Ethics & Behavior
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/hebh20

Internet Research: An Opportunity to Revisit Classic Ethical Problems in Behavioral Research
David J. Pittenger
Available online: 08 Jan 2010

To cite this article: David J. Pittenger (2003): Internet Research: An Opportunity to Revisit Classic Ethical Problems in Behavioral Research, Ethics & Behavior, 13:1, 45-60
To link to this article: http://dx.doi.org/10.1207/S15327019EB1301_08

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.tandfonline.com/page/terms-and-conditions

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae, and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
Internet Research: An Opportunity to Revisit Classic Ethical Problems in Behavioral Research

David J. Pittenger

Department of Psychology
The University of Tennessee at Chattanooga

The Internet offers many new opportunities for behavioral researchers to conduct quantitative and qualitative research. Although the ethical guidelines of the American Psychological Association generalize, in part, to research conducted through the Internet, several matters related to Internet research require further analysis. This article reviews several fundamental ethical issues related to Internet research, namely the preservation of privacy, the issuance of informed consent, the use of deception and false feedback, and research methods. In essence, the Internet offers unique challenges to behavioral researchers. Among these are the need to better define the distinction between private and public behavior performed through the Internet, ensure mechanisms for obtaining valid informed consent from participants and performing debriefing exercises, and verify the validity of data collected through the Internet.

Key words: ethics, Internet, privacy, informed consent, research methods

As a research tool, the Internet portends many opportunities for behavioral researchers as its global scope allows one to sample from larger and more heterogeneous populations than those found at the typical college or university. Using readily available software, one can create and post Web pages that allow participants to complete questionnaires, respond to open-ended questions, and participate in experiments (Birnbaum, 2000; Hewson, Laurent, & Vogel, 1996). Similarly, chat

Requests for reprints should be sent to David J. Pittenger, Department of Psychology, The University of Tennessee at Chattanooga, 615 McCallie Avenue, Chattanooga, TN 37403. E-mail: david-pittenger@utc.edu
rooms, list servers, multiuser dungeons, and other communication mechanisms create “virtual communities” that afford unprecedented opportunities for researchers to examine behavior within groups of people.

Several converging sources of information suggest that many researchers now turn to the Internet as a medium for conducting their research. For example, the American Psychological Society (2002) hosts a Web page that provides links to many Internet-based research projects. These projects range from traditional experiments in sensation and perception to broader topics including personality assessment and various topics in social psychology. A casual review of contemporary journals indicates that researchers have begun to benefit from using the Internet as a venue for conducting research. For instance, a special issue of the journal *Group Dynamics: Theory, Research, and Practice* (Kivlighan, 2002) published a series of research reports that specifically examined intergroup processes via the Internet.

Because the Internet is a new venue for collecting data, it requires researchers to revisit several important ethical principles, namely the preservation of privacy and confidentiality, the issuance of informed consent, and the use of deception and false feedback. In many instances, the difference in venue—intact research laboratory versus Internet Web site—is minimal; thus, using the Internet for behavioral research offers no particularly exceptional ethical challenge. There are, however, components of Internet research that require careful scrutiny. Therefore, I intend to explore several familiar ethical themes within the context of the technology afforded by the Internet.

Other authors have examined components of the relation between ethics and research using the Internet. For example, Childress and Asamen (1998) offered a fine review of and guidelines for conducting research on the effectiveness of Internet psychotherapeutic interventions. Similarly, Humphreys, Winzelberg, and Klaw (2000) examined psychologists’ ethical responsibilities for conducting Internet-based therapeutic groups. Consequently, I do not intend to cover previously explored matters that relate to specific focus research and psychotherapeutic practice through the Internet. Rather, I intend to examine the broader implications of conducting research using the Internet and the attendant ethical responsibilities that psychologists bear. For my review, I rely on the current ethical guidelines codified by the American Psychological Association (APA, 1992) as well as reactions to previously conducted research that has raised ethical concerns.

The contemporary review of behavioral research ethics has a canon of studies and methods that establishes a backdrop for discussions of the ethical appropriateness of various research techniques. Several of the more notable examples in this catalog include Humphrey’s (1970) analysis of men who engaged in homosexual acts in public restrooms (a.k.a. tearooms); Milgram’s (1963, 1974) studies of obedience; and projects wherein the participants receive false information (e.g., the bogus pipeline [Roese & Jamieson, 1993] and the Barnum effect [Dickson & Kelly,
1985]) to list but a few. These studies and research techniques receive ethical scrutiny because they raise fundamental questions regarding invasion of privacy, the necessity of informed consent, and the use of deception and false information. As such, we may review the lessons learned from the analysis of these problems and apply them to ethical questions raised by research conducted using the Internet.

PRIVACY AND CONFIDENTIALITY

The public nature of the Internet heightens concerns for participants’ privacy and confidentiality. In essence, two broad categories of problems require scrutiny. The first concern is technical as it regards the mechanical and software protections the researcher uses to ensure that unauthorized persons (e.g., “hackers”) do not have access to his or her data. The second problem refers to the ethical responsibilities of the researcher who wishes to join a virtual community to conduct his or her research or who wishes to conduct electronic surveillance of computer users.

Preservation of Confidentiality

The design of the Internet provides a common link among computers that supports the rapid exchange of information and serves as a conduit for communication among computer users. This link is both an advantage and a liability for the behavioral researcher. The obvious advantage is that the researcher can communicate with anyone who has access to the Internet. The obvious liability is that a persistent person can gain unauthorized access to a researcher’s data, thus compromising its integrity and confidentiality. Furthermore, data stored on publicly owned computers may be subject to a state’s open records law. For example, in Tennessee, where I work for a state university, the contents of my computer, including personal correspondence and e-mail exchanges, are public record (Public Libraries, Archives and Records, 2001). Consequently, any Tennessee citizen who requests access to my files, whether stored on the computer in my office or on the university’s central server, can review my correspondence. This openness recently led to the publication in a local newspaper of intimate e-mail exchanges between the now-former president of the University of Tennessee system and his paramour (Tanner, 2001). Although these laws recognize the confidentiality of the content of some records (e.g., medical information and student records), researchers should ensure that they may store their data under such protections. Those working in the private sector should note that corporations also own the content of their computers and may monitor the employees’ use of the computer with various electronic surveillance technologies (Alge, 2001).
The solution to the first set of problems is largely technical. One can purchase hardware and software that reduces the chance that a hacker will gain unauthorized access to one’s data. Similarly, one can transfer sensitive files to a portable diskette and then use specialized software to remove remnants of the files from the computer’s hard drive. In addition, one can use encrypting software to render the files unreadable to unauthorized persons. Finally, one can code the data in ways that reduce the chance that one could surmise the identity of the persons providing specific information.

The second concern refers to researchers who wish to conduct naturalistic observations of people engaged in various virtual communities in which people communicate among themselves. At issue is the level of privacy a person may expect when sharing intimate personal information in one of these virtual communities. Framed as a question, can a researcher surreptitiously join chat rooms to record and analyze the dialogues that transpire? Furthermore, are all virtual communities equally public, or are there some forums that should enjoy a greater presumption of privacy?

As an example, Finn and Lavitt (1994) published an account of how victims of sexual abuse used an Internet-mediated self-help support group. To conduct their research, Finn and Lavitt recorded and analyzed many of the exchanges among the members of the group and published samples of the dialogues, including the name of the group as well as the time and dates of the exchanges, without having received permission from members of the group. Other researchers have also examined the exchanges among participants using therapeutic online groups (Chang, Yeh, & Krumboltz, 2001; Klaw, Huebsch, & Humphreys, 2000). In the latter examples, the researchers created an Internet chat room that was open only to those individuals who had offered informed consent to join the group and who knew the researcher’s intent to evaluate the effectiveness of the intervention.

It does not require much imagination to foresee proposals for which the researchers will wish to conduct naturalistic observations of other virtual communities. One can also imagine participant observation research wherein a researcher surreptitiously joins a virtual community and strategically posts comments to evoke reactions among the members of the community. Two examples, one a legal ruling and the other a research project, may help in producing an answer to these questions.

The interaction between technology and the boundaries of privacy is a complicated one and not limited to the Internet. For example, in a recent ruling (Kyllo v. United States, 2001), the Supreme Court examined the right to privacy as defined by the Fourth Amendment of the Constitution. In that case, agents of the U.S. Department of the Interior suspected that Kyllo used high-intensity lamps to maintain a marijuana garden in his house. The agents used an infrared imaging device to confirm that an abnormal level of heat radiated from Kyllo’s house. The agents then used the infrared image and other evidence to obtain a search warrant. Kyllo argued
that using the infrared image was an unconstitutional invasion of his privacy. The court, by a 5 to 4 vote, concurred with Kyllo. Writing for the majority, Justice Scalia argued that Kyllo maintained a subjective expectation of privacy and that the technology violated Kyllo’s privacy by penetrating the metaphorical barrier that separates what is public and what is private. The majority ruling also held that the agents’ use of a device that is not in common use of most citizens further exacerbated the unlawfulness of the search.

Humphreys’s (1970) report of men who engaged in homosexual acts in public restrooms also tested the limits of the presumed privacy of individuals. For his research, Humphreys posed as a lookout while the men engaged in homosexual activities. Using the individuals’ license plate number, Humphreys later went to the homes of the men and, posing as a health service researcher, interviewed them. Although the research did much to challenge the inaccurate stereotypes of homosexual men, the method for collecting the data raised ethical questions concerning whether Humphreys violated the individual’s right to privacy and used inappropriate deception to engage the men in the interview (Sieber, 1992).

The Kyllo ruling and the Humphreys (1970) study are germane to the problem of preserving the privacy of an individual and the role of technology to acquire information. Both Kyllo and Humphreys force us to examine the meaning and privileges of the expectation of privacy. The Kyllo case raises the question of the extent to which technological advances in surveillance violate the reasonable boundary of privacy. The Humphreys case raises the question of whether a researcher can join a group without identifying his or her role as a researcher to collect data.

The current and proposed APA ethical guidelines (1992, 2001) offer faint guidance regarding the preservation of privacy. Principle D of the current guidelines (Principle E for the proposed guidelines) requires that psychologists respect individuals’ right to privacy. Similarly, the ethical code (sections 6.12 and 8.05 of the current and proposed guidelines, respectively) allows researchers to dispense with informed consent to conduct naturalistic observation. Unfortunately, the guidelines do not define privacy per se. As I argue subsequently, privacy is a subjective state that persons may expect under certain conditions and when they exercise specific precautions. Consequently, it is necessary to develop a schema that proves a general test for determining the boundary of expected privacy within the Internet and the domain in which behavioral researchers can stand as nonparticipatory observers of the behavior of others.

From one perspective, the Internet offers no veil of privacy because any disclosure one makes through any Internet forum is, by its very nature, public. Indeed, the Internet is an intentionally public instrument that the government developed as a component of the military defensive organization (Lester, 2001). By analogy, the Internet is a public location in which individuals are free to observe what transpires. Consequently, whether I kiss my wife or scold my children in
public, I cannot expect others to avert their eyes to avoid seeing me do something that I might consider intimate or embarrassing for the simple reason that I have acted where it is easy for others to see what I do and hear what I say. According to this reasoning, the same is true of the Internet. What I send through the Internet, no matter how intimate or embarrassing I believe the information may be, passes through a public medium. Therefore, I cannot expect that others will avert their gaze.

Three additional observations support the argument that the Internet is equivalent to a public place and provides researchers unrestrained access to virtual communities for research purposes. First, the Internet is now a common instrument with which the reasonable person is familiar. In other words, users of the Internet understand the openness of the media for the simple reason that they have unfettered access to the communiqués of others. Second, one can easily retain his or her anonymity by using a pseudonym. Third, as noted earlier regarding the APA's (1992, 2001) code of conduct, this type of research does not require informed consent if the observations and the recordings of the behavior represent naturalistic observation of behavior performed in public places and cannot be used to harm the individual.

The logic of these observations leads to the simple conclusion that the collective exchanges among persons in various virtual communities are public events that support no expectation of privacy. Consequently, a researcher may have access to these records and publish them, exercising moderate discretion, as he or she sees fit. Although this argument offers the behavioral researcher much latitude, there may be additional circumstances that require a greater respect for privacy.

When a person is in a public place, he or she may do things that build an expectation of privacy. For example, I may whisper to my wife to share information that we consider intimate. The whisper affords a modest veil of privacy in that I have taken a precaution to prevent others from hearing what I want to say. Therefore, a researcher's use of a sensitive directional microphone penetrates this expectation of privacy. The Supreme Court used this very standard when it found that using a microphone outside a telephone booth violates a person's expectation of privacy (Kyllo v. United States, 2001).

Consider an individual who joins a moderated chat group specifically created for persons suffering from an affliction (e.g., alcoholism, sexual abuse, or multiple sclerosis). Within such a context, participants in the chat group may reveal intimate information in the hope of receiving support and counsel from other members of the group. Creators of the site may advertise the group as a "confidential" forum for only those persons with the affliction. For example, in the Finn and Lavitt (1994) study, the authors noted that the moderator of the group discouraged professionals who were not victims of sexual abuse from joining the discussion. It is conceivable, too, that a virtual community may limit entry to only those persons who have secured a password after having applied to join the community. Do such conditions represent an expectation of privacy?
It seems reasonable to presume that the level of expected privacy increases with the mechanisms used to screen participants of various virtual communities. Those communities with the fewest barriers to access appear to support the least level of expected privacy. By contrast, those virtual communities requiring an application procedure that assigns screen names to participants, requiring a confidential password for entry into the discussion, or using e-mail as the medium for intragroup communication creates prima facie evidence for the presumption of expected privacy.

The answer to the question is further resolved using the utilitarian principles that permeate the APA’s (1992) Code of Conduct. Specifically, one must consider the ethical costs to the participants relative to the benefits of the research. In the case of moderated support groups, researchers must explore the potential harm created by their passive analysis of ongoing dialogues.

Because of the nascent nature of Internet research, any list of potential harms is speculative, at best. Nevertheless, it is possible that repeated reports of Internet research, shared through the professional (i.e., scholarly journals) and popular media (i.e., television and news magazines) may have a chilling effect on individuals’ willingness to use support groups for fear that the intimate details of their lives will be scrutinized by unwanted intruders. Indeed, both King (1996) and Eysenbach and Till (2001) provided anecdotal evidence of the resentment expressed by members of virtual communities of researchers who were “lurkers” (individuals who read messages but do not participate in the dialogue). Consequently, some people may no longer benefit from participating in these groups. At the same time, however, research that examines the dialogue within these groups may reveal insights that will improve the quality of interventions provided for persons with specific afflictions. Dilemmas such as these illustrate the need to revisit conceptualizations of privacy.

Contemporary legal views of privacy have evolved in conjunction with advances in technology. For example, the advent of mass communication technology spurred Warren and Brandeis (1890) to conclude that the “numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops” (p. 195). Similarly, Westin (1967) helped to articulate the current principle of privacy when he concluded that “privacy is the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others” (p. 7). As Westin argued, the courts have continually refined the definition of privacy as technology has continued to amplify our primary senses and ability to distribute vast amounts of information rapidly.

The most recent iteration in the redefining of privacy appears in the Kyllo case. The justices paid considerable attention to whether the surveillance device represented “off the wall” versus “through the wall” surveillance. At issue was whether the device responded to energy emitted from the dwelling (i.e., the passive reading of radiated heat) or recorded reflected energy it emitted. The majority of the
justices concluded that although the agents used “off the wall” technology, it was nevertheless an invasion of privacy because it would reveal ordinary behaviors that one would wish to keep private such as when “the lady of the house takes her daily sauna and bath” (p. 10).

As behavioral researchers, we cannot necessarily rely on legal definitions to determine the parameters of our ethical behaviors. The constitutional protections of privacy, although designed to defend the person, guard against unwarranted government intrusion, not necessarily from the prying interest of our neighbors.\(^1\) In addition, although a behavior may be legal, it may not be ethical to the extent that it conflicts within the virtues expressed within various codes of conduct.

The APA’s (1992) \textit{Code of Conduct} offers no clear guidance for the current problem. Although the code directs psychologists to respect the autonomy, dignity, and privacy of individuals, section 6.12 allows researchers to dispense with informed consent if the researcher uses “anonymous questionnaires, naturalistic observation, or certain kinds of archival research” and he or she “consults with colleagues as appropriate.” Unfortunately, the guidelines offer no definition of privacy that would allow this consultation to lead to a clear or consistent answer. In other words, the APA \textit{Code of Conduct} requires that researchers respect the privacy of individuals without defining the curtilage of personal privacy. Such a shortcoming suggests that researchers proceed with due caution and seek a mechanism to reduce potential risks to participants. The following are several precautions that researchers should explore. I offer these recommendations in the hope of developing a dialectic that will explore the ethical dimensions of this dilemma.

\subsection*{Definition of Privacy}

The distinction between what is public and what is private is a penumbra as the expectation of privacy is a subjective phenomenon for the individual. Nevertheless, we may use one’s behavior to surmise his or her expectation for privacy. For example, a recovering alcohol-dependent person may reveal his or her condition at the weekly meeting of the Kiwanis Club. Clearly, such an admission implies that the person has no expectation for keeping private the history of his or her alcohol dependence. By contrast, such an admission during an Alcoholics Anonymous meeting implies an expected level of privacy because the members of the group agree that what its members share in the group is anonymous and confidential. Although the group does not enjoy the protections afforded a group conducted by a licensed professional, is open to anyone who wishes to attend, and does not require\(^1\)

\begin{footnotesize}
\begin{enumerate}
\item There are, of course, federal regulations and civil laws that protect the confidentiality of certain kinds of personal records. For example, the Office of Health and Human Services has established new standards for the privacy of individually identifiable health information. These regulations limit access to health-care information for both commercial as well as research purposes (Gunter, 2002).
\end{enumerate}
\end{footnotesize}
participants to use their full names, we would, nonetheless, respect the fact that its members may wish that their admissions remain private. We can apply this distinction to virtual communities. Those virtual communities that do have requirements for participation and requests for confidentiality deserve the respect for privacy one would confer in other venues.

The goal of applying this definition of privacy to the Internet is not to forestall Internet research, but to ensure that the ethical principles psychologists follow find consistent application in different settings. In light of this definition of privacy, researchers can take several steps to conduct ethically responsible research using these virtual communities.

Seek and respect the rules of the virtual community. As noted previously, individuals may organize a virtual community and wish to limit who may have access to the exchanges among the participants and how participants may use those exchanges. Because such moderation creates the presumption of privacy, it appears necessary for the researcher to seek permission to examine exchanges among the members of the community. Such a request is a common courtesy for any researcher who wishes to observe activities of a group. Even without a specific moderator, the virtual community may have established guidelines regarding the privacy of communications and general expectations of etiquette among its participants.

By way of analogy, Hood (1998) extensively studied and documented the religious practices of the serpent handling sects (SHS) by attending the various SHS churches located in the Appalachian states. Members of the church allowed Hood to observe the church services after he asked their permission and made clear his intent to study their beliefs and practices. Consequently, Hood had the implied informed consent of members of different SHS congregations to videotape their services, which occasionally include members handling vipers (a practice that is illegal in most states), drinking a strychnine solution, speaking in tongues, and the practices of laying on of hands and casting out of demons.

Editing of data reported. A second method for preserving the rights of the members of a virtual community revolves around the methods used to present the data collected from the group. The APA (1992) Code of Conduct makes clear that researchers are to present information in such a way that the identity of the participants remains confidential. Applied to data gathering through the Internet, this standard would include removal of references to the person’s name or pseudonym, and other information that could potentially identify an individual; and removal of reference to the name of the group.

Use of multiple groups. Another method for preserving privacy would be to use, when possible, several groups that serve a similar function. Not only will
such a tactic improve the representativeness of the data, the tactic will offer
greater anonymity to the members of the group.

INFORMED CONSENT

Related to the issue of privacy is the question of informed consent. Clearly, reactive
research, whether one uses the Internet or the traditional research setting, requires
that the participant offer informed consent prior to participating. Most Internet-
based research appears to require participants to acknowledge that they understand
the intent of the study and the nature of their participation before proceeding with
the data-gathering phase of the study. In fact, Internet research may make it easier
for the participant to terminate his or her participation by breaking the link to the
researcher's Web page. There are, however, several unique challenges regarding
informed consent that research with the Internet poses.

Technically, minors cannot legally consent to participate in research; they can
only assent to participate (Sieber, 1992). Although the researcher may require ver-
ification of the potential participant's age, there is no trustworthy mechanism to
verify the accuracy of the information submitted to the researcher. Regulations
that govern human research outline conditions for which parental consent is not
required. In essence, research that poses little or no risk to the participant does not
require parental consent (Sieber, 1992). Given that much of the current Internet
research is benign in nature (e.g., experiments in sensation and perception,
general opinion surveys, or measures of personality), the issue of minors offering
informed consent appears to be de minimis.

The problem of verifying the ability to offer informed consent becomes critical
when the researcher wishes to examine topics that are controversial and involve
potential risk to the participant. A researcher may wish to conduct Internet studies
that present material that others perceive as offensive, ask intimate questions, or
both. It is further conceivable that an institutional review board (IRB) in one com-

munity may find a research proposal acceptable by prevailing community stan-

dards that IRBs in other communities would find unacceptable. Researchers’ use
of deception is also problematic if participants can break the link with the Web
page prior to the end of the experiment and the dehoaxing session.

Binik, Mah, and Kiesler (1999) reviewed the ethical issues on conducting sex
research on the Internet and found that “common sense and current ethical
codes…are sufficient in most cases” (p. 82). As an example, they noted that re-
searchers conducting interviews of children may require the permission of the
child’s parent or guardian and that researchers should apply the same rule when
conducting similar studies through the Internet. Unfortunately, the Internet does
not readily allow the researcher to know who is participating. Children can easily
use their parent’s Internet service provider and pretend to act as the parent when
offering consent to participate in the research. Even for adults who wish to participate in a research project, there is no guarantee that they will read with care the informed consent documentation or debriefing materials.

Until a technical solution emerges for the identification of Internet participants, it appears that researchers will need to find alternative methods of enlisting participants in controversial research. First, researchers could require that participants submit their e-mail address thus ensuring that the researcher can send to the participants debriefing information even if the participant breaks communication with the researcher prior to the termination of the study. This option, however, compromises the antinomy of the participant, but may be a necessary risk to ensure that the researcher can adequately debrief the participants. Second, the researcher may use the Internet to enlist participants for a research project and then use other means to collect the data.

Finally, a researcher may create an enclave of research participants by enlisting colleagues who can verify the eligibility of participants. For example, Postmes, Spears, and Lea (2002) examined computer-mediated communication among college students enrolled at the University of Amsterdam and the University of Manchester. For this study, the researchers vetted the participants by having the students sign the necessary informed consent documents before giving them the necessary Web site information and participant-specific passwords to participate in the study. In essence, researchers who wish to engage in potentially controversial research may be able to enlist the aid of trustworthy gatekeepers who will assist in the recruitment and verification of eligibility of persons who may wish to participate in research through the Internet.

**DECEPTION AND FALSE FEEDBACK**

The matter of deception and the use of false information are perennial problems for researchers. The use of deception forces us to revisit issues of privacy to the extent that deception may cause individuals to say or do things they do not wish share in public. Elsewhere, I (Pittenger, 2002) argued that deception and false feedback are justifiable techniques under certain conditions. Among other protections, I recommended that researchers can use deception if their informed consent agreement specifies that the researcher must withhold certain information or may misrepresent specific aspects of the research. This condition presumes that the relative benefits of the research outweigh the relative costs to the participants of being temporarily deceived.

Deception in Internet research may be permissible to the extent that the researcher can obtain verified informed consent from the participants and can dehoax the participant even if he or she terminates participation before the end of the experiment. As noted previously, if the researcher can create an enclave of participants
who have given verified informed consent, then deception may be permissible. Nevertheless, the use of deception and false feedback with Internet research is risky to the extent that the researcher will not have the opportunity to adequately dehoax participants and determine their reactions to the manipulation.

Another concern is the researcher who wishes to engage in participant observation in various virtual communities. Imagine a researcher who wishes to study the depths of racism by joining several hate groups and then, posing as one of the group members, posts statements designed to evoke responses. One might be tempted to defend this tactic by arguing that there is no better way to obtain uncensored and detailed information regarding what many consider a harmful social condition and that such an analysis may lead to alleviating the problem. Two observations weaken this justification.

First, such actions appear to violate Principle B (Integrity) of the current APA (1992) Code of Conduct as well as Principle C of the proposed revisions (APA, 2001), which advise psychologists not to make misrepresentations of fact or engage in subterfuge. As I argued previously, such a ploy clearly violates the individual’s right to privacy as it tricks people to present beliefs that they may not wish to share outside the context of their virtual community. Second, the participants may unwittingly make statements that, according to state or federal law, the researcher must report. As such, the research tactic violates the principle that psychologists make others aware of the limits of confidentiality and minimize the harm caused to others. Therefore, the costs of such a research tactic appear to outweigh the potential benefits. Even in settings where the reactions of the participants may be temperate by comparison, failure of the researcher to disclose his or her intention to gather data represents an exploitation of other people.

In essence, there are three barriers to using deception in research conducted through the Internet. First, researchers cannot establish certain informed consent with the participants. The second problem, which is related to the first, is that the researcher cannot dehoax the participants and readily assess their reactions to the deception. One may address these problems by creating an enclave of research participants. This tactic would require some extraordinary logistical oversight to ensure the protections for the participants. Finally, surreptitious deception, regardless of the data it produces, remains an exploitative technique that falls beyond the range of permissible methods provided by the APA’s Code of Conduct.

METHODOLOGY AND ETHICS

Rosenthal (1994) offered a brief review of the relation between research methodology and ethics. In the main, his argument was that the validity of the research design and the inferences drawn from the data are a central ethical issue inasmuch as one must justify the ethical cost of conducting the research with the potential
benefits derived from the research. Because the Internet is an emerging medium for behavioral researchers, its use requires additional scrutiny. Specifically, review boards and consumers of the research require assurance that the data collected through an Internet research project will support reasonable empirical inferences.

Several methodological matters related to Internet research should receive attention from researchers proposing such projects. These concerns include self-selection of participants, multiple submissions from the same participants, and the veracity of the data collected.

Such concerns are not unique to the Internet, but are exceptionally salient given its structure. For example, many commentators (e.g., Brock, Green, & Reich, 1998; Brock, Green, Reich, & Evans, 1996; Hunt, 1996; Jacobson & Christensen, 1996; Mintz, Drake, & Crits-Christoph, 1996) raised serious questions regarding the Consumer Reports analysis of patients' perceptions of the effectiveness of psychotherapy and Seligman's (1995) interpretation of the results. Central to many of the criticisms were questions regarding the representativeness of the sampling frame and the potential for self-selection bias. It is foreseeable that similar debates regarding Internet-based research will emerge. Poorly conceived methodologies and unjustified inferences become an ethical concern in that conducting the research requires the expenditure of resources, especially the time and effort of the participants, and may "lead to unwarranted and inaccurate conclusions that may be damaging to the society that directly or indirectly pays for the research" (Rosenthal, 1994, p. 127). Hence, researchers who wish to conduct Internet research may need to consider the ethical ramifications of their research methodology.

All behavioral research is subject to self-selection bias. The Internet poses a particular challenge in that the method by which participants discover Internet psychological research is mysterious, at best. For example, Nosek, Banaji, and Greenwald (2002) noted that participants learned of their research project through "media coverage, links from other sites, search engines, and word of mouth, with media coverage having the most significant effect on response rate" (p. 102). Although their sample size was large (over 600,000 responses), the authors were clear to acknowledge that the sample was not necessarily representative of the population.

Indeed, given the fact that large segments of the population, chiefly the poor, do not have ready access to the Internet (Kraut, Scherlis, Mukhopadhyay, Manning, & Kiesler, 1996), one must question the degree to which the Internet will yield an adequate sample of a target population. In addition to the vague nature of participant recruitment is the problem of verifying the veracity of demographic information submitted by the participant and multiple submissions. The anonymity of the Internet also makes it difficult to verify who is participating in the research and how often an individual participates in the same research project.

The validity of the data collected through Internet sources is another point of scrutiny. At present, there are few data that would allow one to assume equivalence between results generated by a survey completed by an anonymous Internet
participant and the results of a survey conducted through conventional means (Buchanan, 2002). As Binik et al. (1999) noted, the Internet might introduce new sources of response bias that are yet unknown. Childress and Asamen (1998) echoed this concern when they noted that the written communication between client and therapist engaged in Internet therapy is qualitatively different from face-to-face verbal communication.

The Internet may well be the portal that provides researchers unprecedented access to diverse populations unimagined by previous generations of researchers. Researchers interested in people with rare diseases, such as multiple sclerosis, are readily able to conduct large-scale surveys that would be impractical if not impossible using conventional means. Nevertheless, the implications for the many unknowns associated with Internet research are that researchers will need to consider with care methodological issues that receive relatively little inspection in more mature research venues.

CONCLUSIONS

Although the Internet originally served the needs of military planners who wanted to ensure an uninterrupted exchange of information during national emergencies, the Internet has become a popular communication medium. More recently, researchers have begun to view the Internet as a new platform for conducting research. The primary focus of this article was to examine four ethical concerns associated with conducting Internet research, namely the preservation of privacy and confidentiality, the issuance of informed consent, the use of deception and false feedback, and the relation between methodological issues related to Internet research and ethics. These matters represent recurrent ethical concerns that researchers must address. These are also matters for which the Internet creates new challenges.

Regarding privacy, I argued that although the Internet is a public medium, individuals may have a reasonable expectation of privacy under certain conditions. Specifically, I argued that some types of virtual communities allow people to share intimate information that they do not wish to share outside the group. This expectation of privacy requires that researchers take steps to secure the permission of the group to engage in naturalistic observation of the exchanges within the group. I also examined the permissibility of researchers engaging in participant observation and found that researchers need to reveal their intent before embarking on such projects.

The Internet also poses interesting challenges for issuance of informed consent and the use of deceptive practices. The primary problem is that the Internet does not guarantee that the individual supplying informed consent understands the ramifications of the consent or is qualified to render consent. Similarly, the Internet does not ensure that the participant will engage in the researcher’s debriefing protocol and assessment of the effects of the deception. These problems suggest that
researchers find suitable means for protecting the participants of such research found in studies conducted in traditional laboratories.

Finally, I considered the ethical concerns related to methodological features of Internet research. In essence, research conducted on the Internet raises important questions related to internal and external validity that researchers need to examine in the design and interpretation of their research.

Although the Internet is a new and emerging resource for psychologists, many of the ethical questions its use poses can be resolved by examining reactions to past research and by refining the definitions of concepts used in ethical discussions. The resolution of potential ethical problems of Internet research will also benefit from researchers’ analysis of these ethical concerns in their research reports. Just as the community of researchers benefits by reading detailed accounts of methodological procedures for collecting and interpreting the data, so too will the community benefit from reading the ethical justification for conducting specific research projects. Given the novelty of the Internet as a research venue, such a discourse is essential.

REFERENCES


