Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace

Michael G. McGrath, MD, and Eoghan Casey, MA

The growth of the Internet has revolutionized how society conducts business in many areas. Not to be left behind, the sexual predator and the obsessional harasser have found cyberspace to be a vehicle capable of meeting their needs: obtaining information, monitoring and contacting victims, developing fantasy, overcoming inhibitions, avoiding apprehension, and communicating with other offenders. Although clearly disparate offender categories, these two groups are included in this article because of the likelihood of their using the Internet in pursuit of their goals. Forensic psychiatrists should become familiar with computers and the Internet so that they can conduct relevant psychiatric evaluations of such individuals and can advise attorneys, victims, and law enforcement personnel competently, when retained in that capacity. This article discusses the Internet and its use by the sexual predator and the obsessional harasser, highlighting information of interest to the forensic psychiatrist, including the poorly understood field of digital evidence. Aspects of the Internet, such as on-line dating and cybersex also are covered, because they relate to sexual predation and stalking.

J Am Acad Psychiatry Law 30:81–94, 2002

The Internet has affected most aspects of our lives, and its ongoing development indicates that it will continue to do so. Those unwilling to venture into its virtual domain (i.e., cyberspace) will surely be at a disadvantage. The digital revolution has affected psychiatry (for better or for worse) in many ways, from e-mailing information regarding patients to on-line therapy.[1,2] Although psychiatrists in general are well advised to become familiar with computers and the Internet to enhance their understanding of patients who are using this technology, forensic psychiatrists may have more of an incentive, because the behavior of those they evaluate may include activities in cyberspace.

Dr. McGrath is Associate Chair, Department of Psychiatry and Behavioral Health, Unity Health System, Rochester, NY, and Clinical Assistant Professor of Psychiatry, University of Rochester School of Medicine and Dentistry, Rochester, NY. Mr. Casey is System Security Administrator at Yale University, New Haven, CT, and a partner in Knowledge Solutions, LLC, Watsonville, CA. The views expressed in this article are those of the authors and do not necessarily reflect those of University Health System, University of Rochester School of Medicine and Dentistry, or Yale University. Address correspondence to: Michael McGrath, MD, 81 Lake Avenue, Rochester, NY 14608. E-mail: mmcgrath@profiling.org

At the very least, forensic psychiatrists should be able to determine what need the Internet fulfills for a given individual, be it anonymity, information about victims, access to victims, or something else. Forensic psychiatrists, if so inclined, can search for an individual's statements and actions on the Internet and compare these with in-person interviews for contradictions. Furthermore, individuals express thoughts and desires on the Internet that they would otherwise keep secret, giving insight into, for example, their fantasies, insecurities, and alter egos.[3] In addition, by recording the interactions between offenders and victims, the Internet offers psychiatrists and other investigators a rare insight into offender-victim interaction and grooming, concealment, and power-assertion behavior. Few crimes enable clinicians to witness offender-victim interaction first hand. In addition to police and victim reports and interviews with offenders, on-line transcripts of conversations and exchanges between offender and victim can only assist a forensic psychiatrist in forming reliable opinions. In addition, a basic knowledge of digital evidence can only benefit the forensic psychiatrist when

consulting on cases in which computers, computer systems, and the Internet are involved. In this article, we explore these subjects and attempt to stimulate discussion in this rapidly evolving area and to provide a stimulus that will ultimately lead to research related to offenders and their use of the Internet.

It should be noted that the authors are not suggesting that forensic psychiatrists should become experts on computers and the Internet so that they can spend their time searching for digital evidence of crimes. Rather, they should educate themselves about the medium and take advantage of it when appropriate. Actual collection of such information is best left to computer experts, but it will be the educated practitioner who knows to ask whether such information has been collected or even sought.

Just What Is the Internet?

The Internet is a collection of interconnected computer networks that facilitates human interaction of all sorts in a place that has come to be called "cyberspace," a term coined by William Gibson in his 1984 science fiction novel *Neuromancer*[4] to describe the virtual space in which computer-based activity occurs. Internet crime occurs "on" the Internet, but "in" cyberspace.[5]

Computers connected to the Internet, generally referred to as hosts, communicate using a set of protocols, collectively called TCP/IP (transport control protocol/Internet protocol). Hosts that provide a service to other computers on a network are commonly called servers, and hosts that access these servers are called clients. Any host, even a personal computer in someone's home, can become a server. All an individual has to do is install a piece of software. Some servers allow anyone to access their resources without restrictions (e.g., Web servers), whereas others (e.g., e-mail servers) allow access to authorized individuals only, usually requiring a user identifier and password.

Every host on the Internet is assigned a unique number, an Internet protocol (IP) address, to distinguish it from other hosts. Before packets of data are sent through the Internet, they are addressed using the IP address of the destination computer, much like an envelope is addressed before it is submitted to a postal system. Routers use these IP addresses to direct information through the Internet to its destination.

There are thousands of programs that allow people to use the Internet in different ways—virtual vehicles on the information superhighway. Also, value-added networks such as America Online (AOL) offer customers a range of services in addition to Internet access. Finally, there is significant growth in wireless networking, bringing the power of the Internet to handheld devices. A basic understanding of the Internet is needed to appreciate how and why people are able to interact with others on-line with varying degrees of anonymity and safety. For the sake of brevity, only the main services are considered here: e-mail, newsgroups, on-line chat, and the World Wide Web. Knowledge of these services can offer some insight into how criminals and investigators use them and how they can be useful to forensic psychiatrists.

Most persons are already familiar with e-mail, a service that enables people to send electronic messages to each other. Few realize that it is quite simple to falsify an e-mail message, to obfuscate the sender's identity, or to pose as someone else. Fortunately for investigators, every e-mail message has a header that contains information about its origin and destination.[6] Even if a header is forged, it can contain information identifying the sender or can be used to locate the computer that generated the message.

To counterbalance the invasion of privacy that can result from the disclosure of such personal information, anonymous remailers[7] (services that forward e-mail after stripping all identifying information) are available to conceal the sender's identity. Victims of abuse often use anonymous remailers when participating in on-line support groups, and some criminals use remailers when contacting victims. Although remailers may have log files that can be used to trace a message to its source, it can be very difficult to obtain such logs, and some remailers purposely discard such information. As people become concerned with privacy on the Internet, more comprehensive privacy protection services[8] have been made available, such as Freedom,[9] that are capable of rendering anonymous all of an individual's Internet activities, not just e-mail.

Newsgroups are the on-line equivalent of public bulletin boards, enabling asynchronous communication that often resembles a discussion. Anyone with Internet access can post a message on these bulletin boards and return later to see whether someone has replied. Most newsgroups are part of a cost-free, global system called the User's Network (also known

as Usenet[10]) begun in 1979. There are archives, (e.g., Deja.com[11], Supernews[12]) containing millions of messages from tens of thousands of newsgroups. These archives are potential tools for forensic psychiatrists, because they contain extensive and detailed information about individuals and their interactions. Aside from their content, newsgroup messages have headers containing information about the sender and the journey that the message took. As with e-mail, the sender can modify the header or use an anonymous posting service to make identification more difficult.

Although it may be tempting to rely on Usenet archives because of the convenience, it can be fruitful to monitor newsgroups actively that may contain information related to a case. Usenet archives do not contain everything that has been posted, with most archives storing only a few years worth of material. Some archives do not retain message headers that can be used for tracking purposes and do not store images or other large attachments, and individuals can opt out of newsgroup archiving mechanisms by setting a flag (a computer rule to avoid archiving) in their messages. Even if a newsgroup does not contain information that is directly relevant, the discussion can improve a forensic psychiatrist's understanding of the individuals involved. Particularly, monitoring newsgroups activity can give forensic psychiatrists information that can help them understand the motivation and behavior of victims and offenders in a given type of crime (e.g., cyberstalking, solicitation of minors, and producing and distributing child pornography).

On-line chat networks comprise chat rooms, sometimes called channels, where people with similar interests gather. By connecting to a chat network such as Internet Relay Chat (IRC),[13] individuals can interact in real time, using text, audio, video, and more. Many chat rooms are open to all, but users can create their own private areas, and some chat programs allow users to initiate a direct connection with each other, bypassing the chat network altogether. The privacy, immediacy, and transient nature of synchronous chat networks make them particularly conducive to criminal activity, allowing predators to obtain victims immediately with little fear of detection by authorities. Because on-line chat communications are rarely archived on central servers as with e-mail and Usenet, investigators must be in the right place at the right time to observe a conversation or must find a transcript of the conversation saved by one of the participants. Ironically, these investigative challenges make on-line chat networks a valuable investigative tool. Forensic psychiatrists can learn a surprising amount from the activities observable in on-line chat rooms, because many offenders are at ease and disclose more than they would in a face-to-face meeting.

The World Wide Web, usually referred to as the Web, first became publicly available in 1991 and has become so popular that it is often mistakenly referred to as the Internet. This is not surprising, because many older Internet services, including e-mail, Usenet, and on-line chat, are now accessible through the Web. Because the Web contains so much loosely ordered information, searching for something in particular can be like looking for a needle in a haystack. Criminals, investigators, and forensic psychiatrists alike can learn a significant amount about an individual or a specific topic (e.g., bondage, sadomasochism) using search engines such as AltaVista[14] and Hotbot.[15] Although search engines are not especially difficult to use, there is some skill involved. Each search engine has different contents, archiving methods, and search features. Some programs (e.g., Copernic[16]) search the Internet using multiple search engines and present a summary of what they decide are the most pertinent Web sites or addresses.

There are many other programs that enable persons to use the Internet in a number of ways. In addition to commonly used services such as e-mail, newsgroups, on-line chat networks, and the World Wide Web, there are powerful programs, such as ICQ,[17] Napster,[18] Freenet,[19] and Hotline,[20] that enable individuals to interact and share all forms of media.

Internet as Opportunity

As with any new technology, the Internet allows for improvement in conducting both legal and illegal activities. For example, in addition to the mail and the telephone, which are often used to make threats, such communications are now being relayed over the Internet. Despite the technological changes, the intent of such acts remains the same: disruption or inducement of fear. In 1998 a Spanish teenager e-mailed a bomb threat to a local library threatening an explosion if $170,000 was not paid. The e-mail message was traced to the 15-year-old boy's e-mail address at a computer science school.[21] A University of Iowa student admitted to sending a bomb threat via

e-mail as well as several racist e-mail threats. The messages were tracked back to a computer in a campus building, and a hidden camera was installed to determine who was sending the messages.[22] A Canadian man was convicted in U.S. federal court in April 1999 of sending threatening e-mail messages to federal judges and Microsoft Chairman Bill Gates.[23] The messages were traced back to the sender, despite his efforts to conceal his identity.[24]

As becomes obvious, the technology did not cause the illegal behavior (in the same way that the invention of the automobile did not cause teenage sex); it simply facilitated it by creating more opportunities. Any technological advance has been followed by ways in which criminals have used it to their advantage. A burglar who used to operate near home and take small items, could (with a car) go farther from home and transport more stolen goods. As with innovations in transport, the evolution of the Internet will create opportunities for ambitious criminals, but the underlying motivations for illegal activity in cyberspace will remain those of crime in the physical world.

The Internet is especially appealing to the sexual predator and the obsessional harasser for several reasons. Because such criminals depend heavily on information, cyberspace is an ideal environment, giving them access to a great deal of information about a large pool of potential targets. Unless one is willing to engage a private investigator, without the Internet, an individual's ability to gather information is usually limited to celebrities, prior relationships, and those nearby. The Internet effectively erases these limitations, supplying sophisticated search tools and many newsgroups and chat rooms organized by topic, providing a veritable menu of hunting grounds. One offender might search the Web for potential victims who are involved with church groups or on-line Bible discussions. Another offender might search for potential victims of a specific age by sifting through personal Web pages or AOL user self-descriptions. Sexual predators can lurk in a Usenet newsgroup dedicated to victims of abuse (e.g., alt.abuse.recovery) or may choose a particular on-line venue because it attracts potential victims who are located geographically near them.

The Internet also enables offenders to monitor potential or existing victims on several levels, ranging from participating in a discussion forum and becoming familiar with the other participants, to searching the Internet for related information about an individual, to accessing a potential victim's personal computer to gain additional information. Many people are not aware, but it may be possible to determine when a person enters cyberspace. For instance, services such as ICQ and AOL Instant Messenger can be configured to sound an alert on the offender's computer when a particular individual connects to the Internet. Also, many computers connected to the Internet provide information about the individual who owns or is using the computer. Many people use their proper names when configuring a computer, effectively exposing their identity to anyone on the Internet who cares to query their personal computer.

In addition to querying a computer for information as described, there are ways to gain unauthorized access to any computer on the Internet and to search the owner's hard drive. For example, a sexual predator or an on-line stalker might send a potential victim an amusing computer animation as an e-mail attachment that surreptitiously installs a Trojan horse program (e.g., Back Orifice,[25] Netbus,[26] or SubSeven[27]) giving the predator complete remote control of the victim's computer. In addition to accessing the computer's hard drive, the offender can monitor the victim's very keystrokes and screen.

Although surreptitiously monitoring a victim while he or she is on-line increases the risk of detection and apprehension, it gives an offender more information and contact with the victim and can fuel voyeuristic fantasies and feed an offender's need for a feeling of power over the victim. Such monitoring is possible in the physical world (e.g., prowling at a playground, following a victim, or peeking in a bedroom window), but can be a high-risk behavior for the offender, whereas monitoring someone on the Internet is a comparatively low-risk activity. In addition to the physical distance that the Internet introduces between a victim and an offender, few victims have the technical sophistication to determine that an offender is monitoring their activities, even if the offender is accessing the victim's computer with a Trojan horse program. Furthermore, the Internet provides offenders with many opportunities to alter or conceal their identities.

Once a sexual predator or obsessional harasser decides to target a specific individual, the offender must decide whether to conceal his or her identity, alter his or her on-line persona for a desired effect, or present himself or herself openly. This decision can depend

on the risk perceived by the offender and his or her skill level. Sexual predators may not hide their identities if they believe they are doing nothing wrong and/or feel protected by the physical separation the Internet provides. Sexual predators who are aware that their activities are illegal and understand that the Internet does not offer inherent protection will make an effort to conceal their identities and locations. Alternately, sexual predators may not want to disclose their identities to victims who know them in the physical world and may have the skill to shield their identities on the Internet.

The ability of stalkers and sexual predators to acquire victims, gather information, lurk in cyberspace, and protect their identities makes the Internet an attractive setting for these individuals, although at times the lack of technological sophistication displayed by offenders is surprising. Some offenders apparently are not aware that it is quite easy to locate them, and they make very little effort to conceal basic information on the Internet. Offenders who do not initially hide their identities may do so once they realize they are at risk. Thus, it may be possible to use the Internet's archiving capabilities to find information on an individual before the covering behavior commences. Many individuals use near-unique words, phrases, nicknames, or signatures that can stick out like a rough edge. Searching for other occurrences of such rough edges can lead to the identity of the offender, somewhat akin to the way in which linguistic evidence is sometimes used to ascribe authorship between documents.

Fantasy Versus Reality: Internet as Crime Catalyst

One aspect of the Internet cannot be overemphasized: the apparent anonymity combined with the lack of face-to-face (or even voice-to-voice) contact can easily lead to a loss of normal social inhibitions and constraints. By reducing disincentives such as embarrassment and apprehension, the Internet can encourage individuals to engage in dialogue and commit acts that they would otherwise only consider and allow the victim (and the offender) to become quickly "intimate" with someone he or she does not know. Just as the voyeur is emboldened in the dark, some exhibit behavior on-line that they would hide in everyday life.[28] The increased sense of safety provided by the Internet may embolden the voyeur to graduate from watching to the on-line equivalent of cyber-exposing or cyber-fondling and may encourage some offenders to contact victims rather than remain silent and observe from a distance. In addition, the Internet provides support groups for previously isolated sexual predators, support that has the potential to encourage some individuals to act on fantasies that would otherwise remain dormant.[29]

By reducing disincentives, the Internet effectively dissolves the boundaries between fantasy and reality, enabling individuals to explore and realize their fantasies. A man who would never approach a child in the real world may make such contact in cyberspace just to see what might happen. A Disney executive established a friendship with a cyber correspondent who he thought was a 13-year-old girl in an on-line chat room titled "Dad&DaughterSex," a place one would hardly enter unwittingly. He claimed he thought the person was really an adult and that they were both merely playing out a fantasy.[30] It is clear that Internet behavior can differ dramatically from behavior in the physical world. Sharon Lopatka, a wife and owner of three Web sites, left her Maine home and traveled to North Carolina to meet a man with whom she had communicated over the Internet. E-mail messages left on her computer indicated she went to meet the man specifically to have rough sex and be killed. Whether she actually wanted to be killed, or was acting out a sadomasochistic fantasy, she was strangled three days after she met up with the man, and her body was buried in a shallow grave.[31] Seemingly low-risk victims can, because of the ease of communication and lowered on-line inhibitions, become high-risk victims.

By reducing the available sensory information, the Internet facilitates fantasy development and transference. In this respect, the Internet can be compared with a mask that conceals more than just the face. A victim usually has only the words of the offender to interpret on-line. Facial expression, tone of voice, body language, and other physical aspects are all missing and subject to being filled in by the victim's unconscious needs and projections. A 13-year-old adolescent girl may entertain the sexual fantasies of a self-described 14-year-old shy boy living 100 miles away, but would be repulsed if made aware that they originate from a middle-aged man living down the block. Some teenagers are quite shocked to discover that the age-congruent peer they have "spoken to" over the Internet for months is a middle-aged pedo-

phile whose idea of "running away" is an afternoon in a cheap hotel.

The lack of sensory information on the Internet may have a significant impact on cyberstalkers, as described by Meloy: "The absence of sensory-perceptual stimuli from a real person means that fantasy can play an even more expansive role as the genesis of behavior in the stalker" (Ref. 32, p 11). The victim becomes an easy target for the stalker's projections and narcissistic fantasies that can lead to real-world rejection, humiliation, and rage.[33] Similarly, sexual predators can project their fantasies onto on-line victims and can manipulate victims by playing into their fantasies. Often poorly understood by the on-line victim is the lure of almost instant intimacy that the Internet offers. A shy, troubled person may find it easy to share his pain with a faceless "listener." Such effortless and rapid intimacy can be very seductive.

An interesting Internet code has developed, whereby one can add an emotional overlay to the typewritten message. A message that is all capitalized is the equivalent of shouting, and certain letter and symbol combinations portray various emotional states. For example, the symbol :-) viewed sideways at the end of a message indicates the writer is smiling.

Sex On-line

To gain a better understanding of how sexual offenders can use the Internet, it is instructive to become familiar with on-line dating. Dating sites, such as www.singles.com, www.americansingles.com, profiles.yahoo.com, and www.flirt.com, have traditional personal advertisements, fewer traditional three-dimensional chat rooms, and databases of individuals' demographics and personal preferences. These databases have many search options, enabling individuals to query for those in a particular age range, in a certain geographical area, and of a specific body type, for example. Some persons make portraits available and others give detailed descriptions of themselves and their interests. Once a suitable individual is found in the database, initial contact is made through personal e-mail within the dating sites. If the correspondence goes well, phone numbers are exchanged and a meeting might be arranged. Individuals who are experienced with these services and are looking for a physical relationship learn to present themselves in a way that attracts desirable partners and make a point of quickly arranging a personal meeting to determine whether the desired physical chemistry exists. Chat rooms are also a source of dating partners, as a recent outbreak of syphilis highlighted.[34]

Not all people are interested in a physical relationship. There are those who are more comfortable with so-called cybersex, which can consist merely of sexual arousal induced through electronic communication with another person, or masturbation while engaged on-line. Some would include any sexual activity that occurs while on-line (e.g., while viewing a pornographic Web site) as cybersex. Some view such phenomena as pathologic, whereas others take the stance that it is merely adaptive.[35]

Cybersex can interfere with established relationships, creating problems with trust and intimacy. Time spent on-line for some can become excessive and possibly meet the criteria for an addiction. This alone can cause problems in a relationship, but, when coupled with either interpersonal virtual relationships or erotic site viewing, the situation can become intolerable for the significant other.

The anonymity of the Internet has allowed those with rare or bizarre sexual needs a place to find "virtual" companionship, validation, and possibly an outlet for their paraphilias. There are many Web sites devoted to bestiality, among other things, and bulletin boards have even had postings from ampotemnophiles, those with an erotic fixation on amputated limbs.[28] It is likely that sexually deviant subcultures will expand their presence and influence by using the Internet. "Deviant sexual fantasies that might have remained simply the distorted musings of an imaginative mind may now be operationalized and implemented" (Ref. 28, p 195).

Internet Use by the Sexual Predator

The authors define a sexual predator as a sex offender who takes advantage of a characteristic (or characteristics) of a victim to further sexual exploitation of the victim, with some element of planning involved. The characteristic can be emotional, psychological, physical, or any combination of these. There may seem to be some lack of clarity inherent in such a definition, because a sex offender, by definition, takes advantage of or exploits the victim. Inherent in the description, though, is the expectation that the predator, on some level, has planned the offense. In a description of affective versus predatory violence, Meloy[36] operationalizes the term predatory to include ego-syntonicity, conscious planning, and

preparation. The sexual predator can gather information about a victim and use that information to gain control of the victim or gain the victim's trust. This includes, but is not limited to, individuals who pose as, or are in, a position of authority or are familiar to the victim and use their status to further sexual exploitation of the victim. Sex offenders using the Internet groom their victims as do offenders in the real world: "Perpetrators attempt to build both a trusting and fear-based relationship with their victim, with an end goal of being able to get sexual contact without significant resistance"(Ref. 37, pp 17, 18). That the Internet has been and will continue to be misused by sexual predators, especially pedophiles, is a given.[38]

The Internet is a particularly powerful tool for sexual predators, giving them access to victims for extended periods of time, allowing ample opportunity to gain control of their victims or gain their victims' trust and possibly to arrange a meeting in the physical world. For instance, in the past, only trusted members of a community, such as relatives, clergy, or teachers, had prolonged private access to children. Currently, however, the Internet enables virtually anyone to communicate privately with children in their homes, conceivably with a parent in the same room. Furthermore, sexual predators can use the Internet at home or work, making themselves highly available to their victims, facilitating development of trust.

Development of trust, also called grooming in the context of sexual predation, helps an offender control a victim and reduce the chance that the victim will inform authorities (e.g., parents, police) of the offender's existence. Grooming usually involves a sexual predator's exploiting a victim's feelings (e.g., loneliness, low self-esteem, sexual curiosity and inexperience) or needs (e.g., money) and taking advantage of this vulnerability to develop a bond. Once a bond is developed, the offender can easily persuade a victim to follow the offender's instruction to keep the relationship secret. Subtle psychological force is a potent weapon for the sexual predator.[37]

In one case indicative of grooming behavior, an investigator posing as a 14-year-old girl first encountered 49-year-old Charles White in an AOL chat room. Over two and a half months, White made an effort to gain the trust of the person he thought was a 14-year-old girl with regular correspondence, on-line chats, and a photograph of himself, alternately playing the role of "daddy" and seducer. White gradually broached the subject of sex, asking for a pair of the victim's "panties" to be sent and e-mailed pornography to lower the victim's sexual inhibitions. White also offered gifts to encourage the victim to meet him in person, suggesting that he would videotape her in her underwear. Ultimately, White committed a crime when he sent child pornography to his "victim," enabling investigators to arrest him and obtain a search warrant for his home where they found additional child pornography, including images of him having sex with a neighborhood girl. White admitted to molesting two children he was baby-sitting, photographing one of them, and videotaping himself having sex with an unconscious woman. White obtained a plea agreement and was sentenced to more than 10 years for sexual exploitation of minors, possession and distribution of child pornography, traveling across state lines for the purpose of engaging in illegal sexual contact with a person under the age of 18, and illegal possession of a sawed-off shotgun.[39]

The Internet also allows sexual predators to hide their identities and locations and to masquerade as a person of any sex or age to gain a victim's trust. For instance, 35-year-old Richard Romero gained the trust of an adolescent boy by posing as a 15-year-old named Kyle. Romero was found guilty of kidnapping, transporting a minor across state lines with the intent to engage in criminal sexual activity, and obstructing justice, because of his efforts to get people in Florida to destroy evidence.[40] In another case, a male psychiatrist masqueraded as a disabled person named "Joan" and used this persona to befriend many people on-line. As one aspect of his on-line exploits, he arranged an introduction between himself and a friend of "Joan's." The introduction led to an affair, and when the truth came out, the person felt victimized by the doctor.[41]

Sexual predators use the Internet to share information and trophies with other offenders. Consider a seemingly limited sexual abuse case in which a 6-year-old girl told her parents that her friend's father, Ronald Riva, sexually abused her at a slumber party.[42] It transpired that Riva and his accomplice, a previously convicted child molester named Melton Myers, were members of an international group of sex offenders called the Wonderland Club, with hundreds of members around the globe who used the Internet to communicate and exchange child pornography. Transcripts of one on-line conversation showed Riva and Myers as they abused one victim,

describing what they were doing for the enjoyment of others in the chat room. Apparently, some members of the Wonderland Club owned production facilities and transmitted live child-sex shows over the Web. Club members directed the sex acts by sending instructions to the producers via on-line chat rooms.[43] It is instructive that after learning of the arrest of some club members, rather than stop their activities, hundreds of other members began to use encryption and other protective mechanisms.

The Internet enables sexual predators to commit an offense even without physically assaulting a victim. For example, a 47-year-old Ohio man posing as a 15-year-old communicated through computer messages with a 14-year-old girl and was able to convince her to send him sexually explicit photographs and videotapes of herself performing sexual acts. The cyber relationship went on for 18 months, beginning when the girl was 12. The offender pled guilty to one charge of inducing a minor to produce child pornography.[44]

It is important to realize that the use of a new technology does not fundamentally change the behavior of criminals who use it. Before the advent of the Internet, sexual offenders established international noncomputerized networks that enabled them to share information and victims.[45] The Internet is mainly a facilitator and a catalyzing agent,[28] helping offenders gather information, contact and monitor victims, develop trust and control, develop fantasy, and avoid apprehension. When evaluating a sex offender, the forensic psychiatrist must be prepared to ask questions related to (and be knowledgeable about) the offender's Internet use and habits, even when that is not an apparent focus of the evaluation.

An interesting case in Tampa, Florida, combines both stalking and predatory sexual behavior on-line. Using an alias and a bogus e-mail address, Robert Harvey Alexander, a deacon at a Florida church, used computer terminals at local libraries to harass victims by threatening to destroy their reputations through on-line postings (in one case a digitally altered photograph), if they would not engage in "cybering" (Internet sexual conversation) and phone sex with him. Alexander boasted to his victims that the police would not be able to track him. He accumulated a "victims list" of 100 e-mail addresses of high school and college students in various states. Using e-mail and telephone records of the victims, the Federal Bureau of Investigation (FBI) was able to target Alexander, and he was arrested in a Tampa library while at a computer terminal. The federal prosecutor tried this case using existing extortion statutes, not stalking laws, and the threats involved were of defamation of character, not physical violence.[46]

As more sexual predators use the Internet, it is important to consider the impact that the technology is having on them. Research has indicated "that most pedophiles are isolated individuals with little or no social contact with age mates."[47] However, as mentioned earlier, the Internet provides some sexual predators with support groups. This peer support may allow these individuals to convince themselves that their behavior is acceptable and does not injure the victims. Durkin and Bryant,[29] in a 1999 study of on-line pedophile behavior, illustrate this phenomenon. The data collected in this study of the alt.support.boy-lovers newsgroup have one major weakness: There is no certainty that all the subjects were in fact pedophiles. In alt.support.boy-lovers and other similar on-line discussion groups, it is difficult to distinguish between a pedophile and an undercover police officer or someone assisting law enforcement by giving a fictitious account or justification to encourage others to incriminate themselves. Although the methodology (i.e., the sample) may be flawed, the study's findings are compelling and are deserving of further research.

Each state has its own statutes dealing with sex crimes. There are few statutes that specifically address sexual predation on-line. In 1998 18 U.S.C. § 2425 was passed making 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." Although 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."[48] While touted as an anti-cyberstalking law, on a practical level it is actually a sexual predator law. This law can be used to prosecute anyone who contacts a minor via the Internet and arranges a meeting with the intent of having sexual contact.

Internet Use by the Obsessional Harasser

Stalking is the repeated uninvited monitoring and/or intrusion into the life and activities of a victim that is usually, but not always, undertaken for the

purpose of frightening or intimidating the victim or those around the victim. Antistalking laws vary, but are generally written to address a pattern of unwanted intrusion that carries an implied or direct threat in which the intrusive behavior leads the subject of the behavior to feel threatened.[32] Cyberstalking is merely stalking that uses the Internet for information gathering, monitoring, and/or victim contact. Meloy and Gothard[49] coined the term "obsessional following" to describe "an abnormal or long term pattern of threat or harassment directed toward a specific individual" (Ref. 49, p 259). Obsessional harasser would be an equivalent term. Obsessional harassers (or followers) have been categorized by Zona *et al.*,[50] who described three subtypes: the erotomanic, the love obsessional and the simple obsessional. These terms, along with others, such as "borderline erotomania,"[51] may give way at some point to a more descriptive and clearer typology.[52] The simple obsessional stalker was found by Zona *et al.*[50] to be the one group most at risk for assaultive behavior. There may be little or no connection between threats of violence and approach behavior.[53] The research and literature on stalking are still nascent, and it may be some time before more definitive correlations can be drawn.

Palarea *et al.*[54] conducted an in-depth analysis (135 intimate versus 88 nonintimate stalkers) of the degree of intimacy of the victim-stalker relationship related to threats and violence. Intimate-relationship stalkers were found to be more dangerous than nonintimate-relationship stalkers. This study highlights the fact that stalking is not a crime limited to celebrities and is more likely to affect the so-called average citizen.[53] Fremouw *et al.*[55] reported finding that 17 percent of male and 30 percent of female undergraduates at West Virginia University said they had been stalked, making this behavior a far-from-rare occurrence. This is troubling, because the effect of stalking on the victim can be catastrophic, and is often compounded by an inadequate legal response.[56] Westrup *et al.*,[57] not surprisingly, found that stalked undergraduate females at West Virginia University reported significantly more (and more severe) posttraumatic stress disorder (PTSD) symptoms than those who were simply harassed or in a control group. Highlighted by the study by Palarea *et al.*[54] was that a prior history of violence in the stalker was a predictor of a violent outcome to the stalking episodes, regardless of the prior type of relationship between victim and stalker.

Research[58] has indicated that the majority of stalkers know the victims before the offense. However, because the Internet provides ample opportunity for stalking strangers, we may see an increase in stalking by offenders with no prior history of contact with the victim. A limiting factor may have been contact with and access to information about victims. The Internet essentially removes this limitation.[48]

Many obsessional harassers combine their on-line activities with more traditional forms of harassment, such as telephoning the victim and going to the victim's home. They harass their victims by means of a wide variety of Internet services, including e-mail, newsgroups, chat rooms, and instant messaging. As well as harassing victims first encountered in the physical world, they target individuals in cyberspace whom they have never met. Other obsessional harassers take a less direct approach to harassment, putting personal information about their victims on the Internet and encouraging others to contact the victim or even to harm them.

One individual posed on-line as his victim, posting personal advertisements with her address and phone number, soliciting people to fulfill a rape fantasy. The victim became alarmed when men began showing up at her apartment. One of them explained that he was responding to her personal ads. When she put a note on her door to discourage visitors, the harasser posted messages on the Internet claiming that the note was part of her fantasy and should be ignored.[59] To date, there have been no studies published about on-line stalkers.

In general, obsessional harassers seek to exert power over their victims, primarily through fear. The crux of a stalker's power is knowledge of the victim. A harasser's ability to frighten and control a victim increases with the amount of information that the harasser can gather. Harassers use information, such as telephone numbers, addresses, and personal preferences, to impinge on their victims' lives. The very fact that the harasser has acquired this knowledge is, in itself, often a cause of fear in the victim.

One violent obsessional harasser published a Web page with his plans to kill his target, and then carried out the plan.[60] An offender's Web site and on-line presence can be useful, even if it is not related to the offense, because it gives the viewer an impression of the offender's self-image, state of mind, interests, and

more. The choice of on-line nicknames can be revealing, and an offender's Web page may contain stories that lend insight into his or her motives and fantasies and may have links to favorite areas on-line that can lead to other victims and additional evidence. Extrapolating this last point to the physical world, an offender's Web page may contain references to or photographs of favorite locations that can be useful when looking for other potential victims or sources of physical evidence.

It is not surprising that on-line dating has led to cyberstalking. A Detroit man pleaded guilty to stalking a woman through a computer and over the telephone. After contacting the woman through a computer dating service, he communicated with her by computer and contacted her by phone. The couple met in person twice. After the second meeting, the woman ended the relationship by e-mail. The stalker continued to leave phone and e-mail messages for the woman, even after police warned him to stop.[61]

There are false reports of crimes for various reasons, ranging from attention to extortion. Even stalking has a certain amount of false reporting, and the forensic psychiatrist must be cognizant of this fact. In a study unrelated to cyberstalking, Pathe *et al.*[62] compared 12 persons who lodged false reports with 100 true stalking victims. They divided the false reporters into five types: (1) a stalker who preempts the victim by leveling an accusation first, (2) false reporters with severe mental illness, (3) past victims of stalking who are now hypersensitive and misinterpret the innocent actions of others, (4) factitious victims, and (5) malingerers.[62] To date, the authors have failed to find any documented false allegations of cyberstalking, but there is no reason to believe they will not surface in the future.

Federal law in the United States addresses cyberstalking to some degree. It is a federal crime to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another under 18 U.S.C. § 875(c), but this does not address cyberstalking that does not include a direct threat. As noted in the U.S. Department of Justice's report,[48] cyberstalking that involves the "use of a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number" may be prosecuted under 47 U.S.C. § 223. However, it is not clear whether this legislation applies to methods of communication such as IRC or AOL's Internet Messenger.

Fortunately, cyberstalking is being dealt with from a legal standpoint at the state level. California was the first state to enact a traditional stalking law in 1990, and this statute was amended in 1998, specifically to include cyberstalking.[63] Although all 50 states and the District of Columbia have enacted traditional stalking laws, as of April 1, 2000, only 23 U.S. states have enacted stalking statutes that explicitly cover electronic communications.[63] However, because each state deals with cyberstalking differently, interstate cyberstalking can be difficult to investigate and may require intervention by federal authorities. Jurisdictional disputes can further complicate investigations when states do not authorize warrants for seizure of evidence in other states. For example, a cyberstalking case worked on by one of the authors was based in Connecticut, but involved evidence on AOL servers in Virginia. It was necessary to contact law enforcement in Virginia and provide them with evidence that they could use to demonstrate probable cause to a court in Virginia to authorize the seizure of evidence from AOL's system and the disclosure of that evidence to investigators in Connecticut.

Digital Evidence

Digital data are combinations of ones and zeros that encode information that can be transmitted through cables (wire or fiber optic), air, or both (as in a relay) and can be stored on media such as magnetic (e.g., hard drives) or optical disks (e.g., compact disks). This encoded information can be interpreted by an appropriate reading device (such as a personal computer or a mobile phone) as text, photographs, audio, or video. The term digital evidence encompasses all digital data that can establish that a crime has been committed or that can provide a link between a crime and its victim or a crime and its perpetrators.[6] Because computers and the Internet are being more widely used by criminals, forensic psychiatrists can expect to encounter an increasing amount of digital evidence in their work. Forensic psychiatrists who become comfortable with digital evidence will be in a better position to interpret the behavior underlying the digital data[3] and incorporate this behavior in their psychiatric evaluations, improving their ability to advise victims or law enforcement when retained in that capacity.

The raw data flowing through a network can be a rich source of evidence. There are many programs for monitoring network traffic, commonly referred to as

network "sniffers." However, capturing live network traffic related to a crime is only possible if the crime is anticipated. Because most criminal acts are reported to investigators only after the fact, it is often necessary to find other sources of digital evidence.

One of the fundamental principles of the forensic sciences applies to digital evidence. Locard's exchange principle states that anyone, or anything, entering a crime scene and leaving, takes something away from the scene and leaves something behind.[64] In the physical world, an offender might inadvertently deposit a hair at a crime scene and leave with a fiber from the scene. Such evidence transfer also occurs on-line. An offender accessing a specific server on the Internet leaves traces of his or her presence on the server and departs with information from the server stored on his or her computer. Therefore, it is important to look for trace evidence on the offender's computer and storage devices, the offender's Internet service provider (ISP), the victim's computer and storage devices, and the victim's ISP and on any systems on the Internet that the offender and/or victim may have used. The following is a summary of these sources of evidence, to offer forensic psychiatrists a better sense of the potential and limitations of such evidence.

Computers used to connect to a network (e.g., the Internet) often contain large amounts of information about its users' activities on the Internet, giving insight into interests, communications, habits, and fantasies. Web browsers on a computer maintain a list of all pages that have been viewed and the time when visited and temporarily store recently viewed content in a cache to improve performance. Programs used to view newsgroups also maintain a list of the newsgroups that have been viewed. E-mail programs contain e-mail content and sometimes transaction logs of when messages were sent and received. Also, many individuals keep logs of their conversations on IRC. These log files contain a full transcript of the conversation and some additional information about the participants, such as nicknames and IP addresses.

One of the primary challenges in cases involving the Internet is locating the offender and solidly linking him or her to the crime. In one case, graphic child pornography showing a range of sexual acts was posted on Usenet, and the incident was reported to the FBI. The FBI used the message headers to determine that the perpetrator connected to the Internet through AT&T. A review of the records at AT&T showed that the subscriber who owned the offending account was a 42-year-old man in San Diego. The FBI compared the man's driver's license photo with the pictures posted on the Internet and determined that the child in the photos was his 10-year-old daughter.[65]

Because it is possible for one person to masquerade as someone else on the Internet or even to use another person's account, linking an individual to an activity on the Internet usually requires corroborating evidence. Server logs and other transaction information are critical for making such connections. For example, many people connect to the Internet through a modem. To connect to the Internet in this way, it is necessary to configure the modem to dial into an ISP's modem bank. Most ISPs keep logs of which subscribers dial into their modem bank at a given time and what IP address each subscriber is assigned while he/she is connected to the Internet. Some ISPs also use automatic number identification (ANI) on their dial-up modem banks, thus enabling investigators to trace a connection to a very specific location (e.g., house, apartment, room).

In an investigation involving the Wonderland Club, investigators linked an on-line screen name in the IRC #w0nderland and #ourplace channels to an IBM Global Network Services ("IBM") dial-up account registered to Gregory Grant. On appeal, Grant argued that all evidence found in his home during a subsequent search should be suppressed, because the investigators who obtained the search warrant for his home had failed to prove that he was using the account at the time of the offenses. Grant's objection was rejected in part because there was a "fair probability" that Grant was the user and that evidence of the user's illegal activities would be found in Grant's home.[66]

There are many other log files that can be useful in a case involving the Internet. Each time a file on a Web server is accessed through the Internet, an entry is made in a log file detailing which computer on the Internet was used to access certain files at a given time. Computers that are connected to the Internet often keep detailed logs of which computers attempted to communicate with them at a specific time. On multiuser systems, there is often a record of who logged in when and even what commands were executed. Every time an e-mail server sends or receives e-mail, details regarding that message are

noted in a log file. Therefore, in addition to examining the actual messages that an e-mail server contains at any given time, an investigator can determine what messages passed through the system. If a message has been deleted from the server to conceal a crime and cannot be recovered, there may still be evidence of its existence in the server's log files. In addition, many e-mail server logs contain information about when individuals checked their e-mail.

An understanding of offender behavior, combined with knowledge of what information exists in log files can lead to key evidence. For example, when an individual creates an anonymous e-mail account with the intent to stalk, he or she usually sends himself or herself a test message to ensure that no personal information is disclosed. When the stalker receives this test messages, an entry is made in his or her ISP's mail server log and can be useful for making a connection between a suspect and an anonymous e-mail address. The usefulness of log files applies to corporate networks as well as generally accessible systems on the Internet. When a victim receives a threatening e-mail message, the organization's e-mail server logs can be searched for messages from the same source to determine whether the offender is also within the organization and sent himself a test message or is targeting multiple victims within the organization.

A final consideration to keep in mind is that personal computers usually contain much more information than is readily visible. Data that have been "deleted" actually remain on the disk indefinitely, and technically savvy individuals can hide data in unused areas on a disk and within another digital object.[67] Software is available that makes it relatively easy to view the full contents of a disk and search for particular patterns. When dealing with digital evidence, an effort must be made to document it and collect it in a way that preserves its integrity. Specialized software, such as EnCase,[68] SnapBack DatArrest,[69] and Safeback,[70] has been developed that can make an exact copy of a drive in a manner that preserves its probity.

One significant barrier that cannot be circumvented using such evidence collection systems is encryption.[71] Files that are encrypted with freely available encryption programs such as PGP are, for all intents and purposes, impregnable. If the individual who encrypted the file is not cooperative, one must either gain access to the decryption key or seek other sources that may contain the information in unencrypted form.

Much of this information regarding digital evidence may seem beyond the expertise of forensic psychiatrists and may seem to lack any direct connection to their practices, but the authors suggest that although the technology may be somewhat foreign and intimidating, an awareness of the problems involved will be helpful to a forensic psychiatrist engaged in an examination of sexual predators or obsessional harassers and/or their victims in which electronic transmissions have, or may have, played a part. As a minor, but important point, the authors see no ethical problems related to inclusion of digital data in an evaluation, assuming the information was obtained in a legal manner.

Conclusions

Although for some the on-line world is a sea of information and interaction, for others it is an unknown void. For still others, it is an opportunity to use a new technology to commit crimes. Both sexual predators and obsessional harassers have taken to cyberspace in the pursuit of their goals. The result is a veritable behavioral archive containing significant data of what people have said and done. It is becoming more and more obvious that the forensic psychiatrist involved in the evaluation of stalkers, pedophiles, and other sexual predators requires at least a basic understanding of the Internet, its uses and misuses, and the emerging field of digital evidence.

Forensic psychiatrists who are comfortable with Internet search tools and are aware of the possibility of tracking offenders on the Internet will be better able to assist their clients when the Internet is involved. Whether performing a full psychiatric evaluation, advising victims or law enforcement or testifying in court, the forensic psychiatrist will find that the ability to locate additional information related to the case at hand is a valuable asset. Whether a practitioner feels comfortable searching for such information is not the issue. A sense of where such evidence can be located on servers and personal computers and the awareness that one must call in experts to obtain digital evidence is a prerequisite for any work involving computers and networks. Just as the forensic psychiatrist might ask whether a confession was videotaped, they are well served to ask whether any digital evidence is available in a particular case. The forensic psychiatrist can only benefit from specific knowledge

of how offenders use the Internet. This knowledge will help in gaining an understanding of offenders' temptations, choices, and potential on-line behavior.

Forensic psychiatrists are uniquely equipped to interpret the behavior represented by digital data found on computers and the Internet. There are texts, on-line and on-site courses, and college courses that can provide the necessary technical knowledge (all easily located on-line). Unfortunately, there is currently no research on the impact of technology on offenders' behavior and offending on the Internet. Questions that should be examined in future studies include whether on-line support encourages sexual predators to act on impulses that would have otherwise remained dormant and whether the Internet is leading to an increase in stranger stalking.

References

1. ABC's of "Internet Therapy" (available at http://www.metanoia.org/imhs/; accessed February 14, 2002)
2. Maheu MM, Gordon BL: Counseling and therapy on the Internet. Profess Psychol 31:484–9, 2000
3. Casey E: Cyberpatterns: criminal behavior on the Internet, in Criminal Profiling: An Introduction to Behavioral Evidence Analysis. Edited by Turvey B. London: Academic Press, 1999, pp 299–327
4. Gibson W: Neuromancer. London: Victor Gollancz, Ltd., 1984
5. Dunne R, Long H, Casey E: Internet crime, in Encyclopedia of Forensic Sciences. Edited by Siegal JA. London: Academic Press, 2000, pp 1085–91
6. Casey E: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. London: Academic Press, 2000
7. Bacard A: Anonymous Remailer FAQ [frequently asked questions], 1999 (available at http://www.andrebacard.com/remail.html; accessed February 14, 2002)
8. Electronic Privacy Information Center: EPIC Online Guide to Practical Privacy Tools, 1999 (available at http://www.epic.org/privacy/tools.html; accessed February 14, 2002)
9. Zero-Knowledge Systems USA, Inc.: http://www.zeroknowledge.com/
10. Usenet: http://www.faqs.org/usenet/
11. Deja.com, Inc.: http://www.dejanews.com
12. RemarQ Communities, Inc.: http://www.supernews.com/
13. Internet Relay Chat: http://www.irchelp.org/
14. AltaVista Company: http://altavista.digital.com
15. Lycos, Inc.: http://www.hotbot.com
16. Copernic Technologies, Inc.: http://www.copernic.com/
17. ICQ, Inc.: www.icq.com
18. Napster, Inc.: www.napster.com
19. The Freenet Project: freenet.sourceforge.net
20. Hotline Communications, Ltd: www.bigredh.com
21. The Associated Press: Spanish teenager nabbed after making e-mail bomb threat. 1998 (available at http://www2.nando.net/newsroom/ntn/info/073098/info13_8097_noframes.html)
22. Black student charged with racist e-mail threats at college. Tribune News Services. April 21, 2000 (available at http://www.chicago.tribune.com/version1/article/0,1575,SAV-0004210233,00.html)
23. Press Release: Man convicted of threatening federal judges by internet e-mail. Washington, DC: U.S. Department of Justice, 2000 (available at http://www.usdoj.gov/criminal/cybercrime/johnson.htm)
24. Boiles G: The CJ File: Documents generated during the investigation and prosecution of Carl Edward Johnson, 1999 (available at http://www.parrhesia.com/cj/)
25. cDc Communications: http://www.bo2k.com/
26. UltraAccess Networks Inc.: http://www.netbus.org/index.html
27. SubSeven: http://subseven.slak.org/main.html
28. Durkin KF, Bryant CD: "Log on to sex": some notes on the carnal computer and erotic cyberspace as an emerging research frontier. Deviant Behav 16:179–200, 1995
29. Durkin KF, Bryant CD: Propagandizing pederasty: a thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles. Deviant Behav 20:103–27, 1999
30. Former executive pleads guilty. Associated Press. March 17, 2000 (available at http://www.xone.net/article.php?981)
31. E-mail indicates woman may have agreed to be slain. USA Today. February 28, 1999 (available at http://usatoday.com/life/cyber/tech/ct309.htm)
32. Meloy JR: The psychology of stalking, in The Psychology of Stalking: Clinical and Forensic Perspectives. Edited by Meloy JR. New York: Academic Press, 1998, pp 1–23
33. Meloy JR: Stalking (obsessional following): a review of some preliminary studies. Agress Violent Behav 1:147–62, 1996
34. Klausner JD, Wolf W, Fischer-Ponce L, Zolt I, Katz MH: Tracing a syphilis outbreak through cyberspace. JAMA 284:485–7, 2000
35. Cooper A, Scherer CR, Boies SC, Gordon BL: Sexuality on the internet: from sexual exploration to pathological expression. Profess Psychol 30:154–64, 1999 (also available at http://www.apa.org/journals/pro/pro302154.html)
36. Meloy JR: Violent Attachments. Northvale, NJ: Aronson, 1997
37. Johnson S: Psychological force in sexual abuse: implications for recovery, in The Sex Offender: New Insights, Innovations and Legal Developments (vol 2). Edited by Schwartz BK, Cellini HR. Kingston, NJ: Civic Research Institute, 1997, pp 17-1–17-11
38. Durkin KF: Misuse of the Internet by pedophiles: implications for law enforcement and probation practice. Federal Probation 61: 14–18, 1997
39. U.S. v. White, Case No. IP99-CR-0005-01-M/F (S.D. Ind. 1999) (Docket sheet available at http://www.insd.uscourts.gov/caseinfo.htm)
40. U.S. v. Romero, 189 F.3d. 576 (7th Cir. 1999) (available at http://www.kentlaw.edu/7circuit/1999/aug/98–2358.html and http://laws.lp.findlaw.com/getcase/7th/case/982358.html)
41. Gelder LV: The strange case of the electronic lover. Ms. Magazine. October, 1985 pp 94, 99, 101–104, 117, 123–124
42. Golden T: 16 Indicted on charges of internet pornography. The New York Times. July 17:1996, p A10
43. Shannon E: Main street monsters. Time Magazine. September 14, 1998, p 11 (available at http://www.time.com/time/magazine/1998/dom/980914/crime.main_street_monst16.html)
44. Burney M: Cyber affair with teen-age girl leads to five years in prison. The Associated Press. August 22, 1997 (also available at http://www.nando.net/newsroom/ntn/info/082297/info10_3348_noframes.html)
45. Testimony of Joseph Francis Henry to the Permanent Subcommittee on Governmental Affairs before the United States Senate, Ninety-Ninth Congress. February 21, 1985 (available at http://www.NOSTATUSQUO.COM/ACLU/NudistHallofShame/Henry.html)
46. Cyber-extortion results in prison sentence. Net4TV Voice News Staff. October 8, 2000 (may be heard at http://www.net4tv.com/voice/story.cfm?storyid=2931)
47. Prendergast WE: Treating sex offenders in correctional institu-

tions and outpatient clinics: a guide to clinical practice. Binghamton, NY: Haworth Press, 1991
48. Report on Cyberstalking: A New Challenge for Law Enforcement and Industry. Washington, DC: U.S. Department of Justice. August 1999 (available at http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm)
49. Meloy JR, Gothard S: A demographic and clinical comparison of obsessional followers and offenders with mental disorders. Am J Psychiatry 152:258–63, 1995
50. Zona MA, Sharma KK, Lane J: A comparative study of erotomania and obsessional subjects in a forensic sample. J Forensic Sci 38:894–903, 1993
51. Meloy JR: Unrequited love and the wish to kill. Bull Menninger Clinic 53:477–92, 1989
52. McCann JT: Subtypes of stalking (obsessional following) in adolescents. J Adolesc 21:667–75, 1998
53. Dietz PE, Matthews DB, Van Duyne C, *et al*: Threatening and otherwise inappropriate letters to Hollywood celebrities. J Forensic Sci 36:185–209, 1991
54. Palarea RE, Zona MA, Lane JC, Langhrichsen-Rohling J: The dangerous nature of intimate relationship stalking: threats, violence, and associated factors. Behav Sci Law 17:269–83, 1999
55. Femouw WJ, Westrup D, Pennypacker J: Stalking on campus: the prevalence and strategies for coping with stalking. J Forensic Sci 42:666–9, 1997
56. Pathe M, Mullen P: The impact of stalkers on their victims. Br J Psychiatry 170:12–17, 1997
57. Westrup MA, Fremouw WJ, Thompson RN, Lewis SF: The psychological impact of stalking on female undergraduates. J Forensic Sci 44:554–7
58. Harmon R, Rosner R, Owens H: Obsessional harassment and erotomania in a criminal court population. J Forensic Sci 40:188–96, 1995
59. Foote D: You could get raped: the inside story of one young woman's terrifying ordeal at the hands of a cyberstalker. Newsweek International. February 8, 1999 (available at http://www.dailydavos.com/nw-srv/issue/06_99a/printed/us/st/ty0106_1.htm)
60. AmyBoyer.org 2000: http://www.amyboyer.org/
61. E-mail stalker sentencing will likely influence future cases. The Detroit News. March 23, 1996 (available at http://detnews.com/menu/stories/41019.htm)
62. Pathe M, Mullen PE, Purcell R: Stalking: false claims of victimization. Br J Psychiatry 174:170–2, 1999
63. Beatty D, Hicket E, Sigmon J: Stalking. Washington, DC: U.S. Department of Justice, National Victim Assistance Academy. Chap 22, Sec. 2, 2000 (available at http://www.ojp.usdoj.gov:80/ovc/assist/nvaa2000/academy/V-22–2ST.htm)
64. Saferstein R: Criminalistics: An Introduction to Forensic Science (ed 6). Upper Saddle River, NJ: Prentice Hall, 1998
65. FBI: man posted sex pictures with daughter on Internet. The Augusta Chronicle Online. February 11, 1998 (available at http://augustachronicle.com/stories/021198/tec_124–8099.shtml)
66. U.S. v. Grant 218 F.3d 72 (Me. 1st Cir. 2000) (available at http://laws.findlaw.com/1st/992332.html)
67. Johnson NF, Jajodia S: Steganalysis of Images Created Using Current Steganograpy Software. Lecture Notes in Computer Science 1525:273–89, 1998 (available at http://www.jjtc.com/ihws98/jjgmu.html)
68. Guidance Software, Inc.: http://www.guidancesoftware.com
69. Columbia Data Products, Inc.: http://www.cdp.com
70. Sydex, Inc.: http://www.sydex.com/
71. Singh S: The Code Book. New York: Anchor Books, 1999

25 25 Stalking Stalking behavior is characterized as obsession with a victim â€“Stalkers who use the Internet often try to conceal identity â€“Obsession with victim usually reveals identity eventually â€“Attempts to discourage them can incite them to violence which places victims at risk.Â 35 35 Resources Digital Evidence and Computer Crime by Eoghan Casey Elsevier Academic Press, 2004 National Center for Victims of Crime, Safety http://www.ncvc.org McGrath, M.G. and Casey, E. (2002) â€œForensic psychiatry and the Internet: Practical perspectives on sexual predators and obsessional harassers in cyberspaceâ€, Journal of American Academy of Psychiatry and Law, 30, 81-94. Characteristics and behaviors of sexual compulsives who use the Internet for sexual purposes. Sexual Addiction & Compulsivity: The Journal of Treatment and Prevention, 13, 53â€“67. Dybul, M., Fauci, A. S., Bartlett, J. G., Kaplan, J. E., & Pau, A. K. (2002).Â Internet pornography: A social psychological perspective on Internet sexuality. Journal of Sex Research, 38, 1â€“11. Fisher, W. A., & Boroditsky, R. (2000).Â Manipulation of self in cyberspace. In Spitzberg, B. H., & Cupach, W. R.. The dark side of interpersonal communication (2nd ed., pp. 93â€“120). Mahwah, NJ: Erlbaum. Forensic psychiatry and the internet: Practical perspectives on sexual predators and obsessional harassers in cyberspace. Journal of the American Academy of Psychiatry and the Law, 30, 81-94. Meloy, J. R. (1996). Stalking (obsessional following): A review of some preliminary studies. Aggression and Violent Behavior, 1, 147-162. https://doi.org/10.1016/1359-1789(95)00013-5. Meloy, J. R. (1998). The psychology of stalking: Clinical and forensic perspectives. New York: Academic Press. Meloy, J. R. (2003).