internet. Today any woman who uses the Internet is an instant target, and the number of cyberstalking cases has increased. Some say online harassment is killing free speech on the Internet, but this type of harassment can be seen in a variety of guises: sending of unwanted emails which are abusive, threatening or obscene; sabotage via the computer by spamming junk email messages; sending computer viruses; impersonating ones victim online and sending abusive emails or spams in the victim's name; and subscribing the victim's names to mailing lists without permission. The Internet has no physical boundaries. Users forget that computers are just tools that give a false sense of security and community. I believe cyberspace encourages us to be individuals within a cyberspace community where we are being watched. In cyberspace it is more difficult to control one's speech, one's privacy, and one's safety rights. It is a place where stalkers can create their own world. Remember, stranger stalking occurs both in the real and virtual world and the majority of victims are women. The aim of the stalker is to control the victim.

Bibliography and Resources

Articles


P.E. Mullen, M. Pathe, R. Purcell & G.W. Stuart, “Study of Stalkers,” *The American Journal of


**Books**


**Hotline**

National Center for Victims of Crime

800-FYI-CALL

National Domestic Violence

800-799-SAFE

**Seminar**

Jayne Hitchcock, Guest Speaker, Internet Librarian, Palm Springs, CA, Nov. 2002.

**Video**

Websites

Anti-Stalking

Resource site for Victim research.

CyberAngels

Guardian Angels for Cyberstalking.

Cyber Criminals Most Wanted

The first cybercrime prevention website to gather evidence against cyberstalkers.

Cyberstalking Study Guide

Information including privacy issues, spamming, etc.

Cyber-stalking.net

Websites about Cyberstalking and/or stalking.

First Amendment

First Amendment website with data on cases and information on the Freedom of Speech.

Privacy Rights Clearinghouse

Information on Internet privacy and Identity Theft.

Research Studies on Cyberstalking

A list of research studies from 1997-2002.

Stalking Resource Center

The National Center for Victims of Crime’s information clearinghouse.

Stalkingvictims.com

A website built by Stalking Victims Sanctuary.

WHOA

Working to Halt Online Abuse

Information on statistics, resources and safety.