Cyberstalking:
Free Speech or High-Tech Harassment

Paul J. Elliott

Introduction

Cyberstalking implies stalking by way of the Internet and its related communication technologies. But cyberstalking as criminal behavior is more than an online extension of harassing behavior. While sending a former partner an unwanted email can by itself be characterized as an incident of cyberstalking, the presence of technology in the conduct is not the concern not the issue. The misuse and abuse of technology to threaten, frighten, coerce another person by hiding one's identity to engage in criminal behavior is a recent and alarming trend the United States and across the entire technologically developed world.

"Stalking is a crime of intimidation. Stalkers harass and even terrorize through conduct that causes fear or substantial emotional distress in their victims" (U.S. Department of Justice 2002). The Justice Department estimates that 1 in 12 women and 1 in 45 men will be stalked at some point during their lifetimes. However, laws related to stalking have only been around for the past decade, and laws related to cyberstalking are even more recent, if they exist at all.

Cyberstalking is a troubling antisocial trend as much as a legal challenge to law enforcement and legislators, dealing with a problem that did not exist a couple decades ago. And yet the behaviors associated with cyberstalking are nothing new. They involve the same elements of fear, intimidation and emotional distress that offline stalkers employ against their victims. However, the threat posed by cyberstalking is spreading like a virus because of the nature of the Internet – its openness and ease of anonymous communication, making vulnerable men, women, children, organizations and society to the dangers lurking behind the mask of cyberstalkers.

Legal background

In January, President Bush signed into the law the reauthorization of the Violence Against

Women Act, extending it to 2011. The Act updates the Communication Act of 1934 to contain a controversial provision on Internet stalking as found in Section 113 of the amendment now includes language that extends regulatory power over "any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet."

The new definition for 'cyberstalking' is now established as an amendment to the U.S. Code (U.S.C § 2261A, 2005). Section 114 of the 2005 Act expands the meaning of "stalking" to now include any use of interactive computer use of interactive, computer services that causes "substantial emotional distress to that person" or places that person in "reasonable fear of the death of, or serious bodily injury" to the "person, a member of their immediate family, or a spouse or intimate partner of that person" (§ 2261A). Sections 114 and 115 also set a minimum penalty of 1 year imprisonment or more for the first offense, and at least 2 years for additional offenses that involve the violation of a temporary or permanent civil or criminal injunction, restraining orders, personal protection orders or other no-contact orders.

Backers of the bill contend these updated provisions to the law will protect victims from individuals who abuse modem technologies such as email, voice over Internet protocol (VoIP), instant messaging, web logging (blogging) and any other communications made possible by the Internet. Proponents argue that related provisions update existing legislation to include newer methods of communication, including email, voice over Internet protocol (VoIP) and instant messaging.

However, by adding the Internet to the existing telecommunication devices included in the 1934 Communications Act, Congress has unintentionally created a constitutional problem. Under Section 223(c), which covers obscene or harassing phone calls, it was illegal to use the

telephone or a "telecommunications device" without first disclosing your identity with the "intent to annoy abuse, threaten, or harass any person at the called number or who receives the communication." The legislation was originally worded in a House version to criminalize only misuse that would cause someone "substantial emotional harm" (McCullagh 2006a). But the final version of the bill did not limit the language in the same way, and left the broader wording of the 1934 Act intact.

The Act specifically includes "any device or software than can be used to originate Telecommunication," but there is a significant difference between annoying phone calls directed to a specific person and Internet messages that are undirected toward an individual such as postings on a web log (blog). Congress has made it illegal to create any type of anonymous electronic annoyance, and instead has created a Constitutional issue with this amendment.

"Who decides what's annoying? That's the ultimate question?" asked Clinton Fein, owner of the website *Annoy.com*. Fein's site allows visitors to send "obnoxious and profane postcards through email" (McCullagh 2006a).

The element of anonymity is a double-edge sword. On one hand, anonymity goes to the heart of free speech and the right not to be identified when criticizing the government without fear of reprisal. Fein points out that you can mail an anonymous letter through the post office, so is email to be treated differently because Congress has put Internet communication on par with telephone use.

Cyberstalking

Is cyberstalking just an extension of offline stalking? Whereas stalking generally involves the physical harassment or threatening of an individual through behaviors such as

following a person, appearing at a person's home or place or business, and may involve the use of the phone or written messages, cyberstalking involves the use of technology that can mask a stalker's identity, whereabouts or intent. Most state's stalking laws necessitate the making of a credible or an implied threat of violence against the victim or the victim's immediate family. However, in cases of cyberstalking, there is no immediate threat of physical violence, as the perpetrator may be some distance from the intended victim-in a different state or even in a different country.

In most cases of stalking, there is an intimate or dating relationship, although some cases of stalking involve strangers. Most victims of stalking are women, and most stalkers are men who attempt to exert control over their victims. Offline stalking most often occurs in the same geographical area, whereas cyberstalking can occur from any distance.

Cyberstalking is a recent phenomenon as the technology is expanding the ease of instantaneous communication. Cyberstalking falls under two broad categories. The first is that of the mere extension of offline stalking to the use of the Internet. The second is the stalking, often anonymous, that is exhibited by hackers, flamers and others whose are driven by the antisocial, isolationist nature of their behaviors. While in many cases of cyberstalking, the cyberstalker and the victim may have had some type of previous relationship, more often than not cyberstalking involves strangers who take advantage of the ease and availability of personal information found on the Internet.

Cyberstalking has been identified by the U.S. Attorney General as a growing problem. The 1999 Report on Cyberstalking reported that “assuming the proportion of cyberstalking victims is even a fraction of the proportion of persons who have been the victims of offline stalking within the preceding 12 months; there may be potentially tens or even hundreds of thousands of victims of

recent cyberstalking incidents in the United States."

The slow pace of updating stalking laws to include cyberstalking is reflected in a misconception that since there is no physical contact involved in the harassment, cyberstalking is not as dangerous to a person as stalking. However, this is a dangerous assumption. Often online contact is a precursor to later physical contact and violence against the victim. The state of California has recognized the distinctive nature of cyberstalking by amending its stalking statute. Now under California law, a "credible threat" can be made if it includes an "electronic communication device" including "telephones, cellular phones, computers, video recorders, fax machines or pagers." Most state laws fail to recognize the threat, real or implied, in acts of cyberstalking.

Researchers and law enforcement personnel are discovering that there is a strong link between child molestation cases and cyberstalking. The ease of exchanging child pornography through secretive and anonymous file sharing is enabling pedophiles to target children through chat rooms, instant messaging and popular web sites used by teens and children. The ease of pedophiles to establish online relationships provides little inhibition to Internet predators.

The chief of the Sex Crimes Unit in the Manhattan District Attorney's Office in New York has estimated that one in five cases it handles involve cyberstalking. New York City Police's Computer Investigations and Technology Unit estimates that "almost 40 percent of the caseload in the unit involves electronic threats and harassment" (1999 Report). If current trends continue, the number of cyberstalking caseloads will be the dominant problem for law enforcement agencies.

> "Cyberstalking has replaced traditional methods of stalking and harassment. In addition, cyberstalking has led to offline incidents of violent crime. Police and prosecutors need to be aware of the escalating numbers of these events and devise strategies to resolve these problems through the criminal justice system."

Linda Fairstein
Chief of Sex Crimes Prosecution Unit
Manhattan District Attorney's Office

Cyberstalking as behavior

Understanding stalking in general is needed before dealing with the problems that arise from cyberstalking; but not all cyberstalkers begin as stalkers. Even normal persons can engage in cyberstalking because of the decrease in inhibition. A person who would never confront one's intended victim in person or even by phone can find it easy to behave in an abnormal way if one feels there are no repercussions of making an online threat. This ease and anonymity of using the Internet can entice a person to harass or threaten another either directly or through the enlistment of others.

The anonymity of the Internet also provides new opportunities for would-be cyberstalkers to hide their identity from their victims. This can begin by using different screen names when emailing or instant messaging. But experienced stalkers also use email remailers to hide their messages not just from their victims, but from law enforcement agencies. Remailers allow anonymity and protection to the stalker and leave the cyberstalker in control of the situation.

Anonymity coupled with harassment and threatening behavior can be very frightening to a person, unsure just where the cyberstalking is – across the country or across the street. And armed with anonymity, cyberstalkers can become offline stalkers, pursuing their victims in their home. This is particularly evident in pedophiles who arrange to meet their victims at their home, an agreed-to public place or anywhere else as long as the stalker believes he is in control. What is most troubling and of concern is that web sites, like Facebook and other community sites, often provide the cyberstalker with personal information, photographs, unlisted and cellular telephone numbers, addresses and details regarding the victim's family and friends, allowing the cyberstalker

to become intimately familiar with the victim, so that they drop their guard to the stranger.

Anonymous identities on the Internet can easily be accomplished by creating a free webmail account. Without authenticating personal information such as requiring the use of a credit card, it is easy for anyone to create an online identity. More troubling is mail servers that fail to include identifying information in the mail header, frustrating the email recipient. It is nearly impossible to report the multitude of false identities to Internet service providers. This type of anonymity permits the cyberstalker to send threatening or harassing communication without fear of being caught. This form of anonymity lacks a legitimate purpose and places persons at risk of receiving threatening communication, not protected by the First Amendment.

Free speech issues

Cyberstalking raises several important issues regarding free speech. Striking the balance between public safety and addressing the demands of the First Amendment is needed as new laws are drafted to combat this criminal activity. The First Amendment does not prohibit any and all regulation that may involve or have an impact on speech. The Supreme Court has recognized that threatening speech is not protected by the First Amendment (see *Watts v. United States*, 394 U.S. 705 (1969).

In addition, the First Amendment issue of anonymity was addressed by the U.S. Supreme Court in 1995. Justice Clarence Thomas wrote in his majority opinion that "the Framers understood the First Amendment to protect an author's right to express his thoughts on political candidates or issues in an anonymous fashion" (*McIntyre v. Ohio Elections Comm 'n*, 1995). Thomas cited the Federalist Papers as the most famous example of anonymous writing that predated the drafting of the U.S. Constitution. Thomas emphasized that the historical evidence

indicates the Founding Fathers "opposed attempts to require that anonymous authors reveal their identities on the ground that forced disclosure violated the 'freedom of the press'" (McIntyre).

Anonymous pamphlets were common in colonial America as many were written under pseudonyms. Even Benjamin Franklin wrote under several pen names in his writings, most famously under the name of Richard Saunders, "author" of Poor Richard's Almanack. Printers at the time were often pressed by the authorities to reveal an author's identity, so pseudonyms were a hedge against political persecution and prosecution by the state.

But with regard to cyberstalking, anonymity gives perpetrators a mask to hide behind, and a disincentive to conforming to social norms, with little regard to their criminal responsibility. So just what is the constitutional standard applicable with anonymous speech?

This type of anonymity can lead to another form of harassing communication. Cyberstalking-by-proxy is the abuse of speech where an individual campaigns against a person, group, or organization so that others spread the harassment to an extreme, creating a false impression of wrong-doing, and at least masking the identity of the originator of the harassment.

Related to cyberstalking-by-proxy is cyberterrorism, which includes the hacking into secure computer systems, denial of service attacks, hijacking web sites, the manipulation of stock prices, and other extreme acts of social disorder. By using others to harass, the cyberstalker fades deeper into anonymity and aware from personal responsibility. This type of speech is particularly harmful to public discourse, as the intent is to silence speech rather than to protest. By using technology to thwart the dissemination of public information, the cyberstalker seeks to control the flow of information, the manner in which the media can access and report responsibly on it and create an atmosphere of untruths and misconceptions.

Responding to online threats

While cyberstalkers take advantage of technology, the Internet industry is employing several new tools to help individuals and families protect themselves against unwanted communication. Chat rooms allow users to alert others and their ISP to annoying, harassing or threatening messages. Email users can block out not just spam, but also any individuals engaging in cyberstalking. The problem remains in how to assess the threat level, as an anonymous person's intent may be as difficult judge as their identity. Other solutions involve safe online communities protected by specialized servers to protect children and teens from unwanted content and intrusions. But cyberstalkers can assume safe identities to infiltrate these communities to prey on children – a continuing challenge to law enforcement.

Technologies such as reverse engineering of security programs enable companies and law enforcement to trace the origins of threatening communication, but technology cannot alone solve the problem unless cyberstalking is taken as a serious crime. State laws are often inadequate to combat the problem, leaving prosecutors with little option except to charge lesser offenses because of lack of demonstrable "threat level" to an individual from anonymous cyberstalking. Only a third of U.S. states have laws dealing with cyberstalking, making prosecution more difficult as incidences continue to escalate. The federal effort must be met by states which have primary jurisdiction in areas of cyberstalking.

The Attorney General in the 1999 Report Federal law recommends that the Cable Communications Policy Act be amended to "provide access to the same type of subscriber records, and under the same standards and privacy safeguards, as those for electronic mail subscribers." However, concerns over access to company database and reported cases of selling personal data

would make such an amendment unpopular currently. Nevertheless, the protection and safety of legitimate users, especially children, must remain the primary concern.

The first step for anyone receiving an unwanted communication is to notify the individual that expressing a request not to be contacted again. However, this is difficult when the cyberstalker has assumed anonymity and is using a public site instead of email to conduct the harassing behavior. Nevertheless, it is important for victims to save all communications that can be used as evidence, no matter the threat level. Keeping adequate records of all communication can provide law enforcement agencies with the information they need. Contacting the victim's Internet Service Provider is important because most ISP's prohibit abusive communication. Contacting the ISPs and domain holders of the cyberstalker is also important to discourage abusive online behavior.

Conclusion

Cyberstalking is an assault on an individual or a group's right to privacy, security and free speech. It is a growing problem involving the abuse of technology to exploit the vulnerabilities of persons known unknown to online predators. By its nature of being antisocial and against the public welfare as a whole, cyberstalking should be treated as a serious crime in and of itself apart from current anti-stalking statutes. The fact that cyberstalking often occurs apart from prior offline stalking behavior makes responding to it a priority for law enforcement, industry and legislators to address. Inadequate responses will only make prosecutions more difficult when relying on outdated statutes. Patching together legislation onto the Communication Act of 1934 has addressed the problem but has inadvertently raised First Amendment concerns that could jeopardize the constitutionality of the recently passed Violence Against Women Act, similar to the

overturning of the Communications Decency Act because they both have prohibited "annoying" communication-a concept too vague to ignore by the courts.

Just as cyberstalking is a recent phenomenon, legislators must address it as a current crime against persons, groups, organizations and businesses, focusing laws against the conduct of harassment, the predatory enticement of teens and children by pedophiles and purveyors of child pornography, the reality of the threats expressed or implied by the communication regardless of physical proximity, and the overt disregard to public safety.

Anonymous speech that furthers the aim of democracy and encourages others to speak out and respond must be protected by the courts, without seeking to punish or retaliate because of an undisclosed identity. But when unprotected speech leading to criminal conduct occurs, the mask of anonymity must be removed to uncover the darkness that would destroy the light of liberty.

REFERENCES

1999 Report on cyberstalking: A new challenge for law enforcement and industry; a report from the Attorney General to the Vice President. (1999) US. Department of Justice. Retrieved from the World Wide Web April 10, 2006 from: http://www.usdoj.gov.criminal/ cybercrime/cyberstalking.htm

Bocij, P. (2004) *Cyberstalking: harassment in the Internet age and how to protect your family*. Westport, Conn.: Praeger, 2004

McCullagh, D. (2006). Create an e-annoyance, go to jail. *CNET News.com*. Retrieved April 21, 2006 from http://news.com.com/Create+an+e-annoyance%2C+go+to+jail/2010--1028_3-6022491.html

----- (2006). FAQ. The new 'annoy' law explained. *CNET News.com*. Retrieved April 21, 2006 from http://news.com.com/FAQ+The+new+law+explained/2100-1028_36025396.html

McIntyre v. Ohio Elections Comm 'n, 514 US. 334 (1995). LII/Legal Information Institute. Cornell Law School. Retrieved from the World Wide Web Apri110, 2006 from http://straylight.1aw .come1l.edu/supct/html/93-986.ZC 1.html

Spitzburg, B. and Hoobler, G. (2002). Cybersta1king and the technologies of interpersonal terrorism. *New Media & Society*, 4 (1).

Twin Cities Public Television, Inc. (2002). *Benjamin Franklin, Wit and Wisdom*. Retrieved April 25, 2006 from http://www.pbs.org/benrranklin/13_wit_name.html

Strengthening antistalking statutes. (2002). US. Department of Justice. Office for Victims of Crime. January 2002. Legal series #1. Washington, D.C.: Government Printing Office.