

Cyberstalking: A New Challenge for Law Enforcement and Industry

A Report from the Attorney General to the Vice President

August 1999

Introduction

The new millennium is fast approaching, and the information superhighway is undergoing rapid growth. The Internet and other telecommunications technologies are promoting advances in virtually every aspect of society and every corner of the globe: fostering commerce, improving education and health care, promoting participatory democracy in the United States and abroad, and facilitating communications among family and friends, whether across the street or around the world. Unfortunately, many of the attributes of this technology – low cost, ease of use, and anonymous nature, among others – make it an attractive medium for fraudulent scams, child sexual exploitation, and increasingly, a new concern known as “cyberstalking.”

***“Make no mistake: this kind of harassment can be as frightening
and as real as being followed and watched in your neighborhood or
in your home.”***

Vice President Al Gore

Recognizing this emerging problem, Vice President Al Gore asked the Attorney General on February 26, 1999, to study the problem and to report back with recommendations on how to protect people from this threat. Responding to this request, this report explores the nature and extent of cyberstalking; surveys the steps law enforcement, industry, victims groups, and others currently are taking to address the problem; analyzes the adequacy of current federal and state laws; and provides recommendations on how to improve efforts to combat this growing problem.

As discussed below, the nature and extent of the cyberstalking problem is difficult to quantify. In addition, while some law enforcement agencies are responding aggressively, others

are not fully aware of the problem and lack the expertise and resources to pursue cyberstalking cases. Similarly, while some Internet Service Providers (ISPs) have taken affirmative steps to crack down on cyberstalking, others have not, and there is a great deal more that industry can and should do to empower individuals to protect themselves against cyberstalking and other online threats.

Indeed, current trends and evidence suggest that cyberstalking is a serious problem that will grow in scope and complexity as more people take advantage of the Internet and other telecommunications technologies. The analysis and recommendations contained in this report offer a framework for an initial response to the problem. These recommendations, however, are only a first step. Important advances can be made if industry, law enforcement, victims service providers and support groups, and others work together to develop a more comprehensive and effective response to this problem. Ultimately, however, the first line of defense will involve industry efforts that educate and empower individuals to protect themselves against cyberstalking and other online threats, along with prompt reporting to law enforcement agencies trained and equipped to respond to cyberstalking incidents.

What Is Cyberstalking?

Although there is no universally accepted definition of cyberstalking, the term is used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat.¹ While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously.

¹ Statutes that require a showing of a "credible threat" may be problematic in the prosecution of stalking. Stalkers often do not threaten their victims overtly or in person; rather, they engage in conduct that, when taken in context, would cause a reasonable person to fear violence. In the context of cyberstalking, a credible threat requirement would be even more problematic because the stalker, sometimes unbeknownst to the victim, may be located a great distance away and, therefore, the threat might not be considered credible. The better approach, codified in the federal interstate stalking statute, 18 U.S.C. 2261A, is to prohibit conduct that places a person in reasonable fear of death or bodily injury.

Protecting Children from On-Line Dangers

Although the Internet and other forms of electronic communication offer new and exciting opportunities for children, they also expose children to new threats. For example, Federal law enforcement agencies have encountered numerous instances in which adult pedophiles have made contact with minors through online chat rooms, established a relationship with the child, and later made contact for the purpose of engaging in criminal sexual activities.

Federal, state, and local law enforcement agencies have responded aggressively to protect children from online sexual predators. For example, in 1995, the Federal Bureau of Investigation launched an undercover initiative, dubbed Innocent Images, to combat the exploitation of children via commercial online services. Based in Calverton, Maryland, "Innocent Images" is the central operation and case management system for all FBI undercover online child pornography and child sexual exploitation investigations. As of December 31, 1998, the initiative has resulted in 232 convictions. Similarly, the U.S. Customs Service's CyberSmuggling Center, based in Sterling, Virginia, plays an important role in combating sexual exploitation of children via the Internet and other online communications media. The Center develops leads and tips for law enforcement investigation, receives complaints via the U.S. Customs Service website, and coordinates undercover operations against international child pornography and child sexual exploitation rings. The National Center for Missing and Exploited Children unveiled a new CyberTipline in March 1998 to serve as a national online clearinghouse for tips and leads about child sexual exploitation. (www.cybertipline.com)

The Department of Justice, through the Office of Juvenile Justice and Delinquency Prevention's Missing and Exploited Children Program (MECP), provides funding to state and local law enforcement agencies to create multijurisdictional responses to prevent and combat Internet crimes against children. In 1998, ten state and local agencies received grants under MECP; an additional eight task forces will be funded in 1999.

There are steps parents and others can take to protect children from online dangers. Parents should teach their children to follow the common-sense "rules of the road" for the Internet, including the need to protect their privacy in the online world. The FBI, for example, has prepared an online "Parent's Guide to Internet Safety." (www.fbi.gov) Moreover, individuals should report inappropriate behavior to their Internet Service Provider (ISP) or, if it involves potentially illegal conduct, to appropriate law enforcement agencies. Law enforcement agencies need to establish and/or improve programs that train their personnel to recognize the seriousness of online child sexual exploitation and how to investigate this new form of criminal conduct. They also need to work closely with ISPs and others to facilitate communication and cooperation. Finally, private companies, including ISPs, need to provide parents and children with effective tools to protect children from online exploitation, including filtering technology, parental controls, and other efforts. ISPs also need to establish clear policies that prohibit online solicitation or exploitation of children and to take appropriate action when such incidents come to their attention, as is now required under federal law. See 42 U.S.C. 13032.

Nature and Extent of Cyberstalking

An existing problem aggravated by new technology

Although online harassment and threats can take many forms, cyberstalking shares important characteristics with offline stalking. Many stalkers – online or off – are motivated by a desire to exert control over their victims and engage in similar types of behavior to accomplish this end. As with offline stalking, the available evidence (which is largely anecdotal) suggests that the majority of cyberstalkers are men and the majority of their victims are women, although there have been reported cases of women cyberstalking men and of same-sex cyberstalking. In many cases, the cyberstalker and the victim had a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship. However, there also have been many instances of cyberstalking by strangers. Given the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes.

The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. Put another way, whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence.

Offline vs. Online Stalking -- A Comparison²

Major Similarities

- o Majority of cases involve stalking by former intimates, although stranger stalking occurs in the real world and in cyberspace.
- o Most victims are women; most stalkers are men.
- o Stalkers are generally motivated by the desire to control the victim.

Major Differences

- o Offline stalking generally requires the perpetrator and the victim to be located in the same geographic area; cyberstalkers may be located across the street or across the country.
- o Electronic communications technologies make it much easier for a cyberstalker to encourage third parties to harass and/or threaten a victim (e.g., impersonating the victim and posting inflammatory messages to bulletin boards and in chat rooms, causing viewers of that message to send threatening messages back to the victim "author.")
- o Electronic communications technologies also lower the barriers to harassment and threats; a cyberstalker does not need to physically confront the victim.

While there are many similarities between offline and online stalking, the Internet and other communications technologies provide new avenues for stalkers to pursue their victims. A cyberstalker may send repeated, threatening, or harassing messages by the simple push of a button; more sophisticated cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal. California law enforcement authorities say they have encountered situations where a victim repeatedly receives the message "187" on their pagers – the section of the California Penal Code for murder. In addition, a cyberstalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message -- whether from the actual cyberstalker or others -- will have the intended effect on the victim, but the cyberstalker's effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender.

² Comparisons based on data currently available. The data for cyberstalking, as noted in the text of this report, is largely anecdotal and informal.

Actual Cyberstalking Incidents

- o In the first successful prosecution under California's new cyberstalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault. He faces up to six years in prison.
- o A local prosecutor's office in Massachusetts charged a man who, utilizing anonymous remailers, allegedly engaged in a systematic pattern of harassment of a co-worker, which culminated in an attempt to extort sexual favors from the victim under threat of disclosing past sexual activities to the victim's new husband.
- o An honors graduate from the University of San Diego terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The graduate student, who has entered a guilty plea and faces up to six years in prison, told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In fact, the victims had never met him.

The anonymity of the Internet also provides new opportunities for would-be cyberstalkers. A cyberstalker's true identity can be concealed by using different ISPs and/or by adopting different screen names. More experienced stalkers can use anonymous remailers that make it all-but-impossible to determine the true identity of the source of an e-mail or other electronic communication. A number of law enforcement agencies report they currently are confronting cyberstalking cases involving the use of anonymous remailers.

Anonymity leaves the cyberstalker in an advantageous position. Unbeknownst to the target, the perpetrator could be in another state, around the corner, or in the next cubicle at work. The perpetrator could be a former friend or lover, a total stranger met in a chat room, or simply a teenager playing a practical joke. The inability to identify the source of the harassment or threats could be particularly ominous to a cyberstalking victim, and the veil of anonymity might encourage the perpetrator to continue these acts. In addition, some perpetrators, armed with the knowledge that their identity is unknown, might be more willing to pursue the victim at work or home, and the Internet can provide substantial information to this end. Numerous websites will provide personal information, including unlisted telephone numbers and detailed directions to a home or office. For a fee, other websites promise to provide social security numbers, financial data, and other personal information.

Evidence suggests cyberstalking is a growing problem

Although there is no comprehensive, nationwide data on the extent of cyberstalking in the United States, some ISPs compile statistics on the number and types of complaints of harassment and/or threats involving their subscribers, and individual law enforcement agencies have compiled helpful statistics. There is, moreover, a growing amount of anecdotal and informal evidence on the nature and extent of cyberstalking.

First, data on offline stalking may provide some insight into the scope of the cyberstalking problem. According to the most recent National Violence Against Women Survey, which defines stalking as referring to instances where the victim felt a high level of fear:³

- In the United States, one out of every 12 women (8.2 million) and one out of every 45 men (2 million) have been stalked at some time in their lives.
- One percent of all women and 0.4 percent of all men were stalked during the preceding 12 months.
- Women are far more likely to be the victims of stalking than men – nearly four out of five stalking victims are women. Men are far more likely to be stalkers – 87 percent of the stalkers identified by victims in the survey were men.
- Women are twice as likely as men to be victims of stalking by strangers and eight times as likely to be victims of stalking by intimates.

In the United States, there are currently more than 80 million adults and 10 million children with access to the Internet. 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.⁴ Although such a “back of the envelope” calculation is inherently uncertain and speculative (given that it rests on an assumption about very different populations), it does give a rough sense of the potential magnitude of the problem.

Second, anecdotal evidence from law enforcement agencies indicates that cyberstalking is a serious – and growing – problem. At the federal level, several dozen matters have been referred (usually by the FBI) to U.S. Attorney’s Offices for possible action. A number of these

³ “Stalking in America: Findings from the National Violence Against Women Survey,” U.S. Department of Justice, Office of Justice Programs, and Department of Health and Human Services, Center for Disease Control and Prevention, April 1998 (available at www.usdoj.ojp).

⁴ The CyberAngels, a not-for-profit organization that assists victims of cybercrimes, including cyberstalking, using statistics from unspecified sources, estimates there are approximately 63,000 Internet stalkers and 474,000 victims worldwide. For additional information about this estimate, see the CyberAngels website at www.cyberangels.org.

cases have been referred to state and local law enforcement agencies because the conduct does not appear to violate federal law.

In addition, some local law enforcement agencies are beginning to see cases of cyberstalking. For example, the Los Angeles District Attorney's Office estimates that e-mail or other electronic communications were a factor in approximately 20 percent of the roughly 600 cases handled by its Stalking and Threat Assessment Unit. The chief of the Sex Crimes Unit in the Manhattan District Attorney's Office also estimates that about 20 percent of the cases handled by the unit involve cyberstalking. The Computer Investigations and Technology Unit of the New York City Police Department estimates that almost 40 percent of the caseload in the unit involves electronic threats and harassment -- and virtually all of these have occurred in the past three or four years.

Third, ISPs also are receiving a growing number of complaints about harassing and threatening behavior online. One major ISP receives approximately 15 complaints per month of cyberstalking, in comparison to virtually no complaints of cyberstalking just one or two years ago.

Finally, as part of a large study on sexual victimization of college women, researchers at the University of Cincinnati conducted a national telephone survey of 4,446 randomly selected women attending two- and four-year institutions of higher education. The survey was conducted during the 1996-97 academic year. In this survey, a stalking incident was defined as a case in which a respondent answered positively when asked if someone had "repeatedly followed you, watched you, phoned, written, e-mailed, or communicated with you in other ways that seemed obsessive and made you afraid or concerned for your safety." The study found that 581 women (13.1 percent) were stalked and reported a total of 696 stalking incidents; the latter figure exceeds the number of victims because 15 percent of the women experienced more than one case of stalking during the survey period. Of these 696 stalking incidents, 166 (24.7 percent) involved e-mail. Thus, 25 percent of stalking incidents among college women could be classified as involving cyberstalking.⁵

Current Efforts to Address Cyberstalking

The law enforcement response

⁵ Fisher, B. S., F. T. Cullen, J. Belknap, and M. G. Turner, "Being Pursued: Stalking Victimization in a National Study of College Women." (From a forthcoming report on sexual violence against college women funded by the US Department of Justice, National Institute of Justice).

Cyberstalking is a relatively new challenge for most law enforcement agencies. The first traditional stalking law was enacted by the state of California in 1990 – less than a decade ago. Since that time, some law enforcement agencies have trained their personnel on stalking and/or established specialized units to handle stalking cases. Nonetheless, many agencies are still developing the expertise and resources to investigate and prosecute traditional stalking cases; only a handful of agencies throughout the country have focused attention or resources specifically on the cyberstalking problem.⁶

Law enforcement response: awareness and training are key factors

Based on recent informal surveys of law enforcement agencies, it appears that the majority of agencies have not investigated or prosecuted any cyberstalking cases. However, some agencies – particularly those with units dedicated to stalking or computer crime offenses – have large cyberstalking caseloads. As noted above, the New York Police Department’s Computer Investigation and Technology Unit and the Los Angeles District Attorney’s Stalking and Threat Assessment Team estimate that 40 and 20 percent of their caseloads, respectively, involve cyberstalking-type cases.

“Cyberspace has become a fertile field for illegal activity. By the use of new technology and equipment which cannot be policed by traditional methods, 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

The disparity in the activity level among law enforcement agencies can be attributed to a number of factors. First, it appears that the majority of cyberstalking victims do not report the conduct to law enforcement, either because they feel that the conduct has not reached the point of being a criminal offense or that law enforcement will not take them seriously. Second, most law enforcement agencies have not had the training to recognize the serious nature of cyberstalking and to investigate such offenses. Unfortunately, some victims have reported that rather than open an investigation, a law enforcement agency has advised them to come back if the cyberstalkers confront or threaten them offline. In several instances, victims have been told by law enforcement simply to turn off their computers.

⁶ The information gathered on the issue of cyberstalking is largely anecdotal. It was gathered through informal surveys of state Attorneys General, U.S. Attorneys’ Offices, and, to a lesser extent, local prosecutors’ offices. Victim accounts were given voluntarily through outreach conducted by the Violence Against Women Office of the U.S. Department of Justice. In addition, the American Prosecutors Research Institute of the National District Attorneys’ Association compiled a report with background information on cyberstalking, which provided valuable information on current law enforcement efforts.

Law Enforcement: Lack of Training and Expertise Can Frustrate Victims, Hinder Response

A recent incident demonstrates how the lack of law enforcement training and expertise can frustrate cyberstalking victims: A woman complained to a local police agency that a man had been posting information on the web claiming that her nine-year-old daughter was available for sex. The web posting included their home phone number with instructions to call 24 hours a day. They received numerous calls. The couple reported the problem to the local police agency on numerous occasions, but the agency simply advised the couple to change their home phone number. Subsequently, the couple contacted the FBI, which opened an investigation. It was discovered that the local police agency did not have a computer expert, and the investigative officer had never been on the Internet. The local agency's lack of familiarity and resources may have resulted in a failure to understand the seriousness of the problem and the options available to law enforcement to respond to such problems.

Another indication that many law enforcement agencies underestimate the magnitude of the cyberstalking problem is the wide disparity in reported cases in different jurisdictions across the country. For example, one state attorney general's office in a midwestern state indicated that it received approximately one inquiry a week regarding cyberstalking cases and that it is aware of approximately a dozen prosecutions last year alone. In contrast, the state attorney general's offices in neighboring states indicated they have never received an inquiry into this type of behavior. Although one would generally expect some disparity in differing jurisdictions, the size of the disparity suggests that some law enforcement agencies do not have the training or expertise to recognize the magnitude of the problem in their jurisdictions.

Law enforcement response: jurisdictional and statutory limitations may frustrate some agencies

Some state and local law enforcement agencies also have been frustrated by jurisdictional limitations. In many instances, the cyberstalker may be located in a different city or state than the victim making it more difficult (and, in some cases, all but impossible) for the local authority to investigate the incident. Even if a law enforcement agency is willing to pursue a case across state lines, it may be difficult to obtain assistance from out-of-state agencies when the conduct is limited to harassing e-mail messages and no actual violence has occurred. A number of matters have been referred to the FBI and/or U.S. Attorney's offices because the victim and suspect were located in different states and the local agency was not able to pursue the investigation.

The lack of adequate statutory authority also can limit law enforcement's response to cyberstalking incidents. At least 16 states have stalking statutes that explicitly cover electronic

communications,⁷ and cyberstalking may be covered under general stalking statutes in other states. It may not, however, meet the statutory definition of stalking in the remainder. In many cases, cyberstalking will involve threats to kill, kidnap, or injure the person, reputation, or property of another, either on or offline and, as such, may be prosecuted under other federal or state laws that do not relate directly to stalking.

Finally, federal law may limit the ability of law enforcement agencies to track down stalkers and other criminals in cyberspace. In particular, the Cable Communications Policy Act of 1984 (CCPA) prohibits the disclosure of cable subscriber records to law enforcement agencies without a court order and advance notice to the subscriber. See 47 U.S.C. 551(c), (h). As more and more individuals turn to cable companies as their ISPs, the CCPA is posing a significant obstacle to the investigation of cybercrimes, including cyberstalking. For example, under the CCPA, a law enforcement agency investigating a cyberstalker who uses a cable company for Internet access would have to provide the individual notice that the agency has requested his/her subscriber records, thereby jeopardizing the criminal investigation. While it is appropriate to prohibit the indiscriminate disclosure of cable records to law enforcement agencies, the better approach would be to harmonize federal law by providing law enforcement access to cable subscriber records under the same privacy safeguards that currently govern law enforcement access to records of electronic mail subscribers under 18 U.S.C. 2703. Moreover, special provisions could be drafted to protect against the inappropriate disclosure of records that would reveal a customer's viewing habits.

Law enforcement response: the challenge of anonymity

Another complication for law enforcement is the presence of services that provide anonymous communications over the Internet. To be sure, anonymity provides important benefits, including protecting the privacy of Internet users. Unfortunately, cyberstalkers and other cybercriminals can exploit the anonymity available on the Internet to avoid accountability for their conduct.

Anonymous services on the Internet come in one of two forms: the first allows individuals to create a free electronic mailbox through a web site. While most entities that provide this service request identifying information from users, such services almost never authenticate or otherwise confirm this information. For these services, payment is typically made in advance through the use of a money order or other non-traceable form of payment. As long as payment is received in advance by the ISP, the service is provided to the unknown account holder. The second form comprises mail servers that purposefully strip identifying information and transport headers from electronic mail. By forwarding mails through several of these services serially, a stalker can nearly perfectly anonymize the message. The presence of both

⁷ These states are Alabama, Alaska, Arizona, California, Connecticut, Delaware, Hawaii, Illinois, Indiana, Maine, Massachusetts, Michigan, New Hampshire, New York, Oklahoma, and Wyoming. Arkansas and Maryland have enacted statutes that cover harassment via electronic communications outside their stalking statutes.

such services makes it relatively simple to send anonymous communications, while making it difficult for victims, providers, and law enforcement to identify the person or persons responsible for transmitting harassing or threatening communications over the Internet.

Law enforcement response: specialized units show promise in combating cyberstalking

A growing number of law enforcement agencies are recognizing the serious nature and extent of cyberstalking and taking aggressive action to respond. Some larger metropolitan areas, such as Los Angeles and New York, have seen numerous incidents of cyberstalking and have specialized units available to investigate and prosecute these cases. For example, Los Angeles has developed the Stalking and Threat Assessment Team. This team combines special sections of the police department and district attorney's office to ensure properly trained investigators and prosecutors are available when cyberstalking cases arise. In addition, this specialized unit is given proper resources, such as adequate computer hardware and advanced training, which is essential in investigating and prosecuting these technical cases. Similarly, the New York City Police Department created the Computer Investigation and Technology Unit. This unit provides regular training for police officers and prosecutors regarding the intricacies of cyberstalking investigations and prosecutions. The training includes understanding how chat rooms operate, how to obtain and preserve electronic evidence, and how to draft search warrants and subpoenas.

The programs in New York and Los Angeles both ensure that enforcement personnel receive proper training and have adequate resources to combat cyberstalking. Other jurisdictions are also taking steps to combat cyberstalking. One of the critical steps is learning how to trace communications sent over computers and the Internet. Traditional law enforcement techniques for surveillance, investigation, and evidence gathering require modification for use on computer networks and often require the use of unfamiliar legal processes. Law enforcement at all levels must be properly trained to use network investigative techniques and legal process while protecting the privacy of legitimate users of the Internet. These techniques are similar to those used in investigating other types of computer crime. Just as a burglar might leave fingerprints at the scene of a crime, a cyberstalker can leave an "electronic trail" on the web that properly trained law enforcement can follow back to the source. Thus, technological proficiency among both investigators and prosecutors is essential.

At present, there are numerous efforts at the federal and state levels that focus solely on high technology crimes. These units do not focus on cyberstalking alone, but they have the necessary expertise in computers and the Internet to assist in the investigation of cyberstalking when it arises. For example, the Federal Bureau of Investigation (FBI) has Computer Crime Squads throughout the country, as well as the National Infrastructure Protection Center in Washington, to ensure cybercrimes are properly investigated. Additionally, they have Computer Analysis and Response Teams to conduct forensics examinations on seized magnetic media. Similarly, in 1996 the Justice Department established the Computer Crime and Intellectual Property Section within the Criminal Division. These units have highly trained personnel who

remain on the cutting edge of new technology and investigative techniques. In addition, each U.S. Attorney's office contains experienced computer crime prosecutors. These individuals -- Computer and Telecommunications Coordinators -- assist in the investigation and prosecution of a wide variety of computer crimes, including cyberstalking. In addition, at the state level, several attorneys general have established special divisions that focus on computer crimes.

Although high-tech expertise is essential, police and prosecutors have developed other strategies for helping victims of cyberstalking. An Assistant U.S. Attorney reported that in two recent cases of e-mail harassment, he asked an FBI agent to confront the would-be harasser. The agent advised that such behavior might constitute a criminal offense. In both instances, the harassment stopped. Such strategies, however, are no substitute for prosecution under federal or state law in the appropriate circumstances.

A critical step in combating cyberstalking is understanding stalking in general. In many instances, cyberstalking is simply another phase in an overall stalking pattern, or it is regular stalking behavior using new, high-technology tools. Thus, strategies and techniques that have been developed to combat stalking in general often can be adapted to cyberstalking situations. Fortunately, many state and local law enforcement agencies have begun to focus on stalking, and some have developed special task forces to deal with this problem. In addition, the Attorney General submits an annual report to Congress entitled "Stalking and Domestic Violence." This report compiles valuable information about what the Department of Justice has learned about stalking and stalkers and is a valuable resource for law enforcement agencies and others.⁸

Cyberstalking is expected to increase as computers and the Internet become more popular. Accordingly, law enforcement at all levels must become more sensitive to cyberstalking complaints and devote the necessary training and resources to allow proper investigation and prosecution. By becoming technologically proficient and understanding stalking in general, agencies will be better prepared to respond to cyberstalking incidents in their jurisdictions. In addition, state and local agencies can turn to their local FBI or U.S. Attorney's office for additional technical assistance. Also, computer crime units and domestic violence units should share information and expertise, since many cyberstalking cases will include elements of both computer crime and domestic violence. Finally, law enforcement must become more sensitive to the fear and frustration experienced by cyberstalking victims. Proper training should help in this regard, but law enforcement at all levels should take the next step and place special emphasis on this problem. Computers and the Internet are becoming indispensable parts of America's culture, and cyberstalking is a growing threat. Responding to a victim's complaint by saying "just turn off your computer" is not acceptable.

Industry efforts

⁸ Copies of "Stalking and Domestic Violence: The Third Annual Report to Congress Under the Violence Against Women Act" can be obtained by contacting the National Criminal Justice Reference Service, Box 6000, Rockville, MD 20849-6000--(800) 851-3420.

Although the Internet industry has tried to combat abusive electronic communications overall, the industry as a whole has not addressed cyberstalking in particular. According to a review conducted as part of the preparation of the report, most major ISPs have established an address to which complaints of abusive or harassing electronic mail can be sent (generally, this address is “abuse@[the ISP's domain]” -- for example, “abuse@aol.com”). In addition, these providers almost uniformly have provisions in their online agreements specifically prohibiting abusive or harassing conduct through their service and providing that violations of the policy will result in termination of the account.

In practice, however, ISPs have focused more on assisting their customers in avoiding annoying online behavior, such as receiving unsolicited commercial electronic mail ("spamming") or large amounts of electronic mail intentionally sent to an individual ("mail-bombing"); relatively less attention has been paid to helping victims of cyberstalking or other electronic threats. For some ISPs, the procedures for lodging complaints of online harassment or threats were difficult to locate, and their policies about what does or does not constitute a violation of service agreements were generally unhelpful. In addition, many ISPs do not inform their customers about what steps, if any, the ISP has taken to follow-up on their customer's complaint. These problems — hard-to-locate complaint procedures, vague policies about what does and does not constitute prohibited harassment, and inadequate follow-up on complaints — may pose serious obstacles to cyberstalking victims who need help.

Online industry associations respond that providing such protection to their customers is costly and difficult. Although they recognize that larger ISPs have begun to commit resources to dealing with harassment online, they caution that the costs of imposing additional reporting or response obligations upon ISPs may make it difficult for small or entrepreneurial ISPs to continue providing service at competitive rates. For example, the Commercial Internet Exchange, whose members carry approximately 75 percent of U.S. backbone traffic, cautions that no attempt to impose reporting requirements should be made unless fully justified by the record. However, according to the same group, the decentralized nature of the Internet would make it difficult for providers to collect and submit such data. Accordingly, the evidence of the scope of the cyberstalking problem is likely to remain for the foreseeable future defined primarily by anecdotal evidence, with no basis to determine whether the phenomenon is growing, static, or declining.

Industry efforts: educating and protecting consumers

Despite the difficulty in fully defining the scope of the cyberstalking problem, however, industry has made notable efforts to inform consumers about ways to protect themselves online. Such information is principally focused on protecting children and consumers on the Internet. For example, since 1996, the Internet Alliance, one of the key Internet industry groups, has worked with the Federal Trade Commission and government agencies on Project OPEN (Online Public Education Network). Project OPEN provides information about fraud, parental controls,

and protecting privacy.⁹ Although this information is not specifically relevant to cyberstalking, much of the advice about protecting children and safeguarding privacy while online may be of assistance to individuals who want to use the Internet while protecting against potential cyberstalkers. More recently, a number of industry organizations have joined together to develop, GetNetWise.Com – a single, comprehensive online resource to help parents and children use the Internet in a safe and educational manner.

Other similar industry efforts have recently been announced to address other aspects of computer-related crime. For example, the Department of Justice and the Information Technology Association of America (ITAA) announced the Cybercitizen Partnership in March 1999. This partnership is intended to boost cooperation between industry and government, expand public awareness of computer crime issues among children and adolescents, and provide resources for government to draw upon in addressing computer crime. The industry has also responded to the complaints of parents who are worried about the content available to their children over the Internet by announcing the "One Click Away" initiative to give parents important information about protecting their children in a central location. Similar education and outreach efforts, approached through cooperation between industry and government, may educate individuals concerned about these issues and therefore mitigate some of the dangers of cyberstalking.

In addition, other Internet industry sectors have begun to address aspects of the cyberstalking problem. Many of these solutions focus on the ability of individuals to protect themselves against unwanted communications. For example, most Internet "chat" facilities offer users the ability to block, squelch, or ignore chat messages or "paging" from individuals who are attempting to annoy or threaten them. Similarly, many e-mail users have tools which allow the users to block e-mail from individuals who are attempting to harass or annoy them. Such a solution may be useful in situations where the communications are merely annoying. Unfortunately, such a solution is less appropriate when threatening communications are received, because a victim who never "receives" the threat may not know they are being stalked, and may be alerted, for the first time, when the stalker shows up to act on the threat.

In another type of response, providers have begun to set up "gated communities" for individuals, families, and children. The techniques used by such communities are still in developmental stages, but they range from specialized servers, which allow potentially objectionable content to be filtered at the server, to designated areas for children and teens, which place restrictions on the amount or types of personal information that will be provided to others. Individuals who are concerned about being stalked may find refuge in such communities.

While these efforts all reflect important initiatives for self-protection, both industry and government representatives agree that a key component of addressing the cyberstalking problem is education and empowerment: If individuals are given clear direction about how to protect

⁹ Other resources available to individuals wishing to protect themselves against cyberstalking are listed in Appendix I, [infra](#).

themselves against threatening or harassing communications, and how to report incidents when they do occur, both industry and law enforcement will be in a position to cooperate to conduct investigations.

Industry efforts: cooperation with law enforcement

Both industry and law enforcement benefit when crime over the Internet is reduced. In particular, the Internet industry benefits significantly whenever citizen and consumer confidence and trust in the Internet is increased. Accordingly, both industry and law enforcement recognize the need to cooperate more fully with one another in this area. Industry representatives have noted that contact between industry and law enforcement — particularly in the area of harassment — is sporadic and episodic. Industry representatives, who were consulted as part of the preparation of this report, indicated their willingness to participate in training efforts for law enforcement. Law enforcement — particularly on the state and local level, who will often be first responders to cyberstalking complaints — should be willing to engage industry in dialogue and take advantage of the expertise offered by industry in designing training programs. Moreover, closer cooperation between law enforcement and industry will help to ensure that law enforcement officers know who at the ISPs to call and how to proceed when they receive a complaint, and ISPs have a contact in law enforcement when they receive a complaint that warrants intervention by law enforcement.

Victims and support organizations

Because cyberstalking is a relatively new criminal phenomenon, very little public attention and resources have been committed to addressing this crime. Consequently, victims of online harassment and threats, often in collaboration with victim service providers and advocates, have had to step in to fill the void by developing their own informal support networks and informational web sites to exchange information about how to respond to these crimes effectively.

Victim service providers report that the Internet is rapidly becoming another weapon used by batterers against their victims. Just as in real life, abused women can be followed in cyberspace by their batterers, who may surreptitiously place their target under surveillance without her knowledge and use the information to threaten her or discredit her by putting misinformation on the Internet. Victim service providers recommend that victims make copies of all e-mails sent by the batterer as evidence of his stalking and advise a victim to let the stalker know that she does not want to have any further contact with him. SAFE House, a domestic violence victim service provider in Michigan, suggests that victims change their passwords often; refrain from telling anyone what the password is; do not use a password or other identifying information that the batterer/stalker can guess; set up a program that requires a password even to get on the computer; be sure to clear out the history information if programs such as ICQ, AOL Communicator, and Excite PAL, are used; remember that many chat rooms have archives that can be accessed later on by anyone; be careful about what is said in chat rooms and use an alias

that is only known to good friends; be aware that if the screen name of the assailant is known, he can be blocked from tracking victims through a buddy list on AOL; and, consult the ISP about the best way to secure their account.

A focus group convened on October 30, 1998, by the Office for Victims of Crime, a component within the U.S. Department of Justice, sought to identify the needs of stalking victims, including victims whose stalkers used the Internet to track and to harass their victims. The victims at the focus group emphasized that although the response of law enforcement and victim service providers is important, stalking victims need a wide range of services from doctors, mental health providers, day care providers, welfare and child protection workers, school staff, and employers. In addition, the focus group participants indicated that community awareness and understanding of what constitutes stalking behavior is critical to the support and well-being of stalking victims. Finally, all of the stalking victims reported that the consequences of not being believed or supported, or having their fears viewed as exaggerated or unrealistic, can be devastating. Some victims feel isolated and alone, are made to believe that the stalking is their fault, lose primary relationships, or fear losing their jobs. These issues are just as relevant to cyberstalking victims as they are to victims of offline stalking.

Adequacy of Existing Laws

Although stalking has been a problem for many years, only in this decade has it received significant attention from lawmakers, policy officials, and law enforcement agencies. In 1990, California became the first state to enact a specific stalking law. Since that time, all 50 states and the District of Columbia have enacted stalking laws.

State cyberstalking laws

Less than one third of the states have anti-stalking laws that explicitly cover stalking via the Internet, e-mail, pagers, or other electronic communications. California, for example, only recently amended its stalking statute to cover cyberstalking. This law was used in the prosecution of a 50-year-old former security guard who pleaded guilty on April 28, 1999, to one count of stalking and three counts of solicitation of sexual assault after using the Internet to solicit the rape of a woman who rejected his romantic advances. While the general stalking statutes in some states may cover cyberstalking, all states should review their laws to ensure they prohibit and provide appropriate punishment for stalking via the Internet and other electronic communications.

Federal cyberstalking laws

Federal law provides a number of important tools that are available to combat cyberstalking. Under 18 U.S.C. 875(c), it is a federal crime, punishable by up to five years in prison and a fine of up to \$250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Section 875(c) applies to any

communication actually transmitted in interstate or foreign commerce – thus it includes threats transmitted in interstate or foreign commerce via the telephone, e-mail, beepers, or the Internet.

Although 18 U.S.C. 875 is an important tool, it is not an all-purpose anti-cyberstalking statute. First, it applies only to communications of actual threats. Thus, it would not apply in a situation where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat). Also, it is not clear that it would apply to situations where a person harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person (as in the California case, discussed infra).

Certain forms of cyberstalking also may be prosecuted under 47 U.S.C. 223. One provision of this statute makes it a federal crime, punishable by up to two years in prison, to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number.¹⁰ The statute also requires that the perpetrator not reveal his or her name. See 47 U.S.C. 223(a)(1)(C). Although this statute is broader than 18 U.S.C. 875 — in that it covers both threats and harassment -- Section 223 applies only to direct communications between the perpetrator and the victim. Thus, it would not reach a cyberstalking situation where a person harasses or terrorizes another person by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person. Moreover, Section 223 is only a misdemeanor, punishable by not more than two years in prison.

The Interstate Stalking Act, signed into law by President Clinton in 1996, makes it a crime for any person to travel across state lines with the intent to injure or harass another person and, in the course thereof, places that person or a member of that person's family in a reasonable fear of death or serious bodily injury. See 18 U.S.C. 2261A. Although a number of serious stalking cases have been prosecuted under Section 2261A, the requirement that the stalker physically travel across state lines makes it largely inapplicable to cyberstalking cases.

Finally, President Clinton signed a bill into law in October 1998 that protects children against online stalking. The statute, 18 U.S.C. 2425, makes it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity. While this new statute provides important protections for children, it does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes.

¹⁰ The definition of the term "telecommunications device" in that section excludes "interactive computer services." The intent of the exclusion is to insulate the service provider from liability, but not to insulate an individual user from liability for his or her criminal behavior. Accordingly, the Department of Justice has taken the position and successfully argued that a modem was a telecommunications device within the meaning of the statute. Therefore, an individual who used a modem to connect to the Internet and harass an individual is likely to fall within the terms of the statute. See American Civil Liberties Union v. Reno, 929 F.Supp. 824, 829 n.5 (E.D. Penn. 1996), aff'd, 521 U.S. 844 (1997); Apollomedia Corporation v. Reno, 19 F.Supp.2d 1081 (N.D. Cal. 1998), aff'd, --- U.S. --, 119 S.Ct. 1450 (U.S. Apr. 19, 1999).

Thus, although current statutes address some forms of cyberstalking, there are gaps in current federal and state law. As outlined in the Recommendations below, States should review their existing stalking and other statutes to determine whether they address cyberstalking and, if not, expeditiously enact laws that prohibit cyberstalking.

Federal legislation also is needed to fill the gaps in current law. While most cyberstalking cases will fall within the jurisdiction of state and local authorities, there are instances – such as serious cyberharassment directed at a victim in another state or involving communications intended to encourage third parties to engage in harassment or threats – where state law is inadequate or where state or local agencies do not have the expertise or the resources to investigate and/or prosecute a sophisticated cyberstalking case. Therefore, federal law should be amended to prohibit the transmission of any communication in interstate or foreign commerce with intent to threaten or harass another person, where such communication places another person in fear of death or bodily injury to themselves or another person. Because of the increased vulnerability of children, the statute should provide for enhanced penalties where the victim is a minor. Such targeted, technology-neutral legislation would fill existing gaps in current federal law, without displacing the primary law enforcement role of state and local authorities and without infringing on First Amendment-protected speech.

First Amendment and Other Legal Considerations

All 50 States, the District of Columbia, and the federal government have passed laws that criminalize stalking to address the serious harms and dangers that result from stalking, including the fear of violence and loss of privacy and control suffered by the victim. In addition to the direct harms caused by stalking, stalking is also frequently a precursor to physical violence against the victim. By its nature, however, stalking is not a crime that can be defined with a particularized, discrete set of acts. Frequently stalking consists of a course of conduct that may involve a broad range of harassing, intimidating, and threatening behavior directed at a victim. The conduct can be as varied as the stalker's imagination and ability to take actions that harass, threaten, and force himself or herself into the life and consciousness of the victim. As new technologies become available, stalkers adapt those technologies to new ways of stalking victims, as is the case with the Internet and cyberstalking.

As a result of the breadth of conduct potentially involved in stalking, anti-stalking statutes need to be relatively broad to be effective. At the same time, however, because of that breadth and because stalking can involve expressive conduct and speech, anti-stalking statutes must be carefully formulated and enforced so as not to impinge upon speech that is protected by the First Amendment. This is particularly true with regard to cyberstalking laws, which frequently will involve speech over the Internet. The Internet, moreover, has been recognized as an important tool for protected speech activities. See, e.g., 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).

The fact that stalking behavior (including cyberstalking) may implicate important issues of free speech, however, does not eliminate the significant public interest in its criminal regulation or suggest that any criminal regulation would be prohibited by the freedom of speech guarantees of the First Amendment. The First Amendment does not prohibit any and all regulation that may involve or have an impact on speech. Of particular relevance to stalking, the Supreme Court has recognized that governments may criminalize true threats without violating the First Amendment. See, e.g., Watts v. United States, 394 U.S. 705 (1969) (per curiam). As discussed in the Introduction of this report, stalking (as well as cyberstalking) generally involves conduct reasonably understood to constitute a threat of violence, and such threats may be criminalized consistent with the First Amendment.

One of the recommendations in this report calls on states to review and update their statutes, where necessary, to cover electronic communications within their stalking laws. Care must be taken in drafting cyberstalking statutes to ensure that they are not so broad that they risk chilling constitutionally protected speech, such as political protest and other legitimate conduct. A carefully drafted statute can provide broad protections against cyberstalking without running afoul of the First Amendment.

Recommendations

General recommendations

- The law enforcement community, private industry, victims assistance providers, and individuals must recognize that cyberstalking is a serious problem -- not only as a potential precursor to offline threats and violence, but also as a serious invasion of an increasingly important aspect of people's everyday lives. At the same time, it is important to note that many forms of annoying and menacing activity on the Internet do not rise to the level of illegal activity and are properly addressed by individuals and service providers without recourse to law enforcement channels.
- The lack of comprehensive data on the nature and extent of cyberstalking makes it difficult to develop effective response strategies. Future surveys and research studies on stalking should, where possible, include specific information on cyberstalking. Industry organizations can and should play a role not only in increasing the amount of data on the cyberstalking problem, but also ensuring that the data can be analyzed in a meaningful way.

Legislative recommendations

- States should review their existing stalking and other statutes to determine whether they address cyberstalking and, if not, promptly expand such laws to address cyberstalking.
- Although State and local law enforcement agencies should retain primary jurisdiction over cyberstalking cases, federal law should be amended to address gaps in existing law where the conduct involves interstate or foreign communications. Such legislation should prohibit the transmission of any communication in interstate or foreign commerce with intent to threaten or harass another person where such communication places another in reasonable fear of death or bodily injury. Enhanced penalties should be available where the victim is a minor. Such legislation should be technology neutral and should apply to all forms of communication technologies.
- Federal law also should be amended to make it easier to track down stalkers and other criminals in cyberspace while maintaining safeguards for privacy. In particular, the Cable Communications Policy Act should 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 under 18 U.S.C. 2703 (while maintaining strict limits on access to records that reveal customer viewing habits).

Recommendations for law enforcement and criminal justice officials

- Law enforcement agencies and courts need to recognize the serious nature of cyberstalking, including the close links between offline and online stalking.
- Law enforcement agencies need training on the nature and extent of the cyberstalking problem, including specific training on the legal tools available to address the problem, the need for, and effectiveness of, prompt action by law enforcement agencies, the most effective techniques to investigate and prosecute cyberstalking crimes, and the resources available to cyberstalking victims.
- Law enforcement agencies with existing stalking or computer crime units should consider expanding the mission of such units to include cyberstalking, and law enforcement agencies that do not presently have a stalking section should consider expanding their capabilities to address this issue. At the least, law enforcement agencies should understand the patterns underlying stalking in general and be prepared to respond and intercede on behalf of cyberstalking victims.
- Law enforcement agencies should use mechanisms for quickly and reliably sharing information about cyberstalking incidents with other law enforcement agencies, thereby making it less likely that a cyberstalker can continue threatening behavior simply because neither the jurisdiction of the sender nor the jurisdiction of the victim believes that it can prosecute the offender.
- U.S. Attorneys' Offices, in consultation with other federal, state and local agencies, should examine the available resources and networks of investigators and prosecutors with the expertise to handle cyberstalking investigations. These include violent crime specialists, computer crime investigators and prosecutors, computer forensic specialists, and victim-witness coordinators, among others. The Law Enforcement Coordinating Committees, which have been established in each U.S. Attorneys' Office and are designed to foster coordination among law enforcement agencies, would be an appropriate body for addressing these issues.
- Law enforcement agencies should work more closely with victim groups to identify cyberstalking patterns and victims' experiences and to encourage cyberstalking victims to report incidents to law enforcement authorities.

Recommendations for the Internet and electronic communications industry

The Internet and electronic communications industry should --

- Create an industry-supported website containing information about cyberstalking and what to do if confronted with this problem. Contact information for the major ISPs should be included so that Internet users can easily report cyberstalking cases after visiting this centralized resource. This recommendation could be implemented by expanding the “One Click Away” initiative or through a complementary but separate initiative focused on cyberstalking.
- Develop additional means to empower individuals to protect themselves against cyberstalking. Such means might include more accessible and effective filtering and blocking options. While some major ISPs already allow such options, others do not.
- Develop training materials designed specifically to assist law enforcement in the investigation and prosecution of cyberstalking and related crimes. For example, a short training video could be developed to increase awareness of the cyberstalking problem and to provide law enforcement officers with essential information on how to work with ISPs and others in the investigation of cyberstalking cases.
- Cooperate fully with law enforcement when investigating cyberstalking complaints. The industry can do this, for example, by immediately freezing and retaining data for law enforcement use on any potential cyberstalking case.
- Establish best business practices to address illicit activity by terminating holders of fraudulent accounts.
- Sponsor an Internet Security and Law Enforcement Council of ISPs and other members of the Internet community to develop and promote industry best business practices relating to security and law enforcement issues (including cyberstalking), develop and distribute training materials for law enforcement on the investigation and prosecution of Internet crime, and promote more effective communication and cooperation between industry and law enforcement in combating online criminal activity.
- Establish and enforce clear policies that prohibit cyberstalking and related behaviors, including the termination of accounts for persons who violate such policies. While it appears that most of the larger ISPs have such policies, some smaller ISPs do not. Representatives from the Internet industry should consider establishing an industry-wide code of conduct that encourages all ISPs to adopt such procedures.

- Establish clear and understandable procedures for individuals – both customers and non-customers – to register complaints about individuals using the company’s service to engage in cyberstalking. Such procedures should be easily accessible to individuals.
- Develop and widely disseminate educational materials to customers and others on how to protect themselves online.

Recommendations for victim service providers and advocates

Victim service providers and advocates should --

- Provide direct services and referrals to available resources that are specifically designed to assist victims of cyberstalking, or stalking in general where cyberstalking services are not available, and work to ensure that cyberstalking services are expanded to meet the needs of victims and enhance their safety;
- Train domestic violence and other victim service providers and advocates on Internet technology, the tactics used by cyberstalkers, and how to respond to the specific needs of cyberstalking victims;
- Name the behavior as cyberstalking and validate that a crime is occurring when working with individual victims;
- Serve as catalysts in community efforts to form partnerships among law enforcement, prosecution, the judiciary, the medical community and other community allies to address the specific safety needs of cyberstalking victims and hold offenders accountable for their actions;
- Raise public awareness about the devastating impact on cyberstalking victims of the tactics used by cyberstalkers and the steps that can be taken to prevent and combat this crime; and
- Inform public policy decision making.

Appendix I: Cyberstalking Resources Online

CyberAngels: Non-profit group devoted to assisting victims of online harassment and threats, including cyberstalking. www.cyberangels.org.

GetNetWise: Online resource for families and caregivers to help kids use the Internet in a safe and educational manner. Includes a guide to online safety, a directory of online safety tools, and directions for reporting online trouble. www.getnetwise.org.

International Association of Computer Investigative Specialists: IACIS is an international volunteer non-profit corporation composed of law enforcement professionals dedicated to education in the field of forensic computer science. IACIS offers professional training to law enforcement agencies in a wide range of computer crime investigative techniques, provides an opportunity to network with other law enforcement officers trained in computer forensics, and promotes research and development of specialized hardware and software to assist computer forensic professionals. www.iacis.com.

National Center for Victims of Crime: The National Center for Victims of Crime (formerly known as the National Victim Center) provides referrals and advocacy services to victims through its toll-free national hotline. Through the hotline, victims are referred to the nearest, appropriate services in their community, including crisis intervention, assistance with the criminal justice process, and counseling and support groups. The National Center publishes bulletins on a number of topics, including domestic violence, sexual assault, and stalking. www.ncvc.org.

National Cybercrime Training Partnership: This interagency, federal/state/local partnership, led by the Department of Justice with extensive support from the Office of Justice Programs and the National White Collar Crime Center, is developing and delivering training to federal, state and local law enforcement agencies on the investigation and prosecution of computer crime. Information about the partnership can be found through the NWCCC website: www.cybercrime.org.

Privacy Rights Clearinghouse: Nonprofit consumer information and advocacy program that offers consumers a unique opportunity to learn how to protect their personal privacy. PRC's services include a hotline for consumers to report privacy abuses and request information on ways to protect their privacy, fact sheets on privacy issues, including one entitled "Are You Being Stalked? Tips For Your Protection." www.privacyrights.org.

Search Group, Inc.: SEARCH, the National Consortium for Justice Information and Statistics, provides assistance to state and local criminal justice agencies on a wide variety of information technology issues. SEARCH, through its National Technical Assistance and Training Program, provides comprehensive, hands-on training on computer crime investigations at its headquarters in Sacramento, CA, and at regional training sites around the country. www.search.org.

Women Halting Online Abuse (WHOA): Founded by women to educate the Internet community about online harassment, WHOA empowers victims of online harassment and develops voluntary policies that systems administrators can adopt to create an environment free of online harassment. WHOA educates the online community by developing website resources, including the creation of a safe-site and unsafe-site list to enable users to make informed decisions, and providing information about how users can protect themselves against harassment. whoa.femail.com.

Appendix II: How You Can Protect Against Cyberstalking – And What To Do If You Are A Victim

Prevention Tips

- * Do not share personal information in public spaces anywhere online, nor give it to strangers, including in e-mail or chat rooms. Do not use your real name or nickname as your screen name or user ID. Pick a name that is gender- and age-neutral. And do not post personal information as part of any user profiles.
- * Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.
- * Make sure that your ISP and Internet Relay Chat (IRC) network have an acceptable use policy that prohibits cyberstalking. And if your network fails to respond to your complaints, consider switching to a provider that is more responsive to user complaints.
- * If a situation online becomes hostile, log off or surf elsewhere. If a situation places you in fear, contact a local law enforcement agency.

What To Do If You Are Being Cyberstalked

- * If you are receiving unwanted contact, make clear to that person that you would like him or her not to contact you again.
- * Save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with Internet system administrators or law enforcement officials.
- * You may want to consider blocking or filtering messages from the harasser. Many e-mail programs such as Eudora and Microsoft Outlook have a filter feature, and software can be easily obtained that will automatically delete e-mails from a particular e-mail address or that contain offensive words. Chat room contact can be blocked as well. Although formats differ, a common chat room command to block someone would be to type: /ignore <person's screen name> (without the brackets). However, in some circumstances (such as threats of violence), it may be more appropriate to save the information and contact law enforcement authorities.
- * If harassment continues after you have asked the person to stop, contact the harasser's Internet Service Provider (ISP). Most ISP's have clear policies prohibiting the use of their services to abuse another person. Often, an ISP can try to stop the conduct by direct contact with the stalker or by closing their account. If you receive abusive e-mails, identify the domain (after the "@" sign) and contact that ISP. Most ISP's have an e-mail address such as abuse@<domain name> or postmaster@<domain name> that can be used for complaints. If the ISP has a website, visit it for information on how to file a complaint.
- * Contact your local police department and inform them of the situation in as much detail as possible. In appropriate cases, they may refer the matter to state or federal authorities. If you are afraid of taking action, there are resources available to help you. Contact either:
 - The National Domestic Violence Hotline, 800-799-SAFE (phone); 800-787-3224 (TDD)
 - A local women's shelter for advice and support.