©ADVANCES IN SOCIAL WORK, VOL. 1, NO.1, SPRING 2000

Ethical Interaction in Cyberspace for Social Work Practice

Stephen M. Marson
Sara B. Brackin

ABSTRACT: *The nature of ethics on the Internet may be confusing to some social workers because of the unique characteristics of client contacts in cyberspace. This article addresses three basic issues/questions that clarify the ethical relationships among clients, other professionals and the Internet. These include: a) What must I do to maintain professional ethical standards on the Internet? b) How do I deal with the unethical interaction of others within cyberspace? c) How do I examine and analyze ethical issues with no clear guidelines?*

Social workers are not alone in noting the complexity of online ethics. Ethical issues equally perplex computer professionals. Laudon (1995:33) states, "There is an ethical vacuum in cyberspace." Stager (1993) shows that there is no clear consensus among computer center directors regarding their legal and ethical obligations. Wood (1993) illustrates that the computer professional's length of experience has little or no influence on understanding computer ethical dilemmas. A computer professional with limited experience can understand the dynamics of ethical decision-making as well as one with 20 years' experience. Neither adequately understands ethics. Wood adds that he does not see any changes in the foreseeable future, and Stager recommends establishing ethical policies at the institutional level

In clarifying the analysis of online ethics, ethical interaction can be divided into two mutually exclusive perspectives. First, some aspects of Internet interaction are so unique that current professional ethical codes cannot provide guidance. These online interactions are unique because they emerged solely from a new technology unfolding new social and ethical norms. Second, some aspects of Internet interaction are *not* unique.

Stephen M. Marson, Ph.D., ACSW, is Professor/Director, Social Work Program, and Sara B. Brackin, MA, is Assistant Registrar and Information System Liaison at University of North Carolina at Pembroke, Pembroke, N.C.

The medium is new but the interactions and ethical dilemmas can be as old as personkind. Unfortunately, the new medium sometimes muddies one's ability to acknowledge that ethical behaviors face-to-face share common ground with ethical interactions in cyberspace. This article reviews the two perspectives by examining both the online implications of the current professional code of ethics and those of established online guidelines.

The authors believe that the most effective method of summarizing and simplifying the practical application of ethical conduct in cyberspace is found in Figure 1.

Figure 1

Source of Ethical Concern

		Self	**Others**
Level of Commonality Between Real World and Cyberspace	**Common**	Code of Professional Ethics Standards of Practice	Control of Outgoing Information Locking Doors
	Unique	Emoticons Bandwidth Flamewars	Cookies Passwords Encryption

The first step in conceptualizing ethics is to appreciate that ethical conduct in cyberspace has a common bond with activity in the real world, but paradoxically it also has unique features. The second step is to acknowledge that sources of ethical concern in cyberspace must include evaluating self-motivation and assessing one's vulnerability to unscrupulous others. The issues addressed in the cells were introduced in this article, but are clearly incomplete. The matrix helps us unlock the seemingly mysterious nature of cyberspace. Ethical conduct in cyberspace has much commonality with the real world with some deviations. In a sense, studying ethical conduct on the Internet is a study of human diversity and should be approached in the same manner.

Despite the lack of clear ethical guidelines, many professionals are providing "therapy" over the Internet. Morrissey (1997) reports that this practice has prompted many intense debates about the lack of regulation and professionalism. In her article, she reports on concerns that have surfaced about providing ethical guidelines with so many undefined parameters. For example, Morrissey states when a professional organization provides guidelines for cyberspace ethics, it is in effect endorsing this kind of service. Lee (1998) sees Web counseling as counter to the standard therapeutic relationship, but agrees that intervention has merit for the new generation of cyberspace clients. Web counseling would eliminate physical closeness and the ability to observe clients in the environment. Lee expresses optimism about the newly established standards for the ethical practice of Web counseling published by the National Board of Certified Counselors. Hughes and Ruiz (1998:11) state, "There are undeniable values in Internet technology for counselors. It has great positive potential, yet we need to always be aware of the potential pitfalls."

The act of communicating over the Internet (newsgroups, chat rooms, discussion groups) is a multilevel activity. If a professional organization publishes ethical standards, the court can impose legal sanctions with ease (Legal Research Network, *et al.* 1996). As a result, counseling over the Internet is being scrutinized. Professional Internet communication guidelines for mental health professionals have been noticeably absent and many of the early Web counseling sites reflect questionable professional judgment. Anyone can offer Web counseling and there is no apparent process in place to verify the professional's credentials or ensure client confidentially. For example, the Institute of Transcedendent Analysis (http://www.itai.com) charges $100 for 30 minutes of therapy with a transcendent analyst. There are no names associated with their analysts. The Institute also offers a discount for clients who join ($300 for membership) and a money back guarantee if their overall level of functioning does not improve within the first three sessions. Our review of this and other Web counseling sites suggest that many professionals do not understand that normal ethical protocols (i.e., confidentiality) are *also* applicable to cyberspace intervention.

Bloom (1997) reports on the National Board of Certified Counselors (NBCC) recently approved standards for Web counseling. While not an endorsement of the practice, these standards result from a need to encourage those professionals engaging in online practice to follow ethical guidelines (Morrissey, 1997). However, Bloom questions where ethical responsibility lies. Some mental health professionals have organized and established ethical standards for Web counseling. The following web sites are relevant:

- http://www.metanoia.org/imhs is a consumer's guide to Internet therapy,
- http://www.mhnet.org assesses the quality of Internet therapy sites, and
- http://netpsych.com/web.htm is a clearinghouse for information regarding Internet therapy.

Nationally known professional organizations do not seem to be taking a lead role in assessing the ethical concerns of these therapy sites. The APA (American Psychological Association, 1997) has issued several statements about services by telephone, teleconferencing, and Internet (http:///www.apa/org/ethics/stmnt01.html). At the time of this writing the statement reads:

> In those emerging areas in which generally recognized standards for preparatory training do not exist, psychologists nevertheless take reasonable steps to ensure the competence of their work and to protect patients, clients, students, research participants and others from harm.

In other words, the APA recognizes that the present code of conduct is not specific with regard to Web counseling. The statement concludes that no present code of ethics bars counseling over the Internet and further stresses that psychologists engaged in this type of counseling must consider how service delivery, client confidentially, and all other characteristics are applicable to the present code of ethics.

MAINTAINING ETHICAL STANDARDS

All cyberspace interactions that have ethical implications do not reflect the same level of seriousness. For example, simple courtesies unique to cyberspace or netiquette fall within the realm of online ethical interaction (Shea, 1994). Unlike other ethical transgressions, violations of netiquette do not fall within the realm of legal sanctions, but the repercussions are social sanctions that include serious cyberspace punishment. For example, the law firm of Canter & Siegal posted the following message on thousands of newsgroups:

> Do you want to get a green card for permanent residence in the
> United States? THE TIME TO START IS NOW!

Over 30,000 users flamed Canter & Siegal, which crashed the firm's computer and led Internet Direct Inc. to terminate their Internet access (Gilpin, 1995). What is confusing about netiquette is that some behavioral standards are unique to cyberspace and do not exist in the real world. On the other hand, many standards of cyberspace behavior are easily recognized from the real world.

NETIQUETTE RULES—UNIQUE TO CYBERSPACE

The most confusing aspect of the code of Internet interaction is that it varies from one location in cyberspace to another. For example, the interactive expectations on a mail list are different from those for a newsgroup. It is common for a particular newsgroup to embrace its own unique code of conduct—different from other newsgroups' code. Serious violations of these codes are dealt with serious social sanctions[1]. Users (either in a newsgroup or a mailing list) attack the offender. How does one learn "how to act?" Shea (1994:60) writes, "Lurk before you leap." Prior to participating, observe and learn how people interact. In this respect, cyberspace applications should be approached in the same manner as any new or unique real social setting. Three unique characteristics of cyberspace merit special attention because they have no functional equivalent in reality. They include: emoticons, bandwidth issues, and flame wars.

Emoticons

Often joking or sarcasm cannot be clearly articulated in the printed word. Emoticons are critical aspects of communications because they are the functional equivalent of facial expressions or tone of voice in which non-verbal messages are transmitted. Although hundreds are employed, some of the most commonly used can be found in Figure 2:

Figure 2

Most Common Emoticons

Emoticon	**Meaning**	**Emoticon**	**Meaning**
:-)	The smiling face.	:-\	The undecided face.
;-)	The winking face.	:-o	The shocked face.
:-(	The unhappy face.	:-&.	A tongue-tied face
:-t	The cross face.	:-#	Lips are sealed face

Emoticons facilitate clarity of meaning. Although they appear humorous, they are critical for imparting ethical standards to others (Argyle & Shields, 1996).

Bandwidth Issues

Bandwidth refers to the volume of information that hardware and software can handle in a given period of time. In nonacademic settings, bandwidth can create a serious problem. Some commercial vendors have a fee schedule for the space and time utilized by a subscriber. Outside of cyberspace, there is no functional equivalent for this term. Unlike the spoken word, cyberspace communication must be more economical because many users are charged for bandwidth. When we are transmitting to a newsgroup or a discussion group, we must be thoughtful of the bandwidth available to others.

Flame Wars

Deliberately insulting another user may result in numerous emails, each becoming more vicious. These emails can flood a location and crash a system. Some people who enjoy upsetting the balance of a discussion group will send offensive remarks to one or more users. These disrupters remaining anonymous or, impersonating another person, become invisible in cyberspace. This cloak allows them to exercise morally disreputable behavior and avoid detection (Parker, 1995). When users begin to respond to the remarks, a flame war may develop. Flame wars are not intended as lively discussions and by nature are destructive. It is best to avoid them.

NETIQUETTE RULES—A REMINDER OF COMMON COURTESIES

Five general guidelines are shared by both cyberspace and the real world (Shea, 1994). They include:

- Do not use harsh or offensive language
- Be willing to share expert opinions
- Respect others' privacy
- Be forgiving of grammar and spelling slips (first drafts are commonly transmitted)
- Do not exploit one's knowledge of cyberspace toward new cyberspace residents

These guidelines reflect basic human courtesies and are essential components of effectively communicating with others in the real world *and* cyberspace. If one is caught in a flame war or is being personally attached by another user, the best advice is to discontinue further communication with that person or discussion group. When making an important point about a subject that might be interpreted as argumentative, remember to use emoticons. Emoticons clarify one's intent and allow the discussion to remain productive.

Professional Code(s) of Ethics

From an historical perspective, Oz (1993) points out that professional ethical codes for computers technicians and other users generally precede the development of laws governing actions on computers. Thus, awareness of one's professional code of ethics becomes the centerpiece of behavior on the Internet. Reamer (1998) offers an excellent outline and critique of National Association of Social Worker's ethical (NASW, 1996) responsibilities to clients, colleagues, practice settings, and, as a professional, to the profession and society. However, he does not elaborate on the online implications for social work because the Code does not explicitly articulate online issues.

Unlike the APA or NBCC, NASW[2] does not explicitly articulate ethical guidelines for online practice. As a result, an individual social worker must extrapolate meaning from the NASW Code of Ethics. This requires more interpretation on the part of the social worker versus those required by counselor or psychologist. However, the process of applying ethics to online activity is not complex. Figure 3 illustrates a selective commentary on the technological interpretation of the NASW Code of Ethics. It is an example of what a professional must do if no specific online guidelines are written by one's professional organization.

Figure 3
Technological Interpretation of the NASW Code of Ethics

- Social workers are required to be knowledgeable about all practice tools including new technologies. Social workers are expected to pursue appropriate education, training, consultation, research and supervision to ensure the protection of clients (standard 1.04 a-c).

- To the extent that is available, social workers should base their learning about online technologies from recognized experts and empirical based research (standard 4.01 b, c).

- Valid and informed consent must be given to cyberspace clients. Social workers must articulate on the web page and in understandable language: 1) purpose of services; 2) cost; 3) alternative treatments; 4) the right to refuse treatment or withdraw consent; 5) time frame of consent; 6) an opportunity to email questions; and 7) the risk and limitations of obtaining treatment via cyberspace (standard 1.03 a, b, c, e).

- Social workers must not only be sensitive to cultural and ethnic issues within the client's experience, but also must be cognizant of the social norms and values held in cyberspace (standard 1.05 b, c).

  Social Workers must not exploit clients with their knowledge of cyberspace (standard 1.06 b).

- On their web sites, social workers must clearly represent their qualifications, credentials, education, competence, affiliations, services provided, results to be achieved from their services and other dimensions of practice that testify to the quality of service (standard 4.04, 4.06 c). Cyberspace services have a clear advantage over treatment available in the real world in that the ethics can be available on the web page without having to verbally repeat it to each new client.

- Social workers may not use derogatory language in cyberspace and must be respectful of clients (standard 1.12).

- Once the process of service begins, the social worker must make an effort to assure technological problems do not interrupt treatment (standard 1.15).

- Social workers must have a system (adapted for cyberspace) by which he/she can determine if and when services are no longer required. In addition, social workers are expected to have a reasonable alternative or backup plan that would prevent a client from feeling abandoned (standard 1.16 a, b).

- When the social worker does not have the competence to address the client's problem situation, the social worker must refer to another professional. Such a referral includes employing cyberspace to locate a competent professional -- assuming that the client specifically desires cyberspace intervention (standard 2.06).

- If for any reason, the social worker anticipates an interruption or termination with treatment incomplete, the social worker is obligated to assure that the client receives email explaining the situation. The social worker is obligated to offer alternative treatment - in cyberspace if desired by client (standard 1.16 e).

- Fees and payment method must be clearly spelled out on the social worker's web page. Fee transfer must be completed in a manner that insures confidentiality and secures private financial transactions (i.e., security for credit card numbers) (standard 1.13).

- Social workers must apply cutting edge standards of security in the computer storage of client records (standard 3.04 a-c).

- Social workers must articulate legal limits of confidentiality. This is especially complex because of difference in state

Figure 3 continued...

statutes. The client and social worker are likely to be located in different states or even countries (standard 1.07).

- Social workers must conduct relevant research and evaluation to assess the impact of online services (standard 5.02 a-c).

Every professional is legally bound to adhere to his or her code of ethics. In cyberspace intervention, this means one must search the code and from it extrapolate the context for cyberspace practice.

DEALING WITH UNETHICAL INTERACTIONS WITH OTHERS

From an ethical perspective, the best analogy for cyberspace is the "Wild West." Without law enforcement, everyone must become self-protective. Cyberspace is a new frontier. As in the Wild West, cyberspace inhabitants must consider the ethical transgressions of others. Major concerns in cyberspace are password protection, encryption, and defense against viruses and worms.

Password Protection

The password is the first line of defense in protecting client confidentiality. Social workers have an especially important responsibility to protect their computer passwords. Crackers,[3] knowing that many cyberspace practitioners do not understand the concept behind the password, have a long history cracking passwords. Disregarding standards for password selection can put a client in serious jeopardy (Rock & Congress, 1999). Stoll (1990) vividly demonstrates the sanctity of passwords. Stoll lays out a story of how spies were able to break into a large number of university computer systems. As a result, the spies (or crackers) were eventually able to tap information from the United States Defense Department.

The accepted standard for password selection can be found in any basic computer article or reference book (Marson, *et al.*, 1994; Raymond, 1996; Santa Cruz Operation, 1995). Guidelines in selection are critical for any cyberspace practitioner housing confidential computer files. If a service provider is found in non-compliance of standard password security measures, a client has solid grounds for a malpractice suit (Legal Research Network, Inc *et al.*, 1996; Sheldon *et al.*, 1999). When selecting a password one must understand how passwords are broken.

The typical methods employed to break passwords include:

- A caller representing himself/herself as being from the computer department asks the secretary to provide the logon ID and other information necessary to get into an account.

- Getting someone's account by watching keystrokes when the password is inputted is extremely common. Some crackers are adept enough at this to be able to do it from across a room.

- Most people adopt a password that is fairly obvious to them—typically the name of their pet, their husband or some other close everyday item that is a favorite of theirs. "Crack" dictionaries exist that will successively attempt to login to an account using all the words in that dictionary.

Counter measures that foil attempts to break a password include:

- Do not share a password with anyone. Instruct your staff not to share one, either.

- Never invoke a password with someone present in your office. This is the functional equivalent of talking about a client in a hallway.

- Never use a password that can be found in any database. Memorize a password and never write it down. Use a mixture of numbers, letters, symbols, and punctuation. Use both upper and lower case letters.

- Change your password at least once every three months.

Encryption

Encryption is the translation of data into a code called cipher text. Only persons with a password or secret key can decode the encrypted data. Encryption is the best method for complying with ethical standards of confidentiality. If we apply the existing standards of NASW, APA, and NBCC concerning a client's right to confidentially, then encryption is a necessity for *all* cyberspace therapy. NBCC's (1997) standards for the ethical practice of web counseling states: "Inform Web clients of encryption methods being used to help ensure that security of client/counselor/supervisor communications." *Any* encryption code can be broken (Electronic Frontier Foundation, 1998) and this is an important point to stress to a client. Almost all web sites boast of secure communications and encryption methods. It is the responsibility of the counselor or therapist to ensure that methods being used are adequate to protect the clients' confidentially. A good example of how encryption and confidentially can be used can be seen by visiting one of the following web sites:

http://www.flash.net/~wmartin/confidentiality.htm
http://www.flash.net/~wmartin/privacy.htm

Defense Against Viruses and Worms

It is impossible to *completely* protect an Internet connected computer from viruses and worms. Software programs can protect a system from being infected, but these programs are vulnerable to unknown viruses and worms. Johnson (1994) defines virus as any unwanted code, specialty machine code, that will attach itself to another program. When this code is activated, the virus is executed and spread. A virus can delete data files and system files rendering the computer useless. A worm is similar and can be as destructive as a virus. A worm is an independent program that may be running at several different locations. Worms can be used to gather and send information and to infiltrate a system for the purpose of copying information that can be used to break into the systems. The people responsible for these destructive acts are called crackers. Johnson (1994) reports that crackers' mentality is that all information is free without regard to the type of information. Crackers believe they are serving an important role by showing others where the leaks and flaws exist in their systems.

The best protection against virus and worm infections includes:

- Constantly update virus protection software.
- Follow the guidelines for password protection.
- Beware that anything downloaded from the Internet may be infected.
- Beware that any file or program uploaded floppy or CDROM may be infected.
- Email from unknown persons or sources may be infected. Delete the entire email.
- Do not open any unknown executable program sent to you or attached to email. Delete the entire email.
- Be aware that files can contain macros or embedded programs. These programs may execute when the file is open.

- Do not copy pirated software. It is often infected.

The precautions above may seem overly harsh. They are not. A Web page that advertises secure transmission or encryption presents a challenge for an unscrupulous cracker. The challenge of breaking into or destroying a computer system is the underlying motivation for a cracker.

Examining and Analyzing Ethical Issues

Two methods can be employed to address ethical dilemmas that surface but do not appear to be articulated implicitly or explicitly in a standard ethical code: 1) use ethical theories; 2) self questions.

Ethical Theories

Spinello (1997) and Van Den Hoven (1998) provide excellent illustrations of how and why ethical theories are necessary in the computer age. Spinello (1997) reviews Utilitarianism, Kant's moral philosophy, W.D. Ross's moral philosophy, and Rawl's Theory of Justice. He provides a contrast among them by stating (p. 44):

> Despite these differences, each approach represents a unique perspective from which one can assess and deliberate over moral issues. All of these theories seek to elevate the level of moral discourse from preoccupation with "feelings" or gut reaction to a reasoned and thoughtful consideration of the right course of action. Reliance on these theoretical frameworks therefore will surely improve the clarity and substance of ethical decision-making.

Every ethical theory has a flaw, but Spinello (1997)insists that the theories provide the best basis for making decisions regarding situations that are not clearly addressed in a code of ethics.

Van Den Hoven (1998) is much more practical in his analysis of ethical theories. He reviews the general tenets of ethical theories and concludes that the most effective theoretical approach to resolving ethical dilemmas created by computer technology is John Rawl's "Method of Wide Reflective Equilibrium" (WRE). He states:

> WRE incorporates the best of both the universalist and the particularist worlds. It allows for appeals to considered judgments and intuitions concerning particular cases and

> acknowledges the appropriateness of appeals to general principles that transcend particular cases. (p. 242)

In brief summary form, Van Den Hoven (1998) notes that WRE is composed of a set of three beliefs. These include: a) considered moral judgments, b) moral principles, and c) relevant background theories. The disciplined WRE user resolves moral dilemmas by intellectually shifting among sets of beliefs.

Self-Questions

The works of Spinello (1997) and Van Den Hoven (1998) were primarily written for engineers, computer programmers, and computer consultants. Thus, their intent has to be stretched to have meaning for social workers. After explaining that each ethical theory has good points and bad; and that ethical theories have fundamental and unresolvable conflicts, Spinello (1997; page 45) synthesizes the "best" of all theories by developing a question/answer framework. This framework, reproduced below, is translated (and is significantly changed) into a social work context. When one is facing an ethical dilemma that is not articulated in a standard code of ethics, one should ask the following questions on a case-by-case basis:

1. What is the ethical issue? Is this issue considered in state or federal statutes? If yes, is there a conflict between law and morality?

2. What was your first (intuitive) reaction to this dilemma? To what do you attribute the feeling of embarking on a moral or immoral course of action?

3. Does the analysis of various ethical theories facilitate a clearer course of action? If not, what ethical principle should take precedence? Although Spinello (1997) and Van Den Hoven (1998) do a splendid job of summarizing the major ethical theories, social workers will find the work of Bloom (1990) and Jansson (1990) clearer. Bloom and Jansson discuss ethical theories in the context of social work, while Spinello and Van Den Hoven focus on engineers and computer personnel.

4. What should be your agency's course of action? What should be your course of action?

5. What are the macro or policy implications? In this case, should norms of behavior be prescribed through legislation or regulation?

Ethical issues can be taxing when there is no clear course of action. Professional standards are based on benefiting our clients, students, and others and doing no harm. With this in mind, one should decide an ethical issue after answering all of the above questions, consulting with a colleague, and then making a decision based on agreement.

CONCLUSIONS AND SUMMARY

Based on our review of online ethics, several recommendations can be made:

- Because cyberspace is a relatively new medium of communication, ethical standards may be confusing to some. However, it is imperative to acknowledge that when ethical standards in the real world are applicable to cyberspace, social and legal norms can be applied in full force.

- When real world ethical standards are not applicable to cyberspace, one must rely on two different sources. First, ethical theories provide a sound basis for making decisions that avoid legal and social sanctions. Second, each type of Internet service (e.g., newsgroups, discussion groups, Local Area Networks) has its unique standards of cyberspace interaction. Users must learn these standards by "lurking." Sadly, these unique standards are rarely provided in writing. Role modeling is the path for learning how to behave in cyberspace.

- The analogy of the "Wild West" is applicable in cyberspace. Residents of cyberspace must be cautious of the unscrupulous interaction of others. The precautions include compliance to password standards, security for incoming email and programs, and virus and worm protection.

As advances continue to open new dimensions within areas of communication, the shifting paradigm cannot change the basis tenets of ethics. As social workers, we must continue to be accountable for our behaviors. Cyberspace will reflect our attitudes (listserves), emotions (emoticons), and interaction (netiquette) for the public to view. The public will decide if we are worthy of their trust. Cyberspace interaction that does not elicit public trust is in effect operating against our code of ethics. Cyberspace is testing our ability to incorporate accepted standards without jeopardizing our public trust.

NOTES

[1] For example, after being cautioned, a Rural Social Work Caucus listserv subscriber continued to violate basic netiquette rules. The manager removed

him from the listserv. Subscribers requested that the manager post a formal netiquette statement. This formal statement is located on the Rural Social Work caucus web page and can be found at: http://www.uncp.edu/ sw/rural/group. html#Netiquette.

2. The 5th edition of NASW's *Social Work Speaks* is likely to include technology policy statement.

3. "Cracker" is a technical term meaning, one who successfully breaks into a secured computer system. Cracking is generally not associated with technological brilliance, but "rather persistence and the dogged repetition of a handful of fairly well-known tricks and exploiting common weaknesses in the security of target systems" (Raymond, 1996, page 130).

REFERENCES

American Psychological Association. (1997, November 5). Services by Telephone, Teleconferencing, and Internet [Statement posted on the World Wide Web]. Washington, DC: Author. Retrieved August 28, 1998 from the World Wide Web: http://www.apa.org/ethics/stmnt01.html

Argyle, K. & Shields, R. (1996). Is there a body in the net? in R. Shields (ed). *Cultures of Internet: Virtual Spaces, Real Histories, Living Bodies.* Thousand Oaks, CA: Sage.

Bloom, J. (1997, November). NBCC Web counseling standards. *Counseling Today* ,pp. 6, 8, 12. Retrieved August 28, 1998 from theWorld Wide Web: http://www.counseling.org/ctonline/news/nbcc_standards.htm

Bloom, M. (1990). *Introduction to the Drama of Social Work.* Itasca, Ill: F.E. Peacock Publishers.

Electronic Frontier Foundation. (1998). *Cracking DES.* Sebastopol, CA: O'Reilly & Associates.

Gilpin, B. G. (1995). Attorney advertising and solicitation on the Internet: Complying with ethics regulations and netiquette. *The John Marshall Journal of Computer & Information,13* (4): 697-728.

Jansson, B. (1990). *Social Welfare Policy.* Belmont, CA: Wadsworth.Johnson, D.G. (1994). Crime, abuse and hacker ethics. In *Computer Ethics* (pp 40-50). Englewood Cliffs, NJ: Prentice-Hall, Inc.

Hughes, A. & Ruiz, N. (1998, April). Cyberspace and the counseling practice. *Counseling Today,*40(10): 16, 22.

Ladd, J. (1997). Ethics and the computer world: A new challenge for philosophers. *Computers and Society, 27* (3): 8-13.

Laudon, K. C. (1995). Ethical concepts and information technology. *Communications of the ACM, 38* (12): 33-39.

Lee C. (1998, April). Counseling and the challenges of cyberspace. *Counseling Today Online,* pp. 5. Retrieved August 28, 1998 from the World Wide Web: http://www.counseling.org/ctonline/sr598/lee498.htm

Legal Research Network, MCI & Benkler, Y. (1996). *Rules of the Road for the Information Superhighway: Electronic Communications and the Law.* St. Paul, Minn: West.

Marson, S. M., Cogswell, D. & Smith, M. (1994). Commonly asked questions about electronic communication and computer networking. *The New Social Worker, 1*(2), 12-15&24.

Morrissey, M. (1997, November). NBCC Web counseling Standards unleash intense debate. *Counseling Today Online*, pp. 6, 8, 12, 14. Retrieved August 28, 1998 from the World Wide Web: http://www.counseling.org/ctonline/archives/ct1197/Web counseling.htm

NASW. (1996). *The National Association of Social Workers Code of Ethics*. Washington, DC: NASW Press.

NBCC. (1997, November). Standards for the ethical practice of Web the World counseling. *Counseling Today*, pp. 6, 8, 12. Retrieved August 28, 1998 from Wide Web: http://www.nbcc.org/ethics/webstandards.htm

Oz, E. (1993). Ethical standards for computer professionals: A comparative analysis of four major codes. *Journal of Business Ethics, 12* (9): 709-726.

Parker, R. (1995). An examination of computer-related problems. *Journal of Information Ethics*, 4(1), 25-35.

Raymond, E. S. (1996). *The New Hacker's Dictionary*. Cambridge MA: MIT Press. Reamer, F.G. (1998). *Ethical Standards in Social Work: A Critical Review of the NASW Code of Ethics*. Washington, DC: NASW Press.

Rock, B. and Congress, E. (1999). The new confidentiality for the 21st century in a managed care environment. *Social Work, 44* (3): 253-262.

Santa Cruz Operation (1995). *Operating Systems User's Guide*. http://www2.sco.com:1996/OSUserG.

Shea, V. (1994). Core rules of netiquette. *Educom Review, 29* (5): 58-63.

Sheldon, R.G., Pollack, D. and Weiner, A.(1999). Confidentiality of social work records in the computer age. *Social Work, 44* (3): 243-252.

Spinello, R.A. (1997). *Case Studies in Information and Computer Ethics*. Upper Saddle River, NJ: Prentice Hall.

Stager, S. (1992). Computer ethics survey. *SIGUCCS Newsletter,* 22 (2): 19-27.

Stoll, C. (1990). *The Cuckoo's Egg*. New York: Basic Books.

Van Den Hoven, J. (1997). Computer ethics and moral methodology. Meta*aphilosophy, 28* (3): 234-248.

Wood, W. A. (1993). Computer Ethics and Years of Computer Use. The Journal of Computer Information Systems, 33 (4): 23-27.

Address correspondence to: Stephen M. Marson, Ph.D., ACSW, Professor/Director, Social Work Program, University of North Carolina at Pembroke, Pembroke, N.C. 28372-1510 marson@papa.uncp.edu