

Victimization Online: The Downside of Seeking Human Services for Women on the Internet

JERRY FINN, Ph.D., and MARY BANACH, Ph.D.

ABSTRACT

This article describes the problems and dangers that may be encountered when women seek health and human services on the Internet. Issues related to online counseling and online self-help groups include: difficulties in ascertaining the credentials and identity of service providers, accessing inaccurate information, reliance on untested methods, difficulties in online assessment, exposure to disinhibited communication, development of inappropriate online relationships, and lack of standards and regulation regarding online human service practice. In addition, potential victimization of women users of the Internet through loss of privacy, cyberstalking, and identity theft is described. Guidelines and resources for prevention of online victimization are presented.

INTRODUCTION

THE INTERNET provides people with new avenues of information and support. These include websites, listservs, usenet groups, and chat groups that offer professional and self-help services in a variety of health and human service-related areas.^{1,2} The public is increasingly using online resources. A 1997 survey found that approximately 47,000,000 adults use a computer and that approximately one-fourth of these use the Internet.³ Moreover, the "gender gap" in computer use is disappearing. A recent study by Nielson/NetRatings notes that one-half of computer users are female, although men still spend more hours online.⁴ Internet usage is likely to continue to expand as business and consumer functions increasingly come online. Furthermore, the public is becoming accepting of using the Internet to find

information about health and human service concerns. One study found that more than 31,000,000 people had done so.⁵ Women are more likely to use the Internet to find information about health and quality of life than are men.⁴

A number of studies have described and documented the benefits of online human services.^{1,6} Human service agencies have begun to use the Internet as a tool for promoting agency visibility, providing community education, offering information and referral services, providing online counseling, obtaining community feedback, and engaging in advocacy activities.⁷⁻⁹ Online resources designed to promote community among women as well as human service agencies that focus primarily on women's issues such as depression, eating disorders, family planning, single parenthood, domestic violence, and sexual abuse can be found

using common Internet search engines. For example, one study found more than 15,000 nonprofit web pages on the Internet related to domestic violence.¹⁰ While the research is promising, it should be noted that the quality and quantity of research that documents the benefits and outcomes of online human services is still in the preliminary stages, and service delivery has far outpaced evaluation of online services.

POTENTIAL HARM IN USING ONLINE RESOURCES

Little has been written about the risks involved in using online human service-related resources, although there is some evidence, both in the research and anecdotal reports, that using the Internet can have negative consequences.¹¹⁻¹⁵ Harm in using online human service and self-help groups can take a variety of forms, including: accessing inaccurate information, loss of privacy; exposure to disinhibited or hyperpersonal communication,¹⁶ "cyberaddiction,"¹⁷ development of inappropriate online relationships, reduction of primary (face to face) relationships,¹⁸ and online harassment or stalking.^{19,20} While these avenues of potential harm can impact either gender, women are more likely to experience difficulties in the areas of health and human services because they are consumers of these services to a greater extent than are men. Women are also more likely to be the targets of online threats and harassment because this is the case in the broader society,^{21,22} and there is some evidence documenting that this is also true in cyberspace. This article reviews the types of harm and victimization that women may experience as they seek human services and social support online. It describes resources that assist women in understanding the online environment and suggests practical and legal remedies for assisting women that may be victimized in their online interactions. In addition, the difficulties faced by human service agencies in providing online service and guidelines for risk management are described.

ONLINE MENTAL HEALTH SERVICES

Women are more likely than men to seek mental health-related services,²³ and there is beginning evidence that this is also true in cyberspace. A number of methods have been developed for providing online mental health services and support, and a growing number of mental health professionals are establishing online services. The most common method is E-mail "therapy" in which asynchronous E-mail messages are exchanged between a human service practitioner and a consumer. In addition, providers have offered "chat" in which a practitioner and consumer exchange messages in real time over the Internet.²⁴ The near future may also include the use of two-way video-conferencing as an adjunct to typed messages.²⁷ The benefits of online counseling have been described, and are similar to those involved in online self-help. These include access to professional help when none is locally available; removal of barriers due to time, distance, scheduling, care-giving responsibilities, and difficulties related to verbal communication; ability of both therapists and clients to think-through and formulate responses; and cost-savings.^{26,27}

Women seeking online counseling need to understand the actual and potential pitfalls involved in online services. First, there is yet little empirical evidence about the effectiveness or harm related to online therapeutic services. Given that these services are so new, there are no "experts" because skills in face-to-face counseling may not translate to the online environment.^{28,29} For example, the ability to "tune in" to nonverbal cues and to convey empathy through gesture, facial expression, and eye contact during in-person treatment will not be available online.²⁸ In addition, standard procedures required by the code of ethics of professional psychologists, social workers, and counselors may be more difficult or impossible to provide in an asynchronous, text-based environment.^{30,31} These include the need for accurate assessment, availability in times of crisis, maintaining confidentiality of records, warning vulnerable third-parties, avoiding inappropriate relationships, and practicing only where

licensed to do so.³²⁻³⁵ In our review of dozens of online counseling websites, very few presented the limitations or experimental nature of their services. Thus, women may be unintentionally victimized as "guinea pigs" in the creation of new services.

Other websites may set out to intentionally victimize women. The unregulated environment of the Internet means that anyone can easily put up a website and claim "expertise" in an area. This is especially problematic when seeking online counseling or therapy. There are no regulations established as to who may set up a website and offer "counseling." For example, one site, Dr. Schuchocolate (<http://adviceguy.hypermart.net>, May 1999), was found by searching the Altavista search engine (<http://www.altavista.com>) for the words, "online counseling." The site stated that it provided "moral advice and therapy." The authors examined the site and concluded that it offered racist, sexist, and homophobic "advice." Given a lack of community standards on the Internet, it is difficult to identify "false advertising." In general, there is no systematic means of quality control of the information on the Internet.

Women should take care to establish the credentials of those offering online counseling services. One helpful resource has been the development of the "Credentials Check" (<http://www.cmhc.com/check>) website. A practitioner can be listed on the website, and their credentials, including degree and professional license number are reviewed and posted on the site. The practitioner is then given a link on their own website to the Credentials Check website so consumers can verify the practitioner's legitimacy.

Another potential source of victimization for women seeking online services is the practice of "page-jacking." It is possible for someone to set up a website that appears to address health or mental health issues, and to supply key words on the site that would allow a search engine to find it when someone searches for "counseling," "therapy," or "domestic violence." The website can not only provide inaccurate information, but can then be programmed to send the user to a different page than was initially sought. In some cases, the

program can disable the "Back" button on the browser making it even more difficult to exit the program. For example, someone seeking a "mental health" website could be immediately sent to a pornographic site upon accessing the "mental health" site.³⁵

Women (and men) should be made aware of the both the potential benefits and problems in the use of online counseling services. They should only use online services to which they have been referred by a trusted source. They should seek sites in which the online practitioner provides links to certification bodies and licensure boards that can verify credentials and provide information about any legal action taken against the practitioner.

ONLINE SELF-HELP GROUPS

There are currently thousands of online self-help groups that may provide clients with supplemental support and psycho-education.² The benefits of online support groups have been described and documented for women's concerns such as breast cancer patients,³⁶ home caregivers,³⁷ eating disorders,³⁸ sexual abuse survivors,²⁷ single young mothers,³⁹ and parents.⁴⁰ These benefits include elimination of access barriers due to time, distance, disability, communication limitations, scheduling, rarity of disease, and fear of face-to-face participation. They also provide access to a broader array of social support, an enhanced sense of universality, and opportunity to participate in a relatively anonymous manner.⁴¹

There is some evidence, however, that participation in online self-help groups may also be harmful to some members. The literature has described a number of areas that may be problematic for women seeking help and support through online groups:

Disinhibited communication

Research on computer-mediated communication suggests that the social control that most communities exert over members may be reduced online.^{42,43} Online communication does not include social status cues such as dress, age, race, body language, and facial expressions

that might normally inhibit inappropriate responses. Interaction may therefore become more disinhibited. In addition, online communication takes place in isolation without the usual group norms that regulate behavior. Thus, there is greater chance that someone will be exposed to threats, profanity, seduction, and personal attacks than in face-to-face groups.¹⁶ Hostile, disinhibited behavior is often referred to as "flaming." Although most groups discourage flaming and may ban someone who violates the social norms of the group, there is the potential for participants to be emotionally abused. Such disinhibited behavior may be especially difficult to handle when someone believes they are in a helping or therapeutic context.

Leadership issues

Anyone can set up an online self-help group and invite users to participate. Many online groups have a moderator who is responsible for promoting interaction and enforcing group norms. The qualifications of moderators are not regulated. This is similar to the case of in-person self-help groups. Leadership is a function of time, interest, and the willingness of others to participate. In addition, other members may state expertise in an area relevant to the group. It should be understood, however, that the anonymous nature of the Internet promotes the development and use of false identities, including those claiming expertise in health and human service related areas.

Member identity

Similar to leadership, the identity of members is largely unknown. This may generally lower the trust level among members, and is especially problematic in self-help groups concerned with issues of violence and abuse. For example, in an online self-help group, [alt.sexual.abuse.recovery](#), a member described a series of messages in which a perpetrator assumed the role of a victim, and later "confessed," creating considerable anger and emotional pain for those with whom he had established a "relationship."

Group disruption

Just as a number of women's organizations such as family planning and domestic violence shelters have been the recipient's of threats and attacks, online women's groups are also vulnerable to "cyberterrorism." The majority of self-help groups are not moderated therefore anyone can post a message. For example, one tactic used to disrupt a group is to turn the focus of the group away from its primary purpose. This is accomplished when one (or several) members join the group and then post racist and sexist messages. This results in the rest of the group arguing with the poster(s), thus losing track of the original purpose of the group. Eventually, members leave the group because it no longer meets their needs. Waldron et al.⁴⁴ described two online self-help groups for people with emotional issues and sexual abuse recovery that disbanded as a result of receiving a barrage of sexually explicit advertising and messages.

Misinformation

A potential disadvantage of online groups is that members may receive misinformation from other group members that may not be corrected or may be corrected only after a time delay. The limited research in this area has found that instances of misinformation do occur, although other group members generally correct them.²⁷

Misinformation can be considered victimization when it is purposefully provided. A more hostile form of group misinformation can occur when women's online groups are the targets of harassment and disruption. One way this occurs is when a "member" posts a message that includes a link to a website. The website may at first appear to be a resource for women, but on closer inspection is filled with misinformation, hostile rhetoric, or pornography. Similarly, a referral to another online group may contain hostile or upsetting messages. While such tactics are merely an annoyance to some women, they can be extremely disturbing to those already in emotional distress.

Loss of privacy

Group norms vary among self-help groups in terms of their stated norms to respect the privacy and confidentiality of members. In any case, messages may be read by anyone with access to the group, and no guarantee can be made that messages will not be forwarded to others. In addition, messages of many groups are archived and can be searched by several Internet search engines. Group members themselves may inadvertently reveal the personal information of another member. For example, in one study of online messages, Waldron et al.⁴⁴ reported a message in which one member was delighted to discover that another lived close by. The group member revealed that a third member also lived nearby, identifying the location quite specifically. This information became accessible to anyone who read the message. Such instances do not in themselves constitute victimization, however, they could be very problematic for someone who is being monitored by an abusive partner or who is being victimized by a stalker.

CYBERSTALKING

Stalking has been a legally designated a crime only since 1990, however, there are descriptions of stalking behavior in film, fiction, and poetry over the past several hundred years.¹⁹ Experts estimate that the vast majority of stalking victims are women, approximately 75%, and their perpetrators are men. Approximately 5% of all women will be stalked during their lifetime.¹⁹ Since many cases are unreported, this figure is likely to greatly underestimate the extent of stalking. While "celebrity stalking" is often presented in sensational media cases, the majority of stalking cases are not related to a celebrity. Stalking involves repeated and unwanted contact or communication that causes a person to fear for her safety. Stalking may result in psychological distress as well as physical and/or sexual assault and even murder. Some view stalking as aberrant behavior related to psychological dysfunction.^{45,46} Rebecca Lee,⁴⁴ however, argues that stalking is rooted in Western tradition in which

pursuit of a reluctant partner is considered part of "romance" and in which a woman must be wooed from "no" to "yes." Thus, stalking is likely to occur among a broader spectrum of the population than those with emotional problems, and is more likely to occur in settings in which romance is part of agenda (e.g., college campuses, singles bars).

"Cyberstalking" refers to stalking behavior in the context of cyberspace.²⁰ Whether perpetrated by an expartner, an acquaintance, or by a stranger, cyberstalking can take many forms, including:

- Threatening or unwanted E-mail; flooding a victim's E-mail box with unwanted mail;
- Sending the victim files with a virus;
- Using a victim's E-mail address to subscribe her/him to multiple listservs or to purchase books, magazines or other services in her/his name;
- Sending misinformation and false messages to chatrooms, Usenet groups, listservs, or places of the victim's employment;
- Stealing a person's online identity to post false information;
- Sending a victim's demographic information and/or picture to sexually oriented or pornographic sites; and
- Seeking and compiling various information that a victim may have posted on newsgroups with the intent to locate personal information and then use this information to harass, threaten, and intimidate the victim either online or in the real world.

There is little known about the extent to which cyberstalking is taking place, but the number of case reports related to online harassment is increasing.¹⁹ Many anecdotes and stories of cyberstalking have been reported online.^{47,48} Colleges across the country are increasingly dealing with cases of cyberstalking.¹⁹ Cyberstalking can be a terrifying experience for women, placing them at risk for psychological and possible physical harm.

It is likely that cyberstalking will be at least as common, if not more so, than offline stalking for several reasons. First, stalking often

takes place within the context (or fantasy) of romantic relationships. The nature of online environments can promote a false sense of intimacy and misunderstanding of intentions. The online environment creates "electronic propinquity," that is, people feel in proximity to each other online despite the physical distance. In addition, Walther¹⁶ finds that hyperpersonal communication, emotionally intensified interactions, often develop in online communication. The limited nonverbal, historical and contextual information available in mediated contexts may promote message recipients (potential cyberstalkers) to develop idealized perceptions of their fellow interactants and to misjudge the intentions of the messages they receive. In addition, the relative anonymity, the lack of social status cues, and the propensity for disinhibited behavior in the online environment may promote greater risk-taking and asocial behavior by a greater number of people.

Cyberstalking presents a particular danger for those seeking help and support online. Survivors of child abuse, sexual assault, and victims of domestic violence may be especially vulnerable to intimidation and loss of control in still another arena. Loss of privacy may be problematic for those who use chatrooms and post messages in online self-help groups. During times of crisis, women are more likely to reveal personal information and be less able to assertively respond to cyberstalking behavior. Cyberstalkers may copy current messages and use the information to harass a victim. In addition, newsgroup messages are often archived and may be searched by a search engine such as DejaNews (<http://www.dejanews.com/>). The content of past messages may be used to help locate or to harass a victim. In addition, a number of Internet sites provide a means for tracking a person through searches of names, telephone numbers, change of address forms, and public information databases. (See for example: *Be your own private investigator* (<http://www.geocities.com/Athens/7374/pi.html>). One site, actually named *The Stalkers Homepage*, (<http://pages.ripco.com:8080/glr/stalk.html>) consolidates resources for uncovering a variety of personal information including name, address, maps to residence, phone number, E-mail address, and social security num-

ber. Another site, SAX (<http://www.saxinvestigations.com/>) offers to monitor and investigate another's computer including reading files and email, tracing "erased" files, and monitoring chat or instant message conversations.

Identity theft

"Identity theft" is another form of victimization that may be part of cyberstalking or may be done for criminal purposes. Identity theft occurs when someone uses bits and pieces of information about an individual, usually the Social Security number, to represent him or herself as that person for fraudulent or harassment purposes. This might include obtaining credit cards and loans in someone else's name, opening utility accounts, renting an apartment, getting a cellular phone, and so on. It is estimated that there are 400,000 victims of identity theft nationally, and there has been a 16-fold increase in reports of this crime from 1992–1997.⁴⁹ While there are criminals that practice identity theft, it is also common for perpetrators of identity theft to be known to the victim. Perpetrators include spouses going through divorce, exspouses and expartners, former employees, exfriends, and coworkers who have a desire to control or hurt the victim. This may also include cyberstalkers. As noted previously, there are websites that facilitate someone collecting enough information to perpetrate identity theft. In addition, there are Websites that specifically offer to sell a person's Social Security (e.g., <http://www.infoseekers.com>). Given the burgeoning commerce that takes place online, identity theft can quickly result in a multitude of illegal purchases. While federal law holds that victims are not liable for the bills accumulated by the imposters, identity theft can result in anxiety and inconvenience related to privacy invasion, regaining financial health, and restoring a good credit history.⁵⁰

LEGAL ISSUES RELATED TO ONLINE VICTIMIZATION

The laws addressing online victimization are reflected in both state statutes and federal laws. All states have stalking laws in effect. Cyber-

stalking, however, has yet to be addressed in all of the states' statutes.⁵¹ At the time of this writing, only five states (Alaska, Michigan, New York, Oklahoma, and Wyoming) specifically contain language in their stalking statutes to include contact through electronic communication. State stalking statutes generally have two criteria that are needed in order to prove evidence of a crime. These criteria include the concept of intent (e.g., the alleged perpetrator must be perceived as making a "credible threat") and the actions must be repeated.¹⁹ "Typically, the threshold is that the behavior would cause a 'reasonable person' to suffer severe emotional distress."⁵¹ Recently, there have been changes, however in the language of some state statutes to modify the "credible threat" definition to a more inclusive "pattern of conduct."⁵⁰ These modifications, as will be discussed below, can support utilizing the existing stalking laws to address cyberstalking. Stalking in most states is considered a misdemeanor unless the victim has been sufficiently harmed, at which time it becomes a felony.¹⁹

The other state statutes addressing online victimization are contained in telephone harassment statutes. Because E-mail is a form of communication utilizing telephone connections, the telephone harassment statutes are pertinent. Although all 50 states have telephone harassment statutes in place, only some contain language specifically addressing electronic communication.⁵² As of this writing, 12 states include electronic communication in their harassment statutes.* Language in some telephone harassment statutes restricts harassment occurring only when there is actual conversation between the harasser and the victim. Ethan Katsh,⁵³ however, in a legal analysis of the use of telephone harassment statutes for computer harassment, analogizes E-mail to telephone answering machines. A victim can use this analogy along with federal case law to support her claims.

Three areas of federal laws are helpful in addressing online victimization. The first area is

in Title 18 Crimes and Criminal Procedures, Chapter 119 Wires and Electronic Communications interception and interception of oral communication.⁵⁴ This part of the Federal legal code precludes interception, use, or disclosure of electronic communication that is unauthorized or exempt from the rules set forth (for example as a result of a court order or governmental reasonable searches). The language in Title 18, Chapter 119 is similar to harassment and stalking state statutes in that there is a requirement of intent on the part of the perpetrator.

The second set of Federal laws that may be utilized to address online victimization is Title 42 of the Civil Rights Act. This statute has been interpreted to prohibit sexual harassment in work environments.⁵¹ Conduct producing a hostile environment is specifically included in this statute. Sexual harassment via E-mail may therefore be prosecuted under this statute. McGraw makes the point that employers have a strong incentive for taking sexual harassment in any form seriously since a suit can be brought against the employer because of the hostile environment interpretation by the courts.

In a similar vein as Title 42, Title 20 of the Civil Rights Act,⁵⁵ addresses discrimination problems in higher education. Women who are victims of sexual harassment via E-mail can find remedies in this statute. Unfortunately, the statute is clearer regarding harassment by school officials than it is harassment of one student by another.⁵¹ This statute, however, remains an avenue of redress for victims of online harassment. Regardless of vagueness in this federal statute, college campuses in particular are addressing this issue in their student conduct and disciplinary codes as a result of the proliferation of E-mail harassment on college campuses.¹⁹

The biggest gap in the current laws entails protecting victims from unknown harassers.⁵¹ Women (and men) unaware of being victimized online, are unable to mobilize legal protection to prevent increased harm. Internet users may be knowledgeable about the many means of electronic communication. Individuals unfamiliar with the Internet are at a complete disadvantage in protecting themselves.

*These states are: Alabama, Arizona, California, Connecticut, Delaware, Hawaii, Idaho, Illinois, Indiana, Massachusetts, Minnesota, New Hampshire, and Oklahoma.

Two recent cases involving unaware victims illustrate the inadequacy of current laws. The first involved a woman who was stalked through a perpetrator's creation of a false identity for her on the Internet.⁵⁶ She was only able to get the attention of the police after she conducted her own investigation and provided the police with evidence of the harassment. The second unfortunate case entailed a woman who was killed after her murderer conducted an online investigation to locate her and revealed his intentions in his own website.⁵⁴ In both situations, laws governing privacy protection were unable to assist the victims.

Extralegal remedies available to online victims are actions able to be initiated without involvement of law enforcement officials. Changing one's E-mail address and provider is one of the first actions a victim might take. Along with this, removing any personal or gender identifying information alleviates some possibilities having unwanted attention.⁵⁸ Ignoring or sending clear statements to the sender that their communication is unwanted may be effective in ending the harassment. With repeated unwanted contact, another action may be to inform the system administrator of the sender's site.⁵¹ The federal laws governing telecommunication mandate that computer systems regulate behavior on that system. Finally, as implied above, should the victimization occur within the workplace or educational setting, notifying the workplace or educational administration may trigger the protective mechanisms needed.

Legal remedies entail use of orders of protection to prevent further contact or tort laws to seek damages as a result of wrongful actions. Orders of protection are typically described in state domestic violence or child abuse statutes and are obtained in district courts after evidence of a threat of harm is produced. The importance for online victims when seeking the attention of law enforcement or the courts is to save and make hard copies of all threatening of harassing electronic communications. Grossman.⁵⁸ makes the important point that police or the courts may never have handled a case of online victimization, so it is imperative to document the harassment or cyberstalking that is occurring. Finally tort remedies (filing a suit against an alleged perpetrator to seek damages)

may be sought if there is assault, intentional infliction of emotional distress and of invasion of privacy.⁵¹

IMPLICATIONS FOR CONSUMERS

The Internet exists within the broader context of a sexist society in which women are disproportionately victims of violence, sexual assault, sexual harassment, invasion of personal space, and "romantic pursuit." Given that cues regarding social status and group norms are largely absent on the Internet, it is not surprising that women are victimized in cyberspace as well. In the larger society, part of women's socialization is to learn survival skills in a hostile environment. They learn where and when it is safe to travel in public. They come to understand cues that signal their interest or lack of interest in engaging in interactions that may be considered romantic or sexual. They learn about sexual harassment, rape, and domestic violence, and the resources available to them help if problems arise. Socialization for survival in cyberspace has not yet become part of the normal growing-up experience of women. For their safety, women who use the Internet, especially those who have been victims of violence or are emotionally vulnerable, need education about the kinds of victimization that can occur online, how best to prevent it, and what to do if victimization occurs. They need information about password protection, encryption software, blocking and filtering software, anonymous remailers, alternate email receiving sites, chatroom and newsgroup safety, the potential for misinformation, how privacy may be lost, how to deal with online harassment, policies and laws regulating (or not regulating) interactions in cyberspace, and where to get help if victimization occurs. There are a number of websites that provide education and resources to promote online safety. A few include:

- Women Halting Abuse Online (W.H.O.A. <http://whoa.femail.com/>) provides education about online harassment, empower victims of, and voluntary policies that systems can adopt in order to create harassment-free online environments.

- Stalking Victim's Sanctuary (<http://www.stalkingvictims.com/>) provides information and resources primarily for those who have been victims of stalking. The site also has an online support group and online chat for discussions of stalking.
- Cyberangels (<http://www.cyberangels.org/>) provides online safety tips primarily for families and children. They also address practical and legal concerns regarding online stalking.
- SafetyEd (<http://www.safetyed.org/>) provides online education regarding online safety and privacy. This site also focuses on child safety but include issues related to cyberstalking. They include research articles, online workshops, and links to many privacy-related organizations.
- Safer Dating (<http://www.saferdating.com/>) provides guidelines for handling online dating-related relationships, safety procedures for privacy protection, and stories of positive and negative online relationships, including cyberstalking.

IMPLICATIONS FOR HUMAN SERVICE ORGANIZATIONS

Identity

Women constitute the majority of the consumers of human service organizations. Public and nonprofit agencies and organizations provide online counseling and support, crisis hotlines and services for victims of rape and domestic violence, parent education, family planning, advocacy, and policy change efforts, among others. In order for online human service organizations to be effective, however, women must feel safe accessing them in cyberspace. Given the prevalence of misrepresented identity and misinformation in cyberspace, human service providers must take steps to help consumers recognize that they are legitimate organizations. In addition to providing online information about their mission, goals, and affiliations, human service organizations should develop a system in which a responsible umbrella organization provides a

graphic on a website indicating that the organization meets certain professional standards. This is already becoming common practice in other areas. For example, private practitioners can participate in the Credentials Check site discussed previously. Other sites, such as Women Halting Abuse Online, provide a graphic indicating that a site meets standards for preventing online harassment. Human service organizations must develop a clear and visible way to help consumers identify legitimate human services.

Privacy, security and confidentiality

Victimization of those seeking human services online is more likely because of the increased risks to the privacy, security, and confidentiality of their records when using online service delivery. Human service professionals are both ethically and legally bound to maintain the confidentiality of client records.⁶⁰ Online practice, however, creates new ways in which confidentiality might be breached. E-mail is not a secure medium. Agency messages to a consumer can be intercepted in transit by computer hackers.⁶¹ They can also be printed, inadvertently rerouted, and read by others if left on a computer screen in a nonsecure environment. Messages can also be read by anyone with access to the consumer's computer (e.g., a spouse or parent). Finally, the privacy of online records is also threatened when clients use their work computers to send and receive online health and human service information. The courts have ruled that an employer can read all E-mail residing on computers using the company network as long as workers are informed that company policy permits it.¹²

Human service organizations should institute measures to protect the confidentiality and security of online messages through using password protection of their computer and maintaining storage of back-up files in a secure place. In addition, encryption software programs should be used to prevent messages from being read by anyone but the intended receiver. Clients should be informed if and for how long their messages are being preserved as part of their file, and agencies should obtain signed informed consent before any materials

are forwarded to another party. Human service organizations should also provide materials that educate their clients about security risks of online communication and legal issues related to the use of E-mail at the workplace. Finally, human service agencies and private practitioners should establish written policies that establish how E-mail is to be used, by whom, and what the sanctions are for violation of those policies.

Education

The risks and dangers in using online resources are not yet common knowledge. Human service agencies should be proactive in educating consumers about their own privacy, security, and confidentiality policies regarding online transactions. In addition, they should raise the consciousness of consumers about these issues in relation to the broader victimization possibilities involved in online communications. Agencies do not need to recreate this information. Rather, each human service agency website, no matter what its primary mission, should consider having links to resources that discuss online safety and privacy issues.

"Spam" and disruption

Just as women may be the targets online harassment, agencies seeking to provide online services to women, such as those providing services in the areas of domestic violence, family planning, and gay/lesbian issues may also be the targets of online disruptions. Because human service agencies can face hostility from some segments of society, they may encounter attempts to disrupt their website through E-mail spam, viruses, provocative messages, or false email requests for help. Spam may involve conscious attempts to hurt a particular agency by disrupting the site's ability to operate by flooding the site with thousands of messages and faxes. In a study of domestic violence sites, two agencies reported receiving E-mail threats to staff through their website.⁶² Human service organizations will need to train staff and volunteers on how to be aware of, and respond to, the range of messages that they may receive, and to consider the use of E-mail filters and

virus protection software. In addition, they will need to work with their ISP in the event of on-line harassment.

CONCLUSION

At the beginning of the new millennium, the Internet has the potential to empower women by allowing them access to information and social support regarding their physical and mental health concerns and by facilitating online advocacy for changes in public and organizational policy. There are risks and potential hazards, however, that need to be confronted. Inaccurate information, loss of privacy, disinhibited communication, online harassment and cyberstalking can all lead to online victimization. Users, both individuals and human service agencies, must understand and protect against these dangers if the potential of the Internet to provide services is to be realized.

Prevention and education about online safety issues are necessary but not sufficient. Laws are reflective of societal values and principles in rules of social conduct.⁶³ The Internet has evolved faster than laws that govern it. Legal mechanisms that both inhibit online abusive behavior and punish it must be developed nationally. No doubt, much of the work involved in advocating for these laws will be done online.

REFERENCES

1. Finn, J. & Holden, G. (2000). *Human services online: A new arena for service delivery*. New York: Haworth Press.
2. Ferguson, T. (1996). *Health Online*. Reading, MA: Addison-Wesley.
3. Newburger, E.C. (1997). Computer use in the United States. Current Population Reports, U.S. Census, Online, October 27, 1999: <http://www.census.gov/prod/99pubs/p20-522.pdf>.
4. Glassner, J. (1999). Gender Gap? What Gender Gap? Wired News, November 8, Online: <http://www.wired.com/news/print/0,1294,32327,00.html>.
5. Green, H., & Himelstein, L. (October 19, 1998). A cyber revolt in health care. *Business Week*, p. 154.
6. Zeff, R. (1996). *The nonprofit guide to the Internet*. New York: Wiley.
7. Finn, J. (1999). Seeking volunteers and contributions: An exploratory study of nonprofit agencies on the In-

- ternet. *Journal of Technology and Human Services*, 15(4), 39–56.
8. Brandt, M.G. (1998). Local nonprofit organizations at work: A composite vision of a community presence on the World Wide Web. Online: <http://www.uwm.edu/People/mbrandt/toc.htm>.
 9. Ensmann, R.G. (1997). Turn small shops into big shops via the Internet. *Fund Raising Management*, 28: 18–19.
 10. Finn, J. (1999). An exploration of helping processes in an online self-help group focusing on issues of disability. *Health and Social Work*, 24:220–231.
 11. Childress, C. (1998). Potential risks and benefits of online psychotherapeutic interventions. International Society for Mental Health Online. Online, February 17, <http://www.ismho.org/issues/9801.htm>.
 12. Pergament, D. (1998). Internet psychotherapy: Current status and future regulations. *Journal of Law Medicine*, 8:233–280.
 13. Lebow, J. (1998). Not just talk, maybe some risk: The therapeutic potentials and pitfalls of computer-mediated conversation. *Journal of Marital and Family Therapy*, 24:203–206.
 14. Huang, M. & Alessi, N. (1996). The Internet and the future of psychiatry. *American Journal of Psychiatry*, 153:861–869.
 15. Trabin T.L., & Freeman, M.A. (1996). *The Computerization of Behavioral Health Care*. San Francisco, CA: Jossey-Bass.
 16. Walther, J. (1997). Group and interpersonal effects in international computer-mediated communication. *Human Communication Research*, 23:342–369.
 17. Young, K.S. (1998). *Caught in the Net*. New York: John Wiley & Sons.
 18. Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukhopadhyay, T., & Scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological Kutchins, H. & Kirk, S. (1987). DSM-III and social work malpractice. *Social Work*, May–June, 205–211.
 19. Lee, R. (1998). Romantic and electronic stalking in a college context. *The College of William and Mary Journal of Women and the Law*. Spring, 373–409.
 20. Jenson, B. (1996). Cyberstalking: Crime, enforcement and personal responsibility in the on-line world. Online: <http://www.law.ucla.edu/classes/archiv/s96/340/cyberlaw.htm>.
 21. Dutton, D.G. (1995). *The domestic assault of women*. (2nd ed.) Vancouver, BC: University of British Columbia Press.
 22. Tannen, D. (1994). Gender gap in cyberspace. *Newsweek*, May 16, p. 52.
 23. Davis, L., J. Hagen; T. Early. (1994). Social services for battered women: Are they adequate, accessible, and appropriate? *Social Work*, 39:695–704.
 24. Stofle, G.S. (1999). Thoughts about online psychotherapy: Ethical and practical considerations. Online, February, 1999: <http://members.aol.com/stofle/onlinepsych.htm>.
 25. Holden, G., Bearison, D., Rode, D., Rosenberg, G., & Fishman, M. (1999). The impact of a virtual environment on hospitalized children: A pilot study with aggregation of the results of replicated single system designs via meta-analysis. *Research on Social Work Practice*, 9:365–382.
 26. Schopler, J.H., Abell, M.D. & Galinsky, M.J. (1998). Technology-based groups: A review and conceptual framework for practice. *Social Work*, 43:254–267.
 27. Finn, J. & Lavitt, M. (1994). Computer-based self-help groups for sexual abuse survivors. *Social Work with Groups*, 17 (1/2):21–45.
 28. Holmes, L. (1997). You can't do psychotherapy on the net, yet. Paper presented at the American Psychological Association Annual Convention, August, 1997. Online: February, 1999, <http://mentalhealth.miningco.com/library/aa010499.htm?/pid=2791&cob=home>
 29. Bloom, J. (1998). The ethical practice of Webcounseling. *British Journal of Guidance and Counseling*, 26:53–60.
 30. Sampson, J.P., Kolodinsky, R. & Greeno, B. (1997). Counseling on the Information Highway: Future possibilities and potential problems. *Journal of Counseling and Development*, 75:203–212.
 31. Appelman, D.L. (1995). The Law and the Internet. Online July 21, 1998: <http://inet.nttam>
 32. Reamer, F.G. (1998). *Ethical standards in social work: A critical review of the NASW Code of Ethics*. Washington, DC: NASW Press.
 33. Speilberg, A. (1998). On call and online. *Journal of the American Medical Association*, 280:1353–1359.
 34. Hafner, A.W. (1989). Computers and the legal standard of care. *Archives of Ophthalmology*, 107:966.
 35. Banks, M.A. (1998). Web psychos, stalkers, and pranksters: How to protect yourself in cyberspace “ Online: <http://w3.one.net/~banks/psycho.htm>
 36. Sharf, B. (1997). Communicating breast cancer on-line: Support and empowerment on the Internet. *Women & Health*, 26:65–84.
 37. Brennan, P.F. & Fink, S.V. (1997). Health promotion, social support, and computer networks. In: Street R.L., Gold W.R., & Manning T. (Eds.), *Health promotion and interactive technology*. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 157–170.
 38. Winzelberg, A. (1997). The analysis of an electronic support group for individuals with eating disorders. *Computers in Human Behavior*, 13:393–407.
 39. Dunham, P., Hurshman, A., Litwin, E., Gussilla, J., Elleworth, T., & Dodd, P. (1998). Computer-mediated social support: Single young mothers as a model system. *American Journal of Community Psychology*, 26:281–306.
 40. Mickelson, K. (1998). Seeking social support: Parents in electronic support groups. In: Kiesler S. (Ed.), *Culture of the Internet*. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 157–178.
 41. Braithwaite, D., Waldron, V., & Finn, J. (1999). Communication of social support in computer mediated self help groups,” *Health Communication*, 11:123–151.
 42. Sproul, L. (1986). *Using electronic mail for data collec-*

- tion in organizational research. *Academy of Management Journal*, 29:159–169.
43. Sproull L., & Kiesler, S. (1986). Reducing social context cues: Electronic mail in organizational communication. *Management Science*, 32:1492–1512.
 44. Waldron, V., Lavitt, M. & Kelley, D. (2000). The nature and prevention of harm in technology-mediated self-help settings: Three exemplars. *Journal of Technology in Human Services*, 17 (in press).
 45. Mullen, P.E. & Pathe, M. (1994). Stalking and the pathologies of love. *Australian and New Zealand Journal of Psychiatry*, 28:469–470.
 46. Zona, M. (1992). A comparative study of erotomaniac and obsessional subjects in a forensic sample. *Journal of Forensic Science*, 28:894–895.
 47. Wildangel (1998). Stories of Stalking. Online December 22: <http://www.wildangel.com/stalk2.htm>.
 48. Whitelaw, K. Fear and dread in cyberspace. *U.S. News and World Report*, 121(18), 50.
 49. U.S. Government Accounting Office (1998). *Report No. GGD-98-100BR*. Also online: <http://www.gao.gov>
 50. Carmody, C. (1994). Stalking—law & legislation. *American Bar Association Journal*, 80:68–72.
 51. McGraw, D. (1997). Sexual harassment in cyberspace: The problem of unwelcome E-mail. 20 *Rutgers Computer and Technology*, 491.
 52. Barton, G. (1995). Note & comment: Taking a byte out of crime: E-mail harassment and the inefficacy of existing law. 70 *Washington Law Review*, 465.
 53. Katsh, E. (1993). Law in a digital world: Computer networks and cyberspace. 38 *Vill. L. Rev.* 403, 427.
 54. *Crimes and Criminal Procedures, Wires and Electronic Communication Interception and Interception of Oral Communication*. Title 18. 18 U.S.C. 2510 (1999).
 55. *Civil Rights, Discrimination Based on Sex or Blindness Act of 1999*. Title 20. 20 U.S.C. 1681–(a)(1)(1999).
 56. Foote, D., & Van Boven, S. (1999). You could get raped. *Newsweek*, 133:64–66.
 57. Barry, E. (1999). Killer's dreams bared on the Internet. *The Boston Globe*, November 29, B1.
 58. Grossman, M. (1997). What to do when on-line stalker strikes. *Palm Beach Daily Business Review*. May 9, p. B1.
 59. McGraw, D., op. cit.
 60. Kagle, J. & Kopels, S. (1994). Confidentiality after Tarasoff. *Health & Social Work*, 19:217–222.
 61. Johnson, D.G. (1994). Crime, abuse, and hacker ethics. In *Computer Ethics*. Englewood Cliffs, NH: Prentice-Hall, Inc., pp. 40–55.
 62. J. Finn (2000). Domestic Violence Organizations on the Web: A new arena for domestic violence services. *Violence Against Women*, 6:80–102.
 63. Hafner, A.W. (1989). Computers and the Legal Standard of Care. *Archives of Ophthalmology*, 107:966.

Address reprint requests to:

Jerry Finn
University of New Hampshire
Department of Social Work
Durham, NH 03824

E-mail: JFWW@cisunix.unh.edu

Copyright of CyberPsychology & Behavior is the property of Mary Ann Liebert, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.