Internet Ethics for Social Workers

by Stephen M. Marson, Ph.D., ACBSW

This article originally appeared in *The New Social Worker*, Summer 2000

The nature of ethics on the Internet may be confusing to many social workers because of the unique characteristics of client contact in cyberspace. Social workers are not alone in noting the complexity of online ethics. Computer professionals are equally perplexed by ethical issues. We can find journal articles (i.e., *The Journal of Computer Information Systems* and *SIGUCCS Newsletter)* and books (i.e., *Case Studies in Information and Computer Ethics)* for computer science personnel, which specifically express the difficulties of establishing ethical standards of cyberspace professional and nonprofessional interaction.

 To clarify ethics for social workers on the Internet, we can create a two by two table. (See Table 1.) On the top horizontal axis, we see the source of ethical concern. On this axis, we must be concerned with our own interaction or the interaction of others. To help us clarify these two sources of concern, we need to examine the vertical axis, or how similar the interaction is to the real (non-cyberspace) world. Thus, interaction on the Internet is either similar to the real world or it is not (unique). Dividing up Internet interaction in this manner is important because it guides us to the most appropriate ethical actions. Each cell is discussed below.

Table 1
Source of Ethical Concern

	SELF	OTHERS
Similar	Code of Professional Ethics Standards of Practice **Cell A**	Control of Outgoing Information Locking Doors **Cell B**
Unique	Emotions Bandwidth Flame Wars **Cell C**	Cookies Passwords Encryption **Cell D**

Level of Commonality Between Real World and Cyberspace

Cell A

Cell A suggests that Internet ethical dilemmas share great commonality with ethical dilemmas in the real world. Sometimes when we use the Internet as a medium for interaction, we forget that we have the same ethical obligations as in face-to-face interaction. Here, the NASW *Code of Ethics* is our best guide. For example, standard 1.12 of the *Code* states that social workers should not employ "derogatory language." A lawyer colleague was interested in social workers' comments regarding the death penalty. He became a lurker on the electronic mailing list, SOCWORK, and was shocked at the crassness and coarseness of the language used. His experience created a negative impression of social workers.

There is something in the nature of the Internet that empowers people to use profanity and derogatory language when they would not normally use such language. Explanations for this phenomenon can be found in books like *Cultures of Internet* by Rob Shields. However, the key point is that the Internet creates the illusion that standards of social/professional interaction change in cyberspace. Standards do not change. Virtually every standard in the NASW *Code of Ethics* can be applied to Internet interaction.

Cell B

Cell B suggests that we must be aware of the ethical standards of others. For example, in the real world, we lock our offices when we leave them. Such an action is considered common sense. Along the same lines of reasoning, we need to physically protect our computers from the intrusion of others. Today, it is common to have locks on computers. In computer labs, it is common for computers and printers to be secured to tables.

Here again, the NASW *Code of Ethics* continues to be an important guide. For example, standard 1.07 addresses the issue of confidentiality. Standard 1.07c states that, "Social workers should protect the confidentiality of all information obtained in the course of professional service ...." Like locking an office or a filing cabinet, professionals are expected to protect their computers. Another example is standard 1.04 a-c. Here, the *Code* notes that social workers should limit their practice to tools for which the social worker has the proper training, education, and experience. Thus, if a social worker has a clinical practice in cyberspace, the *Code* demands technical competence in the area of technology.

Thousands of professionals (and some nonprofessionals) have a clinical practice in cyberspace. Do they meet minimum standards of ethical practice in clinical services? To answer this critical question, one needs to examine cells C and D.

Cell C

Cell C suggests that cyberspace is so unique, there is no functional equivalent in the real world. Social workers have an ethical responsibility to comprehend the ethical subtlety of this unique social environment. In such a new world, two major tools can be employed to give ethical direction. These include knowledge of the social nuances of cyberspace and ethical theories.

Although the complexity of ethical theories is beyond the scope of this article, technological knowledge is the prerequisite of using ethical theory. The best example of this is the concept of "Bandwidth." Bandwidth refers to the amount of information that a computer is able to handle at any one time. In February 2000, computer crackers[1] attacked the Web sites of companies such as eBay, Yahoo!, Amazon.com, and CNN. All of these companies own mammoth computers, but none had the bandwidth for the infinite amount of incoming e-mail. Computers owned by clients and other professionals also have bandwidth limitations.

On social work mailing lists, it is important to be sensitive to the bandwidth limitations of other subscribers. For example, subscribers to the Rural Social Work Caucus mailing list complained to and about one subscriber who sent personal e-mail to the entire mailing list. The manager of the list explained the concept of netiquette and bandwidth to the offending subscriber. The subscriber continued sending messages in this manner and received a warning. The subscriber responded to the private message from the manager to the entire list--which violated the netiquette of the list. At that point, the manager withdrew the offending subscriber from the list and denied him an opportunity to resubscribe. This is a good example of a person who does not know how to interact in cyberspace--but should take the time to learn.

Cell D

Cell D suggests that social workers are ethically obligated to possess special knowledge about technology to protect themselves and their clients. As in Cell C, knowledge of ethical theories is an important aspect of maintaining reasonable levels of ethical interaction in cyberspace. The first line of defense against the attack of others upon the professional computer files is the password. Common rules exist regarding the protection against accessing one's password. These include:

- *Do not share a password with anyone.* Other staff should do the same.

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

Passwords are sacred. Professional social workers are ethically obligated to understand and use them properly.

---

[1] Crackers are those who with malice of forethought break into secure computer systems for the purpose of stealing and corrupting data. Hackers, on the other hand, are computer enthusiasts who sometimes use similar skills to play pranks. They distinguish themselves from crackers, although the two terms are often used interchangeably.

Closing Comments

Cyberspace is an emerging new culture, as illustrated in cells C and D. As such, we require a new social interaction paradigm (a new world view). In March of 1999 at the annual meeting of the Council on Social Work Education, a group of social work professors gathered together to assess the relationship among cells A, B, C, and D. A rare consensus emerged from this formal discussion. All professors agreed that the ethics of cyberspace interaction have a great deal in common with the "real" world and as a result, little content exists in cells C and D. They concluded that the best guide for understanding ethical interaction in cyberspace is the NASW *Code of Ethics.*

Nevertheless, cyberspace remains a new culture and has unique social forces and social sanctions that have no functional equivalent in the real world. NASW made an effort to deal with the uniqueness of cyberspace by including a policy statement entitled "Technology and Social Work," which can be found in the 5th edition of *Social Work Speaks* (NASW's compilation of its policy statements). Yet, regardless of whether social interaction in cyberspace is unique or the same as in the real world, those who plan to practice social work on the Internet must understand that they cannot be relieved from professional ethical standards or responsibility.