Ethical Issues in Conducting Sex Research on the Internet

Yitzchak M. Binik
McGill University and Royal Victoria Hospital
Montreal, Quebec, Canada

Kenneth Mah
McGill University

Sara Kiesler
Carnegie Mellon University

The Internet offers a "virtual world" in which to carry out innovative sex research, but this new world may entail new ethical dilemmas. Ethical issues in recruitment, informed consent, data collection, and record keeping are examined. Applying common sense and current ethical codes for conducting sex research are sufficient in most cases. Special care and procedures may be required to obtain data from children and to protect the privacy of sensitive data and records. Researchers should be aware of, and should report, threats to data integrity and potential biases in participants' responses when they respond by computer.

As the Internet becomes a new household technology, with nearly 20% of the population on-line by 1997, opportunities grow for researchers to conduct sex research using this technology. The growth and popularity of personal Internet services allow for novel investigations of sexuality at home, in the absence of physical presence, and under conditions of relative anonymity. By making use of existing or experimental on-line sex therapists and sexual self-help or entertainment groups, researchers can study topics such as interpersonal attraction, flirting, sexual language, sexual self-help, sexual writing, role playing, and therapeutic relationships. Sexologists interested in the use and effects of sexual images are hard pressed to find a better research environment than the Internet. Researchers can present sexual stimuli on the Web, run interactive virtual experiments, or study people's access to existing sexual material, even recording responses using automated psychophysiological measures that connect participants with a central laboratory through the Internet.

Because the Internet is a somewhat new domain for research, ethical guidelines for conducting research on the Internet are beginning to emerge. Are paper and electronic informed consent forms interchangeable? Can we promise anonymity and confidentiality on the Internet? The newness and technical complexity of Internet technology make the application of current ethical codes ambiguous, a situation that can arouse the concern of researchers, institutional ethical review boards, and others. This article addresses ethical issues related to conducting sex research on the Internet.

Researchers using the Internet for many kinds of behavioral and social science research will be concerned with ethical issues (Hewson, Laurent, & Vogel, 1996; Kiesler, 1997; Kiesler & Sproull, 1986; Kiesler, Walsh, & Sproull, 1992), but sex researchers may be especially interested for three reasons. First, given the sensitive nature of much sex research, uncertainty about appropriate research conduct is likely to affect sex researchers more than other researchers, as became apparent to us in the context of two recent research projects. A furor arose at Carnegie Mellon University about a student's study of pornography on the Internet. The student obtained a database from the computer center that listed monthly-usage statistics on sexually-oriented newsgroups at the university. For technical reasons unrelated to the research, the computer program also stored the names of people who had last read each newsgroup each month in the database. An ethical question rose over the researcher's responsibility to individuals whose sexuality was revealed without their consent by an automated computer routine. A second instance occurred at McGill University in the context of a Ph.D. proposal entitled "The Phenomenology of Orgasm." Two separate ethics committees rejected proposals to allow data collection via the Internet despite safeguards which probably surpassed those used in traditional survey research.

A second reason why questions about ethical conduct on the Internet will affect sex researchers is that people's responses to research on sexuality may change when they use the Internet. For instance, the convenience and speed of the Internet, along with the paucity of social information and perception of anonymity that surrounds many Internet interactions, might lead some individuals to be more open in their network communications and less cautious than they

We thank Shelly Feran, Sunny Handa, Ethan Katsch, Naomi McCormick, David Post and William Scherlis for contributing information and ideas for this article.

Address correspondence to Dr. Irv Binik, Dept. of Psychology, McGill University, 1205 Dr. Penfield Ave., Montreal, Quebec, Canada, H3A 1B1; e-mail: binik@ego.psych.mcgill.ca

might be otherwise (Sproull & Kiesler, 1986). On the other hand, participants who know they will be identified might be particularly wary of public exposure or of the uses that can be made of cross-referenced computer databases. To the degree that the Internet presents unexpected threats to privacy or alters participants' perceptions of the research environment, ethical codes for sex research might need to be revised to fit this new environment.

Finally, government regulation of the Internet has just begun. For instance, the first "hate e-mail" case (U.S. vs Machado, 1998) in the U.S. was prosecuted successfully in February, 1998. Hence, research activities that sex researchers can pursue today, might tomorrow put them or participants at risk. One of our goals is to point out some areas of concern for the future.

We have drawn on three existing ethics codes: Ethical Principles of Psychologists and Code of Conduct (American Psychological Association, 1992), the Canadian Code of Conduct for Research Involving Humans (Tri-Council Working Group, 1996), and the Statement of Ethical Guidelines of the Society for the Scientific Study of Sexuality (SSSS) (http://www.ssc.wisc.edu/ssss/ethics.htm). There also exist other relevant ethical guidelines from electrical and computer engineering (IEEE) and computer science (Association of Computing Machinery), and Netiquette guidelines (e.g., Langford, 1996; Plaut, 1997).

RECRUITMENT

Sex researchers have begun to use the Internet to recruit participants who otherwise may be difficult to recruit locally (M. Diamond, personal communication, 1994; Kendel, Devor, & Strapko, 1997). In discussing their research on sexual bondage, Ernulf and Innala (1995) stress the advantages of using the Internet to recruit participants from distant places, to gain access to populations with paraphilic sexual tastes, and to unobtrusively observe sexually-oriented groups and monitor sexual exchanges.

One major source of bias in using the Internet to recruit subjects for sex research is that Internet users are highly unrepresentative of the population in general. They are younger, richer, better educated, more likely to be male, and more likely to have computer and technical skills than the general population (Anderson, Bikson, Law, & Mitchell, 1996; Kraut, Scherlis, Mukhopadhyay, Manning, & Kiesler, 1996). Furthermore, because of the decentralized nature of the Internet, those who use it reinforce the dominant norms and themes and draw others with like interests to it. The Internet's current population and content is heavily influenced by its beginnings as the Arpanet, an American military-supported facility used almost entirely by young male computer science and engineering graduate students and professionals. It should not be surprising that these early users were drawn to sex, sports, and discussions about computers, topics still extremely popular on the Internet today. The alt.sex newsgroups have been by far the most popular electronic groups on the Internet, and erotic Web sites are extremely popular as well. Considering the very large number of Web sites with sexual themes, it is likely that the bias associated with recruiting subjects from the Internet for sex-related experiments will be different from the bias associated with more traditional recruitment methods.

Two ethical issues particularly relevant to recruiting participants for sex research are electronic advertising and unsolicited e-mail. Section 3 of the APA code on advertising for clinical practice says psychologists should describe themselves and their activities and should avoid deceptive statements and inappropriate or excessive inducements. Common sense would extend this wisdom to advertising research on the Internet. Some ethics committees do not request a copy of the advertisement, whereas others review ads carefully. At McGill University, any form of research advertising, including electronic postings, must be submitted for review. Advertisements must tell participants about compensation, timing, and recruitment criteria must identify researchers and their affiliations and must be "in good taste." Because the Internet reaches individuals in localities with various community standards, advertising for a sex-related study, particularly if it included erotic visual material, might be interpreted as pornography. The ad could be considered illegal at the point of retrieval, thus putting the researcher and the researcher's institution at risk of prosecution. To our knowledge, no researchers have been prosecuted for violating pornography statutes; however, researchers should keep in mind that enforcement activities may change and that research institutions that receive government funding are held to a much higher standard than individuals and firms. Many types of commercial advertising would not be acceptable if a researcher used them.

Another ethical issue related to recruitment on the Internet is the use of unsolicited e-mail to recruit participants. Response rates of electronic surveys are often comparable to traditional survey rates when participants are initially solicited by telephone, postal mail, posts on electronic bulletin boards, or personal e-mail from known persons (e.g., Kiesler & Sproull, 1986; Mehta & Sivadas, 1995; Walsh, Kiesler, Sproull, & Hesse, 1992). Mehta and Sivadas (1995) reported, however, that their cold call unsolicited e-mail surveys resulted in numerous complaints. Respondents complained that they were charged by their Internet provider for their time on-line and unwanted e-mail. The researchers received so many angry complaints that they stopped their study after contacting only 50% of the potential participants. Mehta and Sivadas conclude that the use of an unsolicited e-mail methodology is an unacceptable practice. In the culture of the Internet, sending unsolicited e-mail is frowned upon as spamming. Nonetheless, junk e-mail landing in people's electronic mailboxes is likely to continue. Researchers should avoid becoming part of this problem and turning people against research.

Adverse reaction to unsolicited e-mail for sex research might be especially strong for two other reasons. First, many people read e-mail at work, where their personal e-mail is not necessarily private. Employers are legally free to monitor their employees' e-mail. People might be justifiably concerned that their employers could misinterpret their having been targeted for a sex study. Second, many people who subscribe to Internet services and who read e-mail at home also share their computer account with others in the family, including children, and with friends. In the HomeNet longitudinal study of families on the Internet, people used others' personal e-mail accounts in 13.5% of all Internet sessions (Kraut, Mukhopadhyay, Szezypula, Kiesler, & Scherlis, 1998). This finding implies that unsolicited e-mail to adults may be read inadvertently by children.

Informed Consent

Obtaining informed consent is a crucial part of the research process. Most ethical guidelines require that informed consent describe (a) the research and researchers, (b) risks and benefits, (c) who will have access to the information, (d) the right to withdraw, (e) costs and compensation, and (f) a responsible party other than the researchers. Consent can be written, oral, or in some cases, granted by virtue of participation.

Naturalistic observation in public settings and research using archival data available to the public may not require explicit consent. However, people who use the Internet may well disagree about the definition of public communication. For instance, in Usenet newsgroups, chat rooms, and other electronic groups, the size and presence of the group is unknown or ambiguous, so that many people (and the groups themselves) treat these groups as though they were private discussions. Many do not realize that their visits to MUDs (an interactive computer game derived from "multi-user dungeon," which now refers to a wide variety of adventure, sexually oriented, and other real time programs) and chat rooms can be traced to their computer, that their preferences can be estimated from their behavior over time, and that information they reveal on the Internet could be used for purposes other than those they intended. Legally, the boundary between public and private life is based on people's expectations. Because expectations about the Internet are still evolving, researchers should be sensitive to the possibility that in monitoring public Web sites or electronic groups, they may be violating expectations of privacy, especially when people access those sites and groups from their homes. For a time, researchers might do well to be extra diligent in obtaining informed consent. For example, researchers can post a message in electronic groups or a disclaimer on Web sites informing participants about the topics they are studying.

The requirements for obtaining informed consent can be fulfilled using the Internet itself. Researchers can send or display a consent form to participants and ask them to electronically indicate (e.g., by typing their names) that they understand the research and are giving consent. One advantage of an interactive consent form is that consent can be given for different parts of the consent form—for instance, the form can require readers to click in a check box next to each paragraph. A much larger difficulty is authenticating the identity of the person giving consent. The researcher cannot see the participant, and most systems do not allow the researcher to hear the participant's voice to verify his or her age and mental capacity. Without authentication, the identity of the person participating in the informed consent procedure as well as a sampling strategy that assumes some knowledge of participants, may be open to doubt.

Obtaining informed consent from children and incompetent individuals on the Internet is particularly problematic. In the past, researchers did not have easy or direct access to minors or patients independent of their parents, caretakers, schools, or some third party or institution. This insured that legal third parties were at least minimally aware of the research and were involved in giving consent. Now, many thousands of users under the age of 12 and legally defined as children use the Internet every day, often using a parent's account. Potentially important research with minors (e.g., relating to surviving sexual abuse or childhood sexuality practices) might be effectively carried out over the Internet, possibly even more effectively than through face-to-face interviewing (cf. Romer et al., 1997). In many telephone surveys, when a minor answers the telephone interviewers are required to ask for a parent or head-of-household. The same approach should be used when researchers want to contact minors through the Internet.

In some instances, older children or adolescents are sufficiently mature enough to understand and, if legally able to do so, could give their consent to sex research. The presumption that children and adolescents are capable of understanding their situations and taking action independently of their caretakers would appear to underlie the existence of hotlines for these populations. Thus, research on hotlines might be feasible. However, in most cases this research would not be acceptable except, perhaps, in a clinical setting, where the parents had already given their consent to evaluation and/or therapy. Many parents would not consent to any investigation of their child's sexuality. Even with parental consent, the parents' awareness and potential access to the forms might affect the reliability and validity of their children's responses.

The ethical code of the Society for the Scientific Study of Sexuality (SSSS) discusses situations in which requirement of the parent's or guardian's consent poses an apparent conflict or in which the research is considered minimal risk. In those cases, the code outlines four factors that must be considered: (a) the reason why the legal guardian's consent cannot be obtained (e.g., the study investigates runaways who have no contact with parents or guardians, and the researcher has the permission of a runaway shelter); (b) the importance of the study and whether the information could be collected without participation of minors; (c) the potential for harm or risk to the minors; and (d) the minor's capacity to understand the nature of the research. These guidelines do not apply as easily to the Internet as to traditional face-to-face interviews, ethnographic settings, or laboratory studies, because the researcher probably cannot use the Internet to verify the minor's real circumstances and responses to the research (e.g., whether they are actually safe from harm as a result of participation).

Given the difficulty of authenticating participants' identities and verifying their circumstances, a sensible strategy when research involves highly sensitive information or minors may be to verify the participant's information with a telephone call and to cross-check information from the participant with information from other sources. In some institutions, local participants can be authenticated through their use of local accounts and passwords. Third-party authentication authorities provide a more general solution by serving as electronic notary publics and by requiring users to register with them. If the registration process is successful, then the authentication service will guarantee the authenticity of their client's communications. Such procedures may become commonplace for business transactions and, once they do, they can also be applied to research (cf. Handa & Branchaud, 1996).

Data Collection

Even a cursory search of the Internet will reveal various sites involving research on sexuality. It is not an uncommon experience for members of e-mail discussion groups to see posts from graduate students requesting participation in their thesis research, with requests that participants send their responses by e-mail. Recently, a graduate student posted an interactive Web questionnaire on child and gender development. Because participants were to be asked to respond to potentially distressing questions about childhood abuse, problems with sexuality, and difficult parental relationships, the site included contact information for a 24-hour crisis line. The risk of distress is not unique to sex research on the Internet. We believe providing information about whom to contact with questions or concerns is just as easy on the Internet as in more traditional research settings. However, monitoring participants, as noted above, is more difficult. In one case, researchers gave network access to poor single mothers. A boyfriend, jealous of the attention one of the participants was paying to her electronic group, beat her. The researchers did not anticipate these events and only learned of them much later, but they were able to take some helpful steps because they did follow up on the welfare of the participants.

Data Collection Method

In most kinds of research, the method of data collection and mode of questionnaire administration can have potentially important response effects. This issue is not new to sex researchers, who have long worried about the interpretation of self-report, laboratory, and observational data about sexual attitudes, responses, and behavior. Catania, Binson, van der Straten, and Stone (1995) have provided an excellent review of this literature as well as a theoretical synthesis. Collecting data on the Internet may result in new kinds of response distortion, though at present the nature of the biases is unclear. Richman, Weisband, Kiesler, and Drasgow (1998) found that computer instruments elicited lower scores for self-disclosure and impression management when compared with paper-and-pencil versions of these scales, and that social desirability distortion was also less on the computer than in face-to-face interviews, especially when the computer was used to ask respondents about symptoms or sensitive information such as risky sexual behavior (see also Binik, Ochs, & Meana, 1996; de Leeuw, Hox, & Snijkers, 1995; Lloyd, Schlosser, & Stricker, 1996; Locke et al., 1992; Romer et al., 1997; Turner, Miller, Smith, Cooley, & Rogers, 1996). However, on scales like the Minnesota Multiphasic Personality Inventory, especially when respondents were identified or were in the presence of others, distortion on the computer version was higher than on the traditional paper and pencil forms. The literature so far suggests that, under conditions of perceived anonymity and confidentiality, Internet instruments could be designed to encourage participants to report socially undesirable behaviors, drug use, HIV risk factors, and reports of illegal activity or abuse. However, they would likely do just the opposite under conditions of perceived identification and nonconfidentiality, especially if they thought their data would be sent to other databases (Rosenfeld, Booth-Kewley, Edwards, & Thomas, 1996).

Privacy and Anonymity

Respondent privacy and anonymity are two related issues that affect data collection for sex research on the Internet. The Internet appears to provide a perfect setting in which anonymity and complete privacy can be achieved. This setting could be an important boon for sex research, especially when researchers wish to study socially undesirable or illegal behavior. A recent meta-analysis of 61 studies by Richman et al. (1998) suggests that guarantees of anonymity for electronic surveys and questionnaires are an influential factor in obtaining high self-disclosure on the computer. People's subjective feelings of anonymity and, in turn, their behavior (or responses to surveys) on the Internet will also be affected by whether they are using the Internet alone or in the presence of others, by on-line cues that suggest whether their information will be confidential or sent to other databases, by the presence or absence of social context information in the virtual environment, and finally, by the interface itself.[1] For example, an Internet survey that does not allow people to backtrack and edit responses will increase participants' wariness and social desirability distortion. Researchers conducting on-line surveys and experiments should pretest how participants experience the interactions to be studied, and researchers should not assume

[1] It should not be assumed that people are always alone when they use the Internet. In the HomeNet study, in 25% of the sessions, participants used the Internet at home with friends or family members. Others access the Internet in public settings such as libraries and schools, or at work, where communication is not necessarily private. Richman et al. (1998) found that the presence of others while the participant was using a computer survey or questionnaire was a strong factor in determining social desirability distortion.

that a promise of anonymity or nonanonymity is always viewed as such by participants. They also should describe the interface they used, and report circumstances that may have introduced bias.

In some experiments, researchers use deception or withhold full information about the hypotheses or real purposes of the study to insure the validity of responses. In this case, participants may be exposed to potentially damaging information, or they may be assigned to placebo or control groups. In traditional experiments, researchers can carefully monitor the participants' reactions and rectify misunderstandings or other negative effects. When the research is conducted remotely through the Internet, researchers must take special precautions to prevent harm to participants. In a few cases, the anonymity of the research setting has allowed student participants to engage in "flame wars" and to insult other participants with impunity. One professor's computer-mediated brainstorming sessions led to a sexual harassment suit against the university. (S. Walker, personal communication, March 31, 1992).

Privacy on the Internet is likely to become increasingly important to research participants, and privacy will affect participants' behavior. In one study, inner-city teenagers were given Internet access through their school. They wrote hundreds of messages to their friends to discuss topics ranging from sex to rap music. Project officials became concerned that the school system would learn of the students' frank discussions on-line, so they informed the students that their messages would be monitored. This withdrawal of privacy resulted in a sudden and drastic decline in Internet use by the students, and the end of the study (P. Attewell, personal communication, June 6, 1995).

Unfortunately, promises of anonymity on the Internet can rarely, if ever, be given with 100% certainty, since a persistent hacker or an official with a court order may be able to discover the identity of research participants. Sex researchers may be particularly concerned about the degree of objective anonymity when the research touches on illegal behavior. There are several options to increase participants' objective anonymity on the Internet. First, researchers can use anonymous re-mailers or forms. Re-mailers hide e-mail identities in the same way that post-office boxes hide identities within the postal system. Re-mailers are legal in North America and Europe as long as they are used for legal purposes. But legality differs across localities, and the risks to researchers may increase when the content of the communication is sexual. Re-mailed communications are traceable if the system operator is forced to open the files. In 1995, for example, police raided a well-known anonymous re-mailer, "anon.penet.fi" in Finland, and forced the owner to reveal the identity of at least one user.

Another way to increase objective anonymity is to have participants access the researcher's server directly using an anonymous form or Web site. Researchers can create a Web site or e-mail directory that assigns a unique code to each completed survey or interaction and never requires the participants to enter their names. If the researchers plan to contact the participants again (e.g., to do a follow-up survey) they can use a different form to obtain informed consent and store participants' names and their codes in an unlinked file. This procedure is not completely anonymous because names of participants are stored. Also, if the participants interact remotely, the IP addresses of the participants' computers could be traced. A skilled *hacker* (an Internet user who tries to illegally break into other Internet computers) could put a tag on participants, or a derelict system operator could release user logs, leading to the inadvertent disclosure of people's identities. These risks of exposure to participants are small, but a few incidents have occurred. Researchers using automated techniques should test their procedures for insuring anonymity before employing them for sensitive research.

Special encryption techniques are probably the most effective means for protecting anonymity. These techniques are especially useful to categorize people who have not given their formal consent for a study (e.g., visitors to sexual chat rooms; people, not in the study, who send sexual material to study participants) or to follow or retest participants who have been promised anonymity. One such technique is one-way encryption (W. Scherlis, personal communication, 1997). By using a one-way hashing algorithm (a complex mathematical function), a researcher can turn each person's name and address into a cryptographic representation, protecting their subject's privacy while following the person over time to yield valuable longitudinal data. There is no key or code because the function is computationally feasible in only one direction; therefore, it is not possible to use the cryptographic representation to retrieve the unencoded address or identity of the person. For example, a one-way function could map an e-mail address such as jane.smith@andrew.edu into a number in the range of 1 to 10,000. Then, the name and address is thrown away, and there is no feasible way, given just the result of the one-way function, to retrieve the address. Because the computation done on the address is a function, it always maps a given address into the same (or nearly same) number, and the results of mapping a large set of addresses would yield an approximately even distribution over the full range of the function. Yet the researchers can use the mathematical representations to track each unique participant over time. As in any study requiring the anonymity of subjects, the sampling frame and categories or levels of variables must have a sufficiently large number of participants so that no person could be uniquely identified by them. For example, one would not want to use the category "Smith family" as a variable in the database.[2]

[2] There is a nearly zero risk of identifying anyone using this method. There is a remote possibility of identification of a person who sent e-mail to a participant in the study whose identity was known. This could occur if a researcher within a study, having access to the e-mail representations, collaborated with someone outside the study who was investigating or spying on anonymous participants. The outsider might have obtained a list of the e-mail addresses of possible correspondents with known participants. In this scenario, this information along with the encryption method and access to participants' e-mail records would allow, with some probability, the likely input address for a particular representation. This possibility seems extremely remote.

Representation of the Researcher and Research

Anonymity usually refers to the participant or respondent, but it is also possible to think about degrees of experimenter anonymity. It seems unlikely that research ethics boards would approve any experimental or survey protocol where the identities of the principal researchers were not disclosed. As far as we are aware, however, the identities of researchers observing public behavior need not be disclosed. Also, the sexual orientation, gender, or other personal characteristics of the investigators need not be disclosed. However, electronic communication can narrow the range of paralinguistic cues and social information about the researchers compared with the cues and information participants have in traditional research, and this narrowing may affect how participants respond. Experimenter anonymity could be an advantage in reducing social desirability bias, but it could also be a disadvantage; if a gay researcher, for instance, wanted to reveal his orientation nonverbally to gay participants in order to increase their trust (cf. Behrens, 1997).

We can also consider the anonymity of the research more broadly. The boundaries and norms of electronic groups and Internet activities are diffuse and ambiguous. Participants may have difficulty differentiating legitimate sex research and researchers from commercial sex sites, amateur sex surveys, games, and the like. Several commercial or nonprofit on-line survey companies and sites exist on the Internet, offering sex surveys that have the look and feel of research. Some companies offer sexual information about themselves and others, dating services, and counseling. It would be difficult for an untutored viewer to figure out, for example, how to verify that a research project at a university had passed an institutional ethics review. Researchers doing sex research on the Internet may need to devise explicit techniques to convey the legitimacy of their research, to distinguish themselves from vendors, to describe their methods, and to communicate the sources of their information and pronouncements.

Two kinds of sex research may be especially hard to describe to participants on the Internet. Almost everyone knows what a survey is, but few people understand ethnographic research or research involving automated data collection. Turkle's (1997) study of role-playing in MUDs exemplifies the use of ethnographic methods to collect data on the Internet. Turkle "hung out" with game players in the MUDs, interviewed participants, and held a series of pizza parties for MUDders in the Boston area. " 'This is more real than my real life,' said a character who turns out to be a man playing a woman who is pretending to be a man" (Turkle, 1997, p. 143). Turkle repeatedly told on-line participants she was conducting research because new players continually joined the games.

Research by Mehta and Plaza (1997) exemplifies research involving semi-automated tracking of information on the Internet. They did not use informed consent because they counted and coded public Usenet posts for erotic material, and did not follow people over time. The HomeNet field trial of residential Internet usage by Kraut et al. (1996) exemplifies the use of an automated system that potentially involves more risks to participants because their Internet behavior over time is monitored and stored, including a log of all Web sites visited and e-mail sent and received. The researchers did not store the content of e-mail. The informed consent statement included the information that participants' Web site visits can be tracked, and that children will have access to unlimited material. The researchers held a face-to-face training session with all new families so that participants could obtain basic Internet skills, get a sense of the range of material accessible on the Internet, and meet some of the research staff in person. The HomeNet project also has a Web site where participants can share information. For highly sensitive long distance research, investigators could reduce the anonymity of the research by posting photographs of the researchers and their institutions, and providing Web links to their own Web pages.

Data Storage and Confidentiality

Researchers are responsible for maintaining the confidentiality of data by limiting access to authorized individuals and by implementing adequate data storage procedures. Researchers must also inform potential participants about who will have access to their data. Although ethics codes recognize confidentiality as a requisite of ethical research, they also acknowledge limits to confidentiality. For instance, situations involving child abuse would justify violation of the confidentiality principle. Confidentiality of databases may be violated if an appropriate review body determines that the potential good that may arise from the data outweighs the potential harm. Although anonymous data are thought to be confidential by definition, it is advisable to further safeguard data confidentiality since anonymity rarely can be guaranteed.

The use of the Internet to collect and store data raises a variety of concerns with respect to the principle of confidentiality. Perhaps the most crucial issue concerns the standards by which we judge the confidentiality of Internet communications. Do we use current standards for non-Internet research or are new guidelines required? As far as we know, there are no formal standards for the security of data kept on paper in filing cabinets in most university laboratories. Giving untutored student employees access to records, failing to audit data files, not locking file cabinets, and giving a single person access to all records are probably common failings. Practices with respect to Internet data are probably equally informal, to the point of leaving databases exposed without password protection. Also, it is hard to insure that there is no unauthorized access to e-mail and other files stored on a network. Many university computer systems, especially at the departmental level, are easy targets for amateur hackers. We believe Internet research involving sensitive sexual activity and data should be handled like commercial transactions. Handa and Branchaud (1996) have suggested that for electronic commerce to be feasible, we must be able to communicate information without fear of access or alteration by a third party, goals that can now be achieved by the latest commercially available cryptography programs.[3]

Some in the clinical psychology community are willing to settle for Internet confidentiality standards at a somewhat lower level. There are at least two well-established e-mail psychological-help services on the Internet: Shrink-Link and Help-Net. These e-mail services charge fees and are staffed by licensed professionals who respond to their clients' questions. Shrink-Link is reportedly one of the most popular commercial ventures on the World Wide Web (Shapiro & Schulman, 1996). The APA ethics board has begun to address ethical issues related to the use of these services, but has yet to propose specific guidelines. Shapiro and Schulman (1996) suggest that clinical services should make the following clear to clients:

> [F]irst, that e-mail systems . . . store e-mail interactions; second, that individuals other than the intended recipient may have relatively easy access to e-mail; third, that personal computers may store the interactions and that these may be readable by anyone else with access to the computer; and finally, as in all therapy cases, the clinician might need to divulge confidential information if he or she perceives that the client is at risk for imminently harming him- or herself or someone else. (p. 115)

Shapiro and Schulman believe that although they designed these guidelines primarily with e-mail in mind, the guidelines can be applied to other forms of electronic communication.

Participants need to be instructed carefully regarding how data about them could be used. Communicating remotely on the Internet can create an illusion of privacy, and many people do not realize how information they reveal can be combined and used for other purposes (for an interesting demonstration of how "public" information about people collects on the Internet, see http://www.13x.com/cgi-bin/cdt/snoop.pl). Many people do not know which of their communications on the Internet are legally protected. Electronic break-ins of private e-mail are covered by legal sanctions. The Electronic Communications Privacy Act (ECPA) in the United States is a federal law prohibiting individuals from breaking into others' private telephone and other electronic communications. This law covers deliberate interception of e-mail such as cracking, hacking into someone's data on their computer, and "packet sniffing." Similar laws exist in Canada and many other countries, though the specifics and reach of the laws vary among jurisdictions. However, the ECPA does not cover e-mail sent or received by computers at work organizations. Also, in the United States, purchase information (except personal data about video rentals) that is kept or transmitted by Internet or other means is not protected by law.

Conclusion

Though sex research on the Internet carries a few unusual risks, we advocate the application of normal ethical standards of research. The dangers do not seem so great or insurmountable that the Internet merits arbitrarily strict standards or standards that we would not apply to other research methodologies. As with any new technology, the Internet will create unforeseen consequences as more researchers use it. These consequences should be the topic for ongoing discussions including ethicists, behavioral and social scientists, computer scientists, and others.

We would like to enumerate some limitations to this paper. First, we did not delve in detail into psychophysiological, therapeutic, and other types of experimentation on the Internet. To date, very few researchers have tried these methods. We expect more of these types of research in the next decade. Second, on-line journals have begun to appear, but we have not addressed issues surrounding scientific communication on the Internet such as electronic publication and Web-sharing of data. Legal issues such as copyright and intellectual property, as well as more directly related issues of peer review and the journal system, will be affected by electronic publication (Katsh, 1995).

Virtually all ethical codes and most institutions require researchers who intend to use human subjects to submit their research plans for review by a group of disinterested peers such as an institutional review board. When considering Internet-related research, such review boards should include members with expertise in the technical aspects of the Internet. Also, a significant portion of Internet research is being conducted by nonbehavioral scientists (e.g., computer scientists) in settings without a tradition of formal ethical review. When it involves human participants, such research should be integrated into the local ethics review system. Consistent universal guidelines based on evidence and informed opinions are needed to prevent negative consequences derived from use (or misuse) of the technology. Since many societal and scientific groups already perceive the possible negative consequences of sex research to outweigh the benefit, such guidelines are particularly important for sexologists.

To encourage further discussion, we present some suggestions drawn from this article for researchers conducting sex research on the Internet. These assume normal guidelines apply in most cases.

1. Do not send unsolicited e-mail for sex research.

2. The Internet provides cheap and direct research access to minors and other special populations. With or without informed consent (when it is waived by ethical

[3] The most secure forms of cryptography for (nonanonymous) communication are asymmetric, two-key systems employing public and private keys. To illustrate, Participant Smith wants to complete and send a questionnaire by e-mail to Researcher Jones and be sure only Researcher Jones is able to read the e-mailed questionnaire. Jones would send Smith his "public key." Smith would encrypt the e-mail using this public key and send it to Jones, who would then use his private key and an encryption-decryption program such as PGP (Pretty Good Privacy) to decrypt it. This type of system, which will become increasingly automated and feasible for researchers to use, makes it virtually impossible for someone to uncrack and read a misdirected communication without massive computer power and time; only the person with the "right" private key would be able to decode the text.

review boards for special reasons), researchers should take additional steps to insure the authenticity of the participants' identities and that the circumstances of the participants are as they present them and are appropriate to the research. Additional steps can be used, such as using telephone calls or electronic authentication services to cross check information about participants.

3. Investigators using the Internet to investigate emotionally sensitive issues should make provision for easily accessible clinical and referral backup services in the event that participants require help as a result of participating in the research. Researchers should provide participants with telephone numbers (not just e-mail addresses) of responsible persons to contact concerning potentially harmful aspects of the research. After a study is complete, researchers should verify the well-being of participants and debrief them, just as they would in traditional experiments. Should participants report harm, researchers should consider communicating by telephone with these participants in order to evaluate what should be done.

4. Participants in Internet research may be unaware of threats to their privacy, or may also be concerned about threats that do not exist. Researchers should inform themselves about such risks, reduce the risks as much as possible, and make threats to privacy explicit, not only in the consent and data collection process, but also when they debrief participants. To reduce anonymity, the researchers can provide photos and other social context information for the participants using the Internet.

5. Researchers conducting on-line surveys and experiments should pretest how participants experience the interactions to be studied, and they should not assume that a promise of anonymity or nonanonymity is always experienced as such. They also should describe the interface they used, and report circumstances that may have introduced bias.

6. Researchers should employ appropriate strategies such as anonymous re-mailers, dedicated servers, and encryption to provide anonymity. They should not promise anonymity that they cannot guarantee.

7. Current commercially-available encryption programs provide a level of confidentiality at least as secure as that provided by locked filing cabinets. Where participants are at particular risk of exposure, one-way encryption is a valuable alternative. Researchers and clinicians should protect communications through encryption rather than by informing people that their communications are not confidential. Participants caught up in intense, personal interactions may exert insufficient caution. Internet users also may have seen so many error messages about insecure communications that they have become desensitized to them.

8. Graduate schools should teach students systematic procedures for protecting the confidentiality of electronic (and other) data and for verifying data integrity. Because computer systems are extremely complex and can exhibit unanticipated behavior, researchers using automated techniques to insure anonymity or confidentiality should always test their own systems before putting any participants or data at risk.

9. Legal statutes prohibit breaking into electronic data files in many countries. However, steps should be taken to safeguard the confidentiality of even legally private information. Participants need to be informed that electronic communications at work are not protected. If participants will provide sensitive data while they are at work (or using any systems not their own), then the researcher should take active steps to have these communications encrypted.

10. Researchers should not store raw data received over the Internet in vulnerable electronic files for long periods. Instead, they should be transferred as quickly as possible to separate and more secure databases, and the original files should be deleted. Information should be gathered on what happens to backups of deleted files, and risks to confidentiality should be assessed accordingly.

REFERENCES

American Psychological Association (1992). Ethical principles of psychologists and code of conduct. *American Psychologist, 47,* 1597–1611.

Anderson, R. H., Bikson, T. K., Law, S. A., & Mitchell, B. M. (1996). *Universal access to e-mail: Feasibility and societal implications (MR-650–MF).* Santa Monica, CA: RAND Corporation.

Behrens, D. (1997). *The self-structuring of support: An empirical examination of the personal networks for individuals under stress.* Unpublished doctoral dissertation, Carnegie Mellon University, Pittsburgh.

Bier, M. C., Sherblom, S. A., & Gallo, M. A. (1996). Ethical issues in a study of Internet use: Uncertainty, responsibility, and the spirit of research relationships. *Ethics & Behavior, 6,* 141–151.

Binik, Y. M., Ochs, E. P., & Meana, M. (1996). A Sexpert computer in the bedroom: Fact or fantasy. In M. Miller, M. Hile, & K. Hammond (Eds.), *Mental Health Computing* (pp. 17–34). New York: Springer-Verlag.

Catania, J. A., Binson, D., van der Straten, A., & Stone, V. (1995). Methodological research on sexual behavior in the AIDS era. *Annual Review of Sex Research, 6,* 77–125.

de Leeuw, E. D., Hox, J. J., & Snijkers, G. (1995). The effect of computer-assisted interviewing on data quality: A review. *Journal of the Market Research Society, 17,* 325–344.

Ernulf, K. E., & Innala, S. M. (1995). Sexual bondage: A review and unobtrusive investigation. *Archives of Sexual Behavior, 24,* 631–654.

Handa, S., & Branchaud, M. (l996). Re-evaluating proposals for a public key infrastructure. *Law/Technology, 29(3),* 1–26.

Hewson, C. M., Laurent, D., & Vogel, C. M. (1996). Proper methodologies for psychological and sociological studies conducted via the Internet. *Behavior Research in Methods, Instruments & Computers, 28,* 186–191.

Katsh, M. E. (1995) *Law in a digital world.* New York: Oxford University Press.

Kendel, M., Devor, H., & Strapko, N. (1997). Feminist and lesbian opinions about transsexuals. In B. Bullough, V. Bullough, & J. Elias (Eds.), *Gender blending* (p. 146–159). Amherst, NY: Prometheus.

Kiesler, S. (Ed.). (1997). *Culture of the Internet.* Mahweh, NJ: Lawrence Erlbaum.

Kiesler, S., & Sproull, L. (1986). Response effects in the electronic survey. *Public Opinion Quarterly, 50,* 402–413.

Kiesler, S., Walsh, J., & Sproull, L. (1992). Computer networks in field research. *Methodological Issues in Applied Psychology, 12,* 239–267.

Kraut, R., Mukhopadhyay, T., Szezypula, J., Kesler, S., & Scherlis, W. (in press). Communication and information: Alternative uses of the internet in households. *Proceedings of the CHI 98 Conference*, New York: ACM.

Kraut, R., Scherlis, W., Mukhopadhyay, T., Manning, J., & Kiesler, S. (1996). The HomeNet field trial of residential Internet services. *Communications of the ACM, 39,* 55–65.

Langford, D. (1996). Ethics and the Internet: Appropriate behavior in electronic communication. *Ethics & Behavior, 6,* 91–106.

Lloyd, M. G., Schlosser, B., & Stricker, G. (1996). Cybertherapy. *Ethics & Behavior, 6,* 169–177.

Locke, S. E., Kowaloff, H. B., Hoff, R. G., Safran, C., Popovsky, M. A., Cotton, D. J., Finkelstein, D. M., Page, P. L., & Slack, W. V. (1992). Computer-based interview for screening blood donors for risk of HIV transmission. *The Journal of the American Medical Association, 268,* 1301–1305.

Mehta, M. D., & Plaza, D. E. (1997). Pornography in cyberspace: An exploration of what's in USENET. In S. Kiesler (Ed.), *Culture of the Internet* (pp. 53–68). Mahweh, NJ: Lawrence Erlbaum.

Mehta, R., & Sivadas, E. (1995). Comparing response rates and response content in mail versus electronic mail surveys. *Journal of the Market Research Society, 37,* 429–439.

Plaut, S. M. (1997). On-line ethics: Social contracts in the virtual community. *Journal of Sex Education and Therapy, 22,* 84–90.

Richman, W. L., Weisband, S., Kiesler, S., & Drasgow, F. (in press). A meta-analytic study of social desirability distortion in computer-administered questionnaires, traditional questionnaires, and interviews. *Journal of Applied Psychology.*

Romer, D., Hornik, R., Stanton, B., Black, M., Li, X., Ricardo, I., & Feigelman, S. (1997). "Talking" computers: A reliable and private method to conduct interviews on sensitive topics with children. *The Journal of Sex Research, 34,* 3–9.

Rosenfeld, P., Booth-Kewley, S., Edwards, J. E., & Thomas, M. D. (1996). Responses on computer surveys: Impression management, social desirability, and the Big Brother Syndrome. *Computers in Human Behavior, 12,* 263–274.

Shapiro, D. E., & Schulman, C. E. (1996). Ethical and legal issues in e-mail therapy. *Ethics & Behavior, 6,* 107–124.

Sproull, L., & Kiesler, S. (1986). Reducing social context cues: Electronic mail in organizational communication. *Management Science, 32,* 1492–1512.

Tri-Council Working Group (1996). *Code of conduct for research involving humans (cat. no. MR21–13/1996I).* Ottawa, Canada: Minister of Supplies and Services.

Turkle, S. (1997). Constructions and reconstructions of self in virtual reality: Playing in the MUDs. In S. Kiesler (Ed.), *Culture of the Internet* (pp. 143–155). Mahweh, NJ: Lawrence Erlbaum.

Turner, C. F., Miller, H. G., Smith, T. K., Cooley, P. C., & Rogers, S. M. (1996). Telephone audio computer-assisted self-interviewing (T-ACASI) and survey measurements of sensitive behaviors: Preliminary results. In R. Banks (Ed.), *Survey and statistical computing.* Chesham, Bucks, U.K.: Association for Survey Computing.

Walsh, J. P., Kiesler, S., Sproull, L., & Hesse, B. (1992). Self-selected and randomly selected respondents in a computer network survey. *Public Opinion Quarterly, 56,* 241–244.

Manuscript accepted September 8, 1998