Psychological Research Online

Report of Board of Scientific Affairs' Advisory Group on the Conduct of Research on the Internet

Robert Kraut — *Carnegie Mellon University*
Judith Olson — *University of Michigan*
Mahzarin Banaji — *Harvard University*
Amy Bruckman — *Georgia Institute of Technology*
Jeffrey Cohen — *Cornell University*
Mick Couper — *University of Michigan*

As the Internet has changed communication, commerce, and the distribution of information, so too it is changing psychological research. Psychologists can observe new or rare phenomena online and can do research on traditional psychological topics more efficiently, enabling them to expand the scale and scope of their research. Yet these opportunities entail risk both to research quality and to human subjects. Internet research is inherently no more risky than traditional observational, survey, or experimental methods. Yet the risks and safeguards against them will differ from those characterizing traditional research and will themselves change over time. This article describes some benefits and challenges of conducting psychological research via the Internet and offers recommendations to both researchers and institutional review boards for dealing with them.

The Internet and the widespread diffusion of personal computing have the potential for unparalleled impact on the conduct of psychological research, changing the way psychologists collaborate, collect data, and disseminate their results. In this article, we focus on the way the Internet is changing the process of empirical research, identifying both opportunities and challenges. The Internet presents empirical researchers with tremendous opportunities. It lowers many of the costs of collecting data on human behavior, allowing researchers, for example, to run online experiments involving thousands of subjects with minimal intervention on the part of experimenters (Nosek, Banaji, & Greenwald, 2002b). Internet chat rooms and bulletin boards provide a rich sample of human behavior that can be mined for studies of communication (Galegher, Sproull, & Kiesler, 1998), prejudice (Glaser, Dixit, & Green, 2002), organizational behavior (Orlikowski, 2000), or diffusion of innovation (Kraut, Rice, Cool, & Fish, 1998), among other topics. The Internet is also a crucible for observing new social phenomena, such as the behavior of very large social groups (Sproull & Faraj, 1995), distributed collaboration (Hinds & Kiesler, 2002), and identity switching (Turkle, 1997). These phenomena are interesting in their own right and have the potential to challenge traditional theories of human behavior.

At the same time, the Internet raises concerns about data quality and the treatment of research subjects. Researchers often lose control over the context in which data are procured when subjects participate in experiments online. Ensuring informed consent, explaining instructions, and conducting effective debriefings online may be more difficult than in traditional laboratory settings. Observations in chat rooms and bulletin boards raise difficult questions about risks to subjects, including privacy and lack of informed consent.

This article will discuss both the advantages and the challenges associated with conducting psychological research online. We think the problems in conducting research online can be mastered, and we close with recommendations directed toward both the researcher and the institutional review boards (IRBs) that oversee the protection of human research subjects.

Opportunities of Internet Research

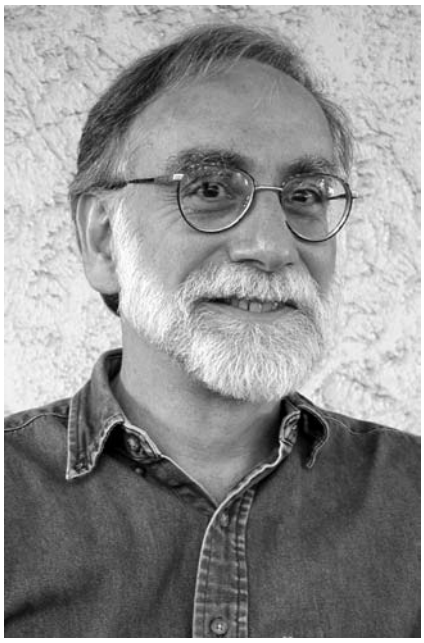
The Internet can have a positive impact on the conduct of psychological research, both by changing the costs of data collection and by making visible interesting psychological phenomena that do not exist in traditional settings or are difficult to study there.

Editor's note. William C. Howell served as action editor for this article.

Author's note. Robert Kraut, Human-Computer Interaction Institute, Carnegie Mellon University; Judith Olson, School of Information, University of Michigan; Mahzarin Banaji, Department of Psychology, Harvard University; Amy Bruckman, College of Computing, Georgia Institute of Technology; Jeffrey Cohen, Weill Medical College, Cornell University; Mick Couper, Institute for Social Research, University of Michigan.

Correspondence concerning this article should be addressed to Robert Kraut, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213. E-mail: robert.kraut@cmu.edu

0003-066X/04/$12.00
Vol. 59, No. 2, 105–117 DOI: 10.1037/0003-066X.59.2.105



Robert Kraut

Making Empirical Research Easier

Compared with other modes of collecting data, the Internet can make observational research, self-report surveys, and random-assignment experiments less expensive and easier to conduct.

Subject recruitment. Use of the Internet decreases the cost of recruiting large, diverse, or specialized samples of research subjects for either surveys or online experiments. This technique can provide a large, diverse sample at low cost. For example, in five years, Nosek et al. (2002b; see www.implicit.edu) collected over 2.5 million responses in tests of implicit attitudes and beliefs. One can post a research opportunity at Web sites that specialize in advertising such opportunities, such as the one hosted by the Social Psychology Network (http://www.socialpsychology.org/expts.htm) or the American Psychological Society (http://psych.hanover.edu/APS/exponnet.html). Commercial services, such as Survey Sampling (http://www.surveysampling.com), can be used to identify and select samples or to post a questionnaire to a nationally representative panel (http://www.knowledgenetworks.com/). Alternately, one can invite participation by sending personalized e-mail messages to active subjects in either specialized or more general online communities (see Couper, Traugott, & Lamias, 2001, for a review of sampling approaches for Internet surveys).

In one sense, the Internet has democratized data collection. Researchers no longer need access to introductory psychology classes to recruit research subjects and often do not need grant money to pay them. One consequence is that faculty at small schools, independent scholars, graduate students, and undergraduates can all potentially contribute to psychological research. For example, an undergraduate psychology major, Nicholas Yee (2003), published findings about the psychology of playing online multiplayer games, collecting over 18,000 responses from 3,300 players of the Internet game EverQuest. However, a corollary of this open access is that those with minimal training and supervision can conduct and publish research, without benefiting from the quality control imposed by subject-pool supervisors, peer reviews, and funding agencies.

Observing social behavior. The Internet provides scientists interested in social behavior with many archives of communication, from online groups discussing topics as diverse as medical support, hobbies, popular culture, and technical information. Researchers have used these online groups to study such social processes as personal influence (Cummings, Sproull, & Kiesler, 2002), negotiation (Biesenbach-Lucas & Weasenforth, 2002), and identity formation (McKenna & Bargh, 1998). Because people communicate online using text, these conversations are pretranscribed. The use of automated coding and content-analysis tools, such as MacWhinney's (2000) CLAN software, available at http://childes.psy.cmu.edu/clan/, further speeds the research process.

Many online forums make visible psychological phenomena that would be much more difficult to study in traditional settings. Some phenomena, like the evolution of groups or long-term learning, are difficult to study because of the difficulties and costs of tracking many individuals over long periods. The Internet provides a new venue for such long-term research on groups. For example, Baym (1998) was able to explore the way groups develop a sense of community, by examining an e-mail distribution list about soap operas over several years. Bruckman (1999) was able to study the influence of groups on long-term learning, by examining the online conversations of 475 children learning a programming language over a five-year period. Finally, Bos, Olson, Gergle, Olson, and Wright (2002) examined the development of social capital, by having large groups participate in an experiment on the Web over a 30-day period. In contrast to conducting observational research in face-to-face settings, such as classrooms or public parks where researchers' presence may contaminate the phenomenon under study, researchers can be less obtrusive when conducting observation online. For example, Butler (2001) was able to study attraction of individuals to groups and their retention by surreptitiously creating an archive of all messages sent to 206 online groups over a three-month period.

Access to other archival data. The detailed transaction logs that people leave when using the Internet provide a wealth of detailed, unobtrusive data for phenomena other than social behavior (Webb, Campbell, & Swartz, 1999). These transaction logs include browsing behavior, software use, purchasing behavior, file uploads and downloads, subscription to communication forums, e-mail sending, and a host of other digital transactions. For example, researchers have used the Internet as a source of data about individual preference and choice (Montgomery, 2001), so-

Judith Olson

cial loafing and altruism (Adar & Huberman, 2000), and friendship patterns (Adamic & Adar, 2001), among other topics.

Automation and experimental control. One of the benefits of online research is that it allows automation and experimental control that can be otherwise difficult to achieve without the use of computers. A primary advantage of the Internet for both survey and experimental research is the low marginal cost of each additional research subject. Unlike traditional laboratory experiments or telephone surveys, where each new subject must be greeted, instructed, and supervised by a person, most online experiments and surveys are automated. A human experimenter does not need to give instructions, introduce the experimental manipulation, and/or supervise data collection.

Consider how Web surveys are changing the nature and economics of questionnaire-based research. Cobanoglu, Warde, and Moreo (2001) estimated that marginal unit costs for postal mail surveys are $1.93. Practitioners estimate that the per-completed interview costs for telephone surveys range from $40 to well over $100. In contrast, the marginal cost is close to zero for a Web-based survey, although fixed costs for the Web are higher.

Unlike conventional paper-based questionnaires, Web surveys are both flexible (asking different questions based on earlier responses) and less error prone (because they don't require human transcription). This flexibility means that researchers can embed true experiments in surveys, varying instructions, scenarios, or questions based on subject characteristics or on responses to earlier items. The National Science Foundation has funded infrastructure to support nationally representative experiments using Internet technology (http://experimentcentral.org/). In addition to self-reports, researchers can capture metrics such as time online, response latencies, changed answers, or backing up, permitting richer analysis of the process of the experiment and variations in its execution across subjects.

Many software packages and services, such as http://www.surveymonkey.com, can create and host simple online questionnaires, with data automatically written to a database and statistically summarized. Complex experimental or survey logic, however, is currently beyond the capabilities of many of these questionnaire generators, and constructing complex questionnaires or experiments requires programming expertise (see Crawford, 2002, for a review of this type of software; http://www.asc.org.uk/ maintains a list of software for online surveys).

Examining the Internet as a Social Phenomenon

Not only can the Internet increase the efficiency of studying traditional psychological phenomena, its use is also an important phenomenon in its own right. Just as psychologists have long been interested in the way that television influences child development, prejudice, and violent behavior (Huston et al., 1992), they are now examining the impact of the Internet on individuals (e.g., Kraut, Patterson, et al., 1998), dyads (McKenna, Green, & Gleason, 2002), groups (Cramton, 2002), and organizations (Sproull & Kiesler, 1991). For example, some researchers have focused on how computer-mediated communication differs from traditional face-to-face communication (see Walther & Parks, 2002, for a recent review). Others have used global teams and other new forms of work enabled by the Internet to reexamine how shared context and trust, often taken for granted in face-to-face settings, have their influence on group performance (e.g., G. M. Olson & Olson, 2000; Rocco, 1998).

Challenges of Internet Research: Data Quality

Although the Internet can expand research opportunities, it also raises concerns about data quality and generalizability.

Sample Biases

To whom does research based on Internet samples generalize? For psychologists, who often value internal validity over generalizability, the large and diverse samples online are preferable to the college sophomores on whom much psychological theory rests. But for sociologists, political scientists, and others who attempt to track the pulse of the nation or to generalize to broader groups beyond the subjects, the nature of Internet samples makes generalizability problematic (Couper, 2001a; Robinson, Neustadtl, & Kestenbaum, 2002; Smith, 2002).

Unlike random digit dialing of telephone numbers, which approximates a random sample of the U.S. population as a whole, no sampling frame currently exists that provides a random sample of Internet users. Generalizing from Internet samples to the larger population is especially problematic. Although the large demographic differences

Mahzarin Banaji

between Internet users and nonusers that existed in the 1990s have diminished, the two populations still differ on many demographic, social, and psychological dimensions (Robinson et al., 2002). For example, Internet users are more likely to be White and young and to have children than the nation as a whole (U.S. Department of Commerce, 2002).

Not only are Internet samples potentially biased, but further bias arises because of self-selection and dropout. Response rates to online surveys are typically lower than comparable mail or telephone surveys, and when given a choice of Internet or paper questionnaires, respondents still overwhelmingly choose paper (Couper, 2001b; Fricker & Schonlau, 2002). The problem of biased sample selection is especially problematic for longitudinal data collection. In surveys, for example, it is more difficult to maintain contact with Internet respondents than those contacted by telephone or mail because e-mail addresses change much more frequently than phone numbers or postal addresses. To increase response rates, researchers must be willing to switch to alternate modes of contact during the panel. To reduce nonresponse biases that result from drop out, researchers should consider adjustment strategies such as weighting and multiple imputation methods during data analysis (Rubin, 1987).

Control Over the Data-Collection Setting

When conducting surveys and experiments online, researchers lose control over the environment in which the research is conducted. In the laboratory, for example, an experimenter can verify subjects' identities, age, or gender; can tailor instructions to each subject; can monitor their behavior to ensure that they are involved and serious; can assess the effect of the research experience on them; and can intervene if the researcher perceives undesirable effects. When the researcher decides to collect data online, much of this monitoring and control is difficult if not impossible. These difficulties in monitoring and intervening in online data collection should encourage researchers to pretest instructions, manipulations, and data-collection instruments more thoroughly than they might do in laboratory settings.

The anonymous nature of the Internet allows people to participate frivolously or with malicious intent. This could involve multiple submissions by the same individual, widespread dissemination of the uniform resource locator (URL) for the purposes of flooding the site, and other nefarious behaviors designed to undermine the integrity of the research. Even if the distortions are not deliberate, online subjects may simply invest less time and energy in the research task than those involved in a telephone survey or laboratory experiment. For example, Williams and his colleagues (Williams, Cheung, & Choi, 2000; Williams et al., 2002) reported substantially higher dropout rates in conducting online experiments than they have observed conducting similar research in the laboratory.

Online research may require larger samples than comparable telephone-based and laboratory research to compensate for the greater error introduced when research subjects are not diligent. Inviting known individuals who are assigned unique identifiers to participate in online research and tracking Internet protocol (IP) addresses can help guard against multiple submissions. To assess and improve the quality of their data, researchers should use exploratory data analysis and systematic data mining to identify and eliminate records with anomalous data patterns or to determine the need for statistics robust to outliers.

Challenges of Internet Research: Protection of Human Subjects

In addition to potentially affecting data quality, conducting research online can affect human subjects and the actions that researchers must take to protect their welfare. We believe that online research poses no more risk to human subjects than comparable research conducted through other means, but conducting research online changes the nature of the risks and investigators' ability to assess it. Some of the challenges arise because fundamental concepts that underlie federal regulation for the protection of human subjects, such as the concept of minimal risk and public behavior, change or become ambiguous when research is conducted online. Other challenges arise because it is more difficult to assess subjects' identities or their reactions to the research experience online.

The basic ethical principles underlying research involving human subjects—respect for persons, beneficence, and justice—are contained in the Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). These principles have been formalized into the Federal Policy for the Pro-

Amy Bruckman

tection of Human Subjects (known as the *Common Rule*).[1] The regulation sets standards for assessing the degree of risk to human subjects and trade-offs between risk and benefit; for establishing and documenting voluntary, informed consent before people participate in research; and for the treatment of minors and other vulnerable populations. It established an oversight process called the IRB system, which assists those conducting research involving human subjects to comply with the spirit and the letter of the regulation.

Ambiguities in Key Concepts When Research Is Conducted Online

Both the broad ethical principles articulated by the Belmont Report and the detailed federal regulations about the protection of human subjects depend on key concepts, such as minimum risk, expectations of privacy, the notion of preexisting records, and anonymity, whose complex meanings are affected when research is conducted online. To illustrate this point, consider Figure 1, a flow chart outlining some of the criteria that a researcher or IRB needs to consider in determining whether the researcher needs to obtain and document informed consent from a research subject.[2] This decision involves determining:

- whether individuals are identifiable or anonymous,
- whether behavior is public or involves reasonable expectations of privacy,
- whether individuals expected that records were being created or expected that their behavior was ephemeral,
- whether subjects expected that records about them would be made public or kept private,
- and the degree of risk associated with the research experience.

Each of these determinations is likely to change when the research is conducted online, rather than through a more conventional mode. We consider these issues in more detail below.

Identifiable Versus Anonymous Information

Determining whether an individual is identifiable or anonymous has implications for the risks subjects are exposed to, whether the research is exempt from federal human-subjects regulations, and whether the research is even defined as involving human subjects at all. According to the federal regulations (C.R. § 102(f)), research involves human subjects only if data are collected through interaction with a subject or if it collects "identifiable private information." Observations of public behavior, in which individuals cannot be identified directly or indirectly, are exempt from the federal regulations protecting human subjects (C.R. § 101(b)).

As we will discuss, the greatest risk associated with online research centers on breaches of confidentiality, in which private, identifiable information is disclosed outside of the research context. In the case of online survey and experimental research, the researcher can often reduce this risk by explicitly not asking for identifying information or by recording personal identifiers separately from the research data.

In observations of naturally occurring online behavior, however, anonymity is more difficult to achieve, and the very nature of anonymity versus identifiability becomes ambiguous. Suppose one wishes to quote statements made in an online forum. One cannot assume that pseudonyms, often used by individuals to simultaneously mask and express their identities online, render their conversations anonymous, because posters may choose pseudonyms that contain part or all of their real names or disclose information that publicly links their pseudonyms to their real identities (see Bassett & O'Riordan, 2002, for a fuller discussion). Even seemingly anonymous snippets of text posted in an online diary (known as a Web log or blogs) or online forum may be traced back to individual posters through the use of Internet search engines. Therefore, to preserve anonymity, researchers should disguise pseudonyms and alter quoted text.

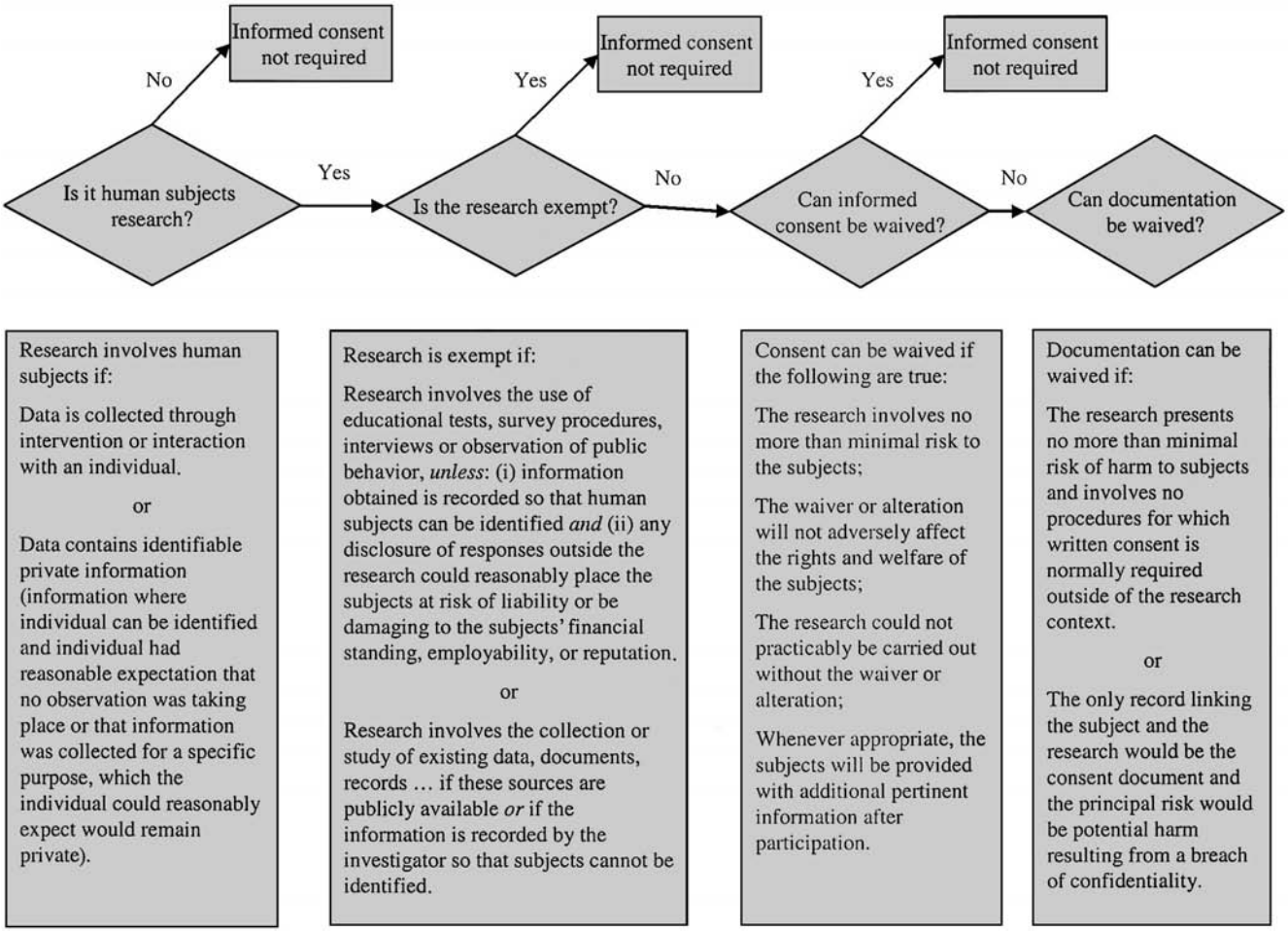
Public Versus Private Behavior

Some have argued that scientists can record public Internet-based communication without the knowledge or consent of

[1] Federal regulations are published in the Code of Federal Regulations (C.F.R.). Each of the federal agencies and departments that has adopted the Common Rule has published it with different C.F.R. numbers (e.g., the Department of Health and Human Services' regulations are published as 45 C.F.R. pt. 46, 1999). The content is identical for each. In referring to sections of the Common Rule in this document, we will use the notation C.R. § 102(b), where the C.R. stands for the document (i.e., the Common Rule) and the code following the § stands for a part number and letter subsection. The Office of Human Subjects Protections posts a copy of the Common Rule at http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm

[2] For a complete set of criteria, see the Common Rule.

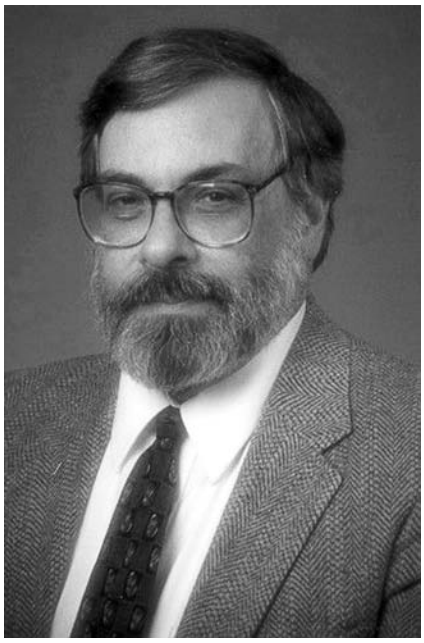
Figure 1
Some Factors Relevant to Internet Research Influencing Whether Informed Consent Is Required and Must be Documented



subjects, because this constitutes observation of public behavior (Herring, 1996). Many online communication forums have unrestricted membership, allowing anyone who comes by to participate in conversation or observe it. For example, lurkers (individuals who read messages but don't post them) represent well over 50% of subjects in many e-mail distribution lists (Nonnecke & Preece, 2000). In such cases, we believe that people who post in these groups should have no reasonable expectation of privacy, and researchers and IRBs should be able to treat online communication in them as public behavior.

There are, however, important caveats about when online communication should be treated as public behavior. The federal regulation bases its definition of private information on the expectation of privacy. Whether a person conversing online can reasonably expect the communication to be private depends on legal regulation, social norms, and specific details of implementation, all of which are changing. Implementation details include such features of the online settings as the number of people who subscribe, whether membership is restricted or open, whether membership is static or rapidly changing, whether conversations are ephemeral or archived, whether the presence of lurkers is visible, and whether the forum has posted explicit recording policies. Researchers and IRBs need to take considerations such as these into account on a case-by-case basis when deciding about the status of online communications among individuals on an electronic distribution list (e.g., Baym, 1993) or an Internet chat room (e.g., Bull & McFarlane, 2000).

The ethical considerations should be influenced by relevant legislation, but the laws about the privacy of computer-based electronic communication are still evolving. The Electronic Communications Privacy Act (1986) states that it is illegal to intercept electronic communications. Private e-mail and instant messaging exchanged be-



Jeffrey Cohen

tween individuals are considered protected communication. However, this protection does not include most group-oriented communication, such as bulletin boards, public distribution lists, and chat rooms, even ones where members must enter a password before participating, if the person recording the information is considered a "party to the communication." The communication is also not protected if "the electronic communication system . . . is configured so that such electronic communication is readily accessible to the general public" (Electronic Communications Privacy Act, 1986, 18 U.S.C. § 2511(2)(g)(I)).

Whether behavior should be considered public or private also depends on changing features of technology. For example, many Web sites automatically create logs showing the IP address of the machines that visit the site. When a person has exclusive use of a personal computer with a fixed IP address, knowing the IP address is tantamount to knowing the identity of its user. However, dynamic IP addresses, in which one of a fixed number of addresses is assigned to a machine on the fly, do not translate into individual identifiers. In the case of dynamic IP addresses, tracing the address only identifies the machine pool, not the individual machine or its user.

Preexisting Public Records

Research is exempt from human-subjects regulations if it involves collecting preexisting public data, documents, and records (C.R. § 46.101(b)(4)). We addressed the ambiguity in the definition of *public* previously. The concept of preexisting is also ambiguous. In order to be preexisting, all of the data must exist prior to the beginning of the research, such as research on archives of online discussions. Data that are generated during the course of the research, such as postings to a blog (i.e., a Web log or online diary posted for public consumption and comment) or to a live discussion group would not be considered preexisting. Such research would qualify for expedited review: "Research involving materials (data, documents, records, or specimens) that have been collected, or will be collected solely for nonresearch purposes" (Categories of Research That May Be Reviewed by the Institutional Review Board [IRB] Through an Expedited Review Procedure, 1998). Under expedited review, the requirements for informed consent must be considered, but the expedited reviewer can waive those requirements if the regulatory criteria are met.

Risk to Subjects From Internet Research

Both general ethical principles and federal regulation require that the risks to subjects from participating in research be minimized. Although few psychological studies involve physical risk, they can involve social, psychological, economic, and legal outcomes that may have harmful effects. According to the federal regulations, research has minimal risk when "the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life" (C.R. § 102.(i)).

Internet research involves two potential sources of risk:

- harm resulting from direct participation in the research (e.g., emotional reactions to questions or experimental manipulations) and
- harm resulting from breach of confidentiality.

Harm as a Consequence of Participation in Online Research

Much online research involves minimal risk. It exposes subjects to innocuous questions and benign or transient experiences with little lasting impact. In general, online surveys, experiments, or observations are no more risky than any of their offline counterparts. In some respects, they may be less risky, because the reduced social pressure (Sproull & Kiesler, 1991) in online surveys or experiments makes it easier for subjects to quit whenever they feel discomfort. This freedom to withdraw is no trivial benefit, given the strong pressures to continue in face-to-face studies (e.g., Milgram, 1963) and even telephone calls.

Although risk in online settings is typically low, the actual risk depends on the specifics of the study. For example, some questions in a survey or feedback from an experiment may cause subjects to reflect on unpleasant experiences or to learn something unpleasant about themselves (e.g., Nosek et al.'s, 2002b, research on automatic stereotyping). Experiments that deliberately manipulate a subject's sense of self-worth, reveal a lack of cognitive ability, challenge deeply held beliefs or attitudes, or disclose some other real or perceived characteristic may result in mental or emotional harm to some subjects. The concern in online research is not that some subjects are at risk. Risks can be justified if the potential benefits of the research are substantial enough and the cost—benefit analysis

Mick Couper

is no different in evaluating online research than in medical research or in traditional psychological research. Rather, the special concern is that researchers may have a diminished ability to monitor subjects in online research and remediate any harm caused by the research.

Although not explicitly covered in the Common Rule, research subjects may be harmed if the welfare of the online groups in which they participate is damaged by the research. Consider online social-support groups, where people who confront a common health or other problem share information, empathy, and advice. King (1996) quoted a member of an online support group who wrote that she was not going to participate actively because of a researcher's presence in the group: "When I joined this I thought it would be a *support* group, not a fishbowl for a bunch of guinea pigs" (p. 122; see Eysenbach & Till, 2001, for similar concerns). When conducting cost—benefit analysis for research, investigators and IRBs alike must consider these subtle consequences of their decisions.

Debriefing

American Psychological Association (2002) ethical guidelines call for debriefing subjects—providing an explanation of the nature, results, and conclusions of the research—as soon after their participation as practical. If deception was involved, the researcher needs to explain the value of the research results and why deception was necessary. If investigators become aware during the debriefing that research procedures have caused harm to a subject, they are to take steps to ameliorate the harm.

When conducting research online, researchers can post debriefing materials at a Web site, can automatically update these material as new results become available, and can tailor debriefing materials to particular experimental conditions or even individual subjects. There are even methods to provide debriefing materials to those who leave before completing the research (Nosek, Banaji, & Greenwald, 2002a). For example, researchers can deliver debriefing material through a link to a "leave the study" button or through a pop-up window, which executes when a subject leaves a defined Web. As suggested earlier, however, appropriate debriefing in online research may be difficult. The absence of a researcher in the online setting makes it difficult to assess a subject's state and therefore to determine whether an individual has been upset by an experimental procedure or understands feedback received.

Breach of Confidentiality

We believe that a greater risk of harm in online research comes from possible disclosure of identifiable private information outside of the research context, not from the experience of participating in the research itself. The identifying information can include records of statements, attitudes, or behaviors coupled with names, e-mail addresses, partially disguised pseudonyms, or other identifying information. Researchers must ensure adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

Identifying information may be inadvertently disclosed either as the data are being collected or, more commonly, when they are stored on a networked computer connected to the public Internet. Data in transit are vulnerable, for example, if a subject or automated process sends data to the investigator by e-mail. The store-and-forward nature of e-mail means that the message may rest in temporary directories on intervening computers before it is finally delivered to the addressee. The danger is less for data collected through automated Web surveys, although "sniffing" programs can eavesdrop on data in transit to search for known patterns, such as social security numbers, credit card numbers, or e-mail addresses. These risks can be avoided by not collecting identifying information or by separating these data from other research data. Although analogous risks can occur with paper forms, they are higher when data are shipped over the Internet, because of the openness of the networks and the possibility of automated pattern detection.

Greater risks to confidentiality result from outsiders gaining access to stored data files, either through deliberate hacking or because researchers mistakenly distributed them. This risk is not unique to online research but is a challenge for all data stored on networked computers. The standard approach to dealing with problems of confidentiality is to separate personal identifiers from other data describing subjects. Thus, one should keep identifying information, such as names and addresses, in one file and data in a second, with an arbitrary code number to link the two. Tourangeau, Couper, and Steiger (2003) illustrated some techniques used to maintain separation of identity from data in survey research involving sensitive data.

Maintaining the confidentiality of data stored on computer systems may require psychologists to become more sophisticated about computer technology than

many currently are. Researchers should configure their computers so that only those with a need to know have access to directories containing research data and should regularly check the permissions. They should routinely keep abreast of the security alerts issued by their vendors and apply security updates when these are released. For sensitive data, directories can be password protected, and sensitive files can be encrypted. Many investigators, however, fail to take these precautions to protect their data.

A special complication in maintaining a subject's anonymity arises when an investigator conducting online research must match different pieces of information from the same respondent. For example, the hypertext markup language (HTML) protocol, in which most Web surveys are authored, does not keep history from one page view to another and link responses from a single respondent. There are a variety of ways to keep track of a respondent's answers across several Web pages without compromising anonymity, such as session cookies, which are stored in memory; hidden values embedded in the HTML; or environment variables such as IP address.

Paying online subjects for their participation may also link subjects' responses to their identities when sending a payment requires a mailing address or accounting regulations require a social security number. Some researchers have severed this link by buying gift certificates from online retailers, such as Amazon.com, and displaying the unique certificate number to a respondent at the completion of a questionnaire. Thus, subjects can redeem their certificates without revealing their identity.

The degree of concern over confidentiality and steps taken to ensure it should be directly related to the sensitivity of the data being collected. One is less concerned when subjects are anonymous or when the information about them is innocuous (i.e., its revelation would bring no harm or embarrassment to subjects). Many online surveys and experiments fall into one or both of these categories. In these cases, use of passwords, encryption, or strong assurance to research subjects is not needed and may harm the research. For example, as Singer, Hippler, and Schwarz (1992) demonstrated, overly elaborate assurances of confidentiality may actually heighten rather than diminish respondents' concern, causing subjects to be less willing to provide sensitive information. Strong security measures (e.g., using secure socket layer protocols) may prohibit some research subjects from participating.

However, when subjects are identifiable and the research involves data that place them at risk of criminal or civil liability or that could damage their financial standing, employability, insurability, reputation, or could be stigmatizing, investigators must be especially concerned about breaches of confidentiality. Under these circumstances, standard security measures in place for electronic commerce, such as encryption and secure protocols, are likely to be sufficient. Numerous tutorials outline the options (e.g., Garfinkel, Spafford, & Russell, 2002).

Informed Consent

Investigators must typically obtain and document voluntary informed consent from research subjects, in which subjects freely agree to participate after they understand what the research involves and its risks and benefits (C.R. § 116). Federal human-subjects regulation also requires that informed consent be documented by the use of a "written consent form approved by the IRB and signed by the subject" (C.R. § 117). It is difficult to obtain legally binding signatures online. However, IRBs can waive the requirements for written documentation of informed consent for minimal-risk research either when the research would not require informed consent outside a research context or when the documentation is the only link between the research data and a subject's identity (C.R. § 117(c)). In the case of much online research involving adults, these conditions for waiving documentation of informed consent are met, and we recommend that IRBs should waive the document and allow a procedure in which subjects click a button on an online form to indicate they have read and understood the consent form.

As we have indicated earlier, the lack of interactivity in online research means that the investigator often cannot tell whether a subject understood the informed consent statement. As a result, online research may require more pretesting of these statements than research conducted in other venues. Researchers can increase the likelihood that subjects are granting truly informed consent by requiring feedback from subjects about their level of understanding, for example, by requiring a "click to accept" for each element in an informed consent statement or even administering short quizzes to establish that a subject understood. As with efforts to protect confidentiality, however, these extra efforts to ensure informed consent may reduce response rates, increase nonresponse to sensitive items (Singer, 1978), and possibly produce biased data (Trice, 1987). Therefore, these techniques are recommended only for research involving more than minimal risk to the subject.

These simple procedures for research involving competent adults may not be appropriate for online research involving children and other vulnerable groups, such as the mentally handicapped. According to federal regulation, these populations are not empowered to give consent for themselves. Their parent or guardian must consent, and the child may optionally be asked to assent. Here the inability to establish the subjects' identity is especially problematic, because researchers cannot easily determine whether online subjects are revealing their true age and because children can easily pretend to be their parents. Researchers can institute procedures to more reliably distinguish children from adults by having subjects enter information that is generally available only to adults (e.g., credit card numbers) or by requiring that they register with a trusted authority, such as VeriSign (http://www.verisign.com/products/asb/). Depending on the risk involved, the researcher and IRB must either accept the possibility that unidentified minors participated in the research or that they

forged parental consent or insist that a legally verified signature accompany the consent form, by conducting the research offline. Note that researchers working with children online are subject not only to human-subjects regulations, but also to the Children's Online Privacy Protection Act (1998; see http://www.ftc.gov/ogc/coppa1.htm). Researchers are prohibited from collecting personal information from a child without posting notices about how the information will be used and without getting verifiable parental consent.

Advice to Researchers and Institutional Review Boards

Conducting research online offers great opportunities for psychological research, and researchers should embrace this way of conducting empirical research, while protecting data quality and the rights of human subjects. In general, research on the Internet is not inherently more difficult to conduct or inherently riskier to subjects than more traditional research styles. But because the Internet is a relatively new medium for conducting research, it raises ambiguities that have been long settled in more conventional laboratory and field settings. The sections below provide some guidance to researchers and to the IRBs that monitor their conduct.

Understand and Guard Against Potentially Biased Samples

Guarding against sampling biases, aberrant behavior, and fraudulent data are all issues to be addressed before the study begins. Investigators can reduce fraudulent data by tracking IP addresses, putting cookies on subjects' computers, and tracking sign-ons from those who were invited to participate. They can improve the validity of data from experiments and surveys by programming input forms to check for anomalous values or suspicious patterns of data and by using exploratory data analysis to understand their data before analyzing it using inferential statistics.

Keep Quality Up and Do Not Pollute the Pool

The very economies and ease of access that make the Internet an attractive research medium pose a dilemma of the commons (Hardin, 1968; M. Olson, 1971). Without the quality control imposed by granting agencies or those who supervise subject pools, it is easy for unqualified or neophyte researchers to contaminate large numbers of potential research subjects. Low-quality academic research conducted online is having consequences similar to that of commercial e-mail and telemarketing—undermining the ability of legitimate researchers to collect data online. Researchers should restrain themselves and supervise their students, so that they contact the minimal number of potential subjects appropriate to their research goals.

Pilot and Pretest

Because research online is new and researchers get less direct feedback from subjects than they do in other settings, they should pretest informed consent forms, manipulations, and measures with a wide range of people. Researchers who have run surveys and experiments online recommend starting with small pilot projects to identify how online data-collection methods differ from conventional ones. Nosek et al. (2002a), for example, recommended that a pilot project explicitly attempt to replicate a phenomenon well known in the offline setting. Once comparability of subject behavior can be established, then new variables can be addressed with greater confidence.

Distinguish Between Public and Private Behavior Online

Many unrestricted e-mail distribution lists, online chat rooms, and multiplayer games provide opportunities to observe behaviors that are as public as the behaviors seen in city streets and parks. In the case of research involving minimal risks, these observations should be considered preexisting records or nonidentifiable public behavior and will be exempt from the Common Rule regulations, requiring only administrative review from an IRB. Some research involving online behavior, however, is less clear cut and may pose more subtle ethical dilemmas than those surrounding observation in more conventional public places. Seemingly anonymous conversations can be tracked down to individual Internet users. Data recording should disguise pseudonyms and text, because these can be often traced back to subjects' identities. Subjects who communicate or leave transaction data online may have reasonable expectations of privacy, depending on posted privacy policies, the size and stability of the forum, and many implementation details, such as whether conversations are routinely archived. When the research involves subject observation, with researchers themselves contributing to online forums, then the online communication should no longer be considered the study of existing records or observation in public places. Researchers and IRBs guiding them must take these ethical considerations into account when assessing the status of online records. We believe they should also take into account harm to the community of users frequenting an online site and not just a particular research subject from whom data are collected when assessing risks to human subjects.

When Risk Is Low, Use Sensible But Not Extreme Protections

No purpose is served when researchers or their IRBs place hurdles in front of research involving minimal risk. One should not use overelaborate informed consent statements, extensive assurances of confidentiality, encryption, or digital signatures when risks are minimal. Instead, one can guard against risk with lower keyed approaches. IRBs should waive documentation of informed consent, for example, by agreeing to a "click to assent" button for experiments and by permitting continued participation to signal consent for minimal-risk, online surveys. For low-risk surveys and experiments, debriefing material can be customized to subjects' behavior and delivered as an updated set

of frequently asked questions, if necessary. Because the most likely risk for data collected online is the breach of confidentially, investigators should use good data-management practices to lessen this risk. In particular, stripping identifiers from data, storing identifiers and data in separate files, auditing the security of data directories, and installing security patches on operating systems should be routine practice for all research involving human subjects, whether conducted online or off.

When Risk Is High, Use Stronger Safeguards or Do Not Use the Internet

Research that places human subjects at greater risk, either as a direct consequence of the research experience itself or from disclosure of sensitive data, requires stronger safeguards or may not even be appropriate for the Internet. Because investigators have reduced ability to assess a subject's state or to respond to evidence of distress when conducting online research, deception experiments and research that exposes subjects to stressful events may be problematic if conducted online. Researchers should screen respondents, either through sample selection or through preliminary data collection, to screen out vulnerable populations. The greater freedom of subjects to withdraw from online research is a mixed benefit. Subjects can more easily leave online settings before experiencing severe distress than they can in phone interviews or laboratory settings, but they can also leave before being adequately debriefed. To counteract early withdrawal, researchers can arrange their study so that subjects are sent to a debriefing site automatically at the end of a session, and debriefing material can be customized to their behavior.

If the data collection involves highly sensitive information, engage extra precautions. In addition to the standard practice of separating identifying information from the data itself, a researcher might consider engaging an outside service to acquire subjects, collect the data, and arrange for payment, if appropriate. In this way, the researcher is never in possession of the identifying information that would harm the subject.

With sensitive topics, such schemes as certified digital signatures for informed consent, encryption of data transmission, and technical separation of identifiers and data may be warranted. Research with sensitive topics may require strong verification that the assent is from the person who purports to be answering, including digital signatures or mailed consent. There are special difficulties if the research involves minors. Depending on the sensitivity of the information collected, parental consent may have to be acquired on paper, to ensure the parents are fully informed about the experience their child will have in the research.

Take Special Precautions When Dealing With Research Involving Minors

The Internet may appeal to researchers conducting research on children and adolescents because of the large numbers of minors using it. Research involving minors requires parental consent. Because of the difficulty of verifying the age and identity of people online, researchers will need to take special steps in conducting research with minors. For example, to ensure parental consent, they may need to ask for data that only an adult would have (e.g., a portion of a driver's license). Even if the research targets adults, if the research also appeals to minors (e.g., research about an online game), researchers may need to program their site to screen out self-identified minors or to place more effortful guards around the site.

Populate IRB Boards With People Who Understand These Issues

The Internet as an environment through which to conduct research is in flux. The ambiguities in defining what public behavior is and in choosing the technologies to obtain informed consent and document it are but two cases in point. As Figure 1 illustrates, even a seemingly simple decision about whether data collection should be considered human-subjects research becomes ambiguous when research is conducted online. In navigating these issues, researchers and IRBs will need expertise, which many currently lack. This includes expertise both about online behavior and about technology. For example, whether communication in a support group should be considered private or public may depend on conventions established by those who frequent support groups and on developments in commercial services that archive and index online communication.

A number of issues about security, digital signatures, procedures for stripping identifying information, and provisions for one-on-one debriefing require specialized technical expertise. Federal regulations encourage IRBs to consult with "individuals with competence in special areas to assist in the review of issues which require expertise beyond or in addition to that available on the IRB" (C.R. § 46.107). We recommend that all IRB boards have technical consultants who can be called on when needed. Because these issues of protecting data quality and human subjects in online research are new, we recommend that IRBs undertake an educational mission to inform researchers about the issues, the judgments that are now involved, and remedies for ensuring the health and protection of subjects in online research.

REFERENCES

Adamic, L., & Adar, E. (2001, March 2). *Friends and neighbors on the Web.* Retrieved November 2, 2003, from http://www.hpl.hp.com/shl/papers/web10

Adar, E., & Huberman, B. A. (2000). Free riding on Gnutella. *First Monday, 5*(10).

American Psychological Association. (2002). *Ethical principles of psychologists and code of conduct, Draft 7.* Washington, DC: Author.

Bassett, E. H., & O'Riordan, K. (2002). Ethics of Internet research: Contesting the human subjects model. *Journal of Ethics and Information Technology, 4,* 233–247.

Baym, N. (1993). Interpreting soap operas and creating community: Inside a computer-mediated fan culture. *Journal of Folklore Research, 30,* 143–176.

Baym, N. (1998). The emergence of on-line community. In S. Jones (Ed.), *CyberSociety 2:0: Revisiting computer-mediated communication and community* (pp. 35–68). Newbury Park, CA: Sage.

Biesenbach-Lucas, S., & Weasenforth, D. (2002). Virtual office hours: Negotiation strategies in electronic conferencing. *Computer Assisted Language Learning, 15,* 147–165.

Bos, N., Olson, J., Gergle, D., Olson, G., & Wright, Z. (2002). Effects of four computer-mediated communications channels on trust development. *CHI 2000, ACM Conference on Human Factors and Computing Systems, CHI Letters, 4*(1), 135–140.

Bruckman, A. (1999). The day after net day: Approaches to educational use of the Internet. *Convergence, 5*(1), 24–46.

Bull, S., & McFarlane, M. (2000). Soliciting sex on the Internet: What are the risks for sexually transmitted diseases and HIV? *Sexually Transmitted Diseases, 27,* 545–550.

Butler, B. (2001). Membership size, communication activity, and sustainability: A resource-based model of online social structures. *Information Systems Research, 12,* 346–362.

Categories of Research That May Be Reviewed by the Institutional Review Board (IRB) Through an Expedited Review Procedure, 63 Fed. Reg. 60364–60367 (Nov. 9, 1998)

Children's Online Privacy Protection Act, 13 U.S.C. §§ 1301–1308 (1998).

Cobanoglu, C., Warde, B., & Moreo, P. J. (2001). A comparison of mail, fax and web-based survey methods. *International Journal of Market Research, 43,* 441–452.

Couper, M. P. (2001a). The promises and perils of web surveys. In A. Westlake, W. Sykes, T. Manners, & M. Rigg (Eds.), *The challenge of the Internet* (pp. 35–56). London: Association for Survey Computing.

Couper, M. P. (2001b). Web surveys: A review of issues and approaches. *The Public Opinion Quarterly, 64,* 464–494.

Couper, M. P., Traugott, M. W., & Lamias, M. J. (2001). Web survey design and administration. *The Public Opinion Quarterly, 65,* 230–253.

Cramton, C. (2002). Attribution in distributed work groups. In P. Hinds & S. Kiesler (Eds.), *Distributed work* (pp. 191–212). Cambridge, MA: MIT Press.

Crawford, S. (2002). Evaluation of Web survey data collection systems. *Field Methods, 14,* 226–240.

Cummings, J. N., Sproull, L., & Kiesler, S. B. (2002). Beyond hearing: Where the real-world and online support meet. *Group Dynamics, 6,* 78–88.

Electronic Communications Privacy Act, 18 U.S.C. § 2511 (1986).

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on Internet communities. *British Medical Journal, 323,* 103–105.

Fricker, R. D., & Schonlau, M. (2002). Advantages and disadvantages of Internet research surveys: Evidence from the literature. *Field Methods, 14,* 347–365.

Galegher, J., Sproull, L., & Kiesler, S. (1998). Legitimacy, authority, and community in electronic support groups. *Written Communication, 15,* 493–530.

Garfinkel, S., Spafford, G., & Russell, D. (2002). *Web security, privacy and commerce.* Cambridge, MA: O'Reilly & Associates.

Glaser, J., Dixit, J., & Green, D. P. (2002). Studying hate crime with the Internet: What makes racists advocate racial violence? *Journal of Social Issues, 58,* 177–193.

Hardin, G. (1968). The tragedy of the commons. *Science, 162,* 1243–1248.

Herring, S. (1996). Linguistic and critical analysis of computer-mediated communication: Some ethical and scholarly considerations. *The Information Society, 12,* 153–168.

Hinds, P., & Kiesler, S. (Eds.). (2002). *Distributed work.* Cambridge, MA: MIT Press.

Huston, A. C., Donnerstein, E., Fairchild, H. H., Feshbach, N. D., Katz, P. A., Murray, J. P., et al. (1992). *Big world, small screen: The role of television in American society.* Lincoln: University of Nebraska Press.

King, S. (1996). Researching Internet communities: Proposed ethical guidelines for the reporting of results. *The Information Society, 12,* 119–127.

Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukhopadhyay, T., & Scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological well-being? *American Psychologist, 53,* 1017–1031.

Kraut, R. E., Rice, R. E., Cool, C., & Fish, R. S. (1998). Varieties of social influence: The role of utility and norms in the success of a new communication medium. *Organization Science, 9,* 437–453.

MacWhinney, B. (2000). *The CHILDES project: Tools for analyzing talk. Vol. 1: Transcription format and programs* (3rd ed.). Mahwah, NJ: Erlbaum.

McKenna, K. Y. A., & Bargh, J. A. (1998). Coming out in the age of the Internet: Identity "demarginalization" through virtual group participation. *Journal of Personality and Social Psychology, 75,* 681–694.

McKenna, K. Y. A., Green, A. S., & Gleason, M. E. J. (2002). Relationship formation on the Internet: What's the big attraction? *Journal of Social Issues, 58,* 9–31.

Milgram, S. (1963). Behavioral study of obedience. *Journal of Abnormal and Social Psychology, 67,* 371–378.

Montgomery, A. L. (2001). Applying quantitative marketing techniques to the Internet. *Interfaces, 31,* 90–108.

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979, April 18). *Belmont report: Ethical principles and guidelines for the protection of human subjects of research.* Retrieved, November 2, 2003, from http://ohsr.od.nih.gov/mpa/belmont.php3

Nonnecke, B., & Preece, J. (2000). Lurker demographics: Counting the silent. *CHI 2000, ACM Conference on Human Factors in Computing Systems, CHI Letters, 4*(1), 73–80.

Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002a). E-research: Ethics, security, design, and control in psychological research on the Internet. *Journal of Social Issues, 58,* 161–176.

Nosek, B. A., Banaji, M., & Greenwald, A. G. (2002b). Harvesting implicit group attitudes and beliefs from a demonstration web site. *Group Dynamics, 6,* 101–115.

Olson, G. M., & Olson, J. S. (2000). Distance matters. *Human-Computer Interaction, 15,* 139–178.

Olson, M. (1971). *The logic of collective action: Public goods and the theory of groups.* Cambridge, MA: Harvard University Press.

Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organizational Science, 11,* 404–428.

Robinson, J. P., Neustadtl, A., & Kestenbaum, M. (2002, May). *Why public opinion polls are inherently biased: Public opinion differences among Internet users and non-users.* Paper presented at the annual meeting of the American Association for Public Opinion Research, St. Petersburg Beach, FL.

Rocco, E. (Ed.). (1998). *Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact.* Los Angeles: ACM Press.

Rubin, D. B. (1987). *Multiple imputation for nonresponse in surveys.* New York: Wiley.

Singer, E. (1978). Informed consent: Consequences for response rate and response quality in social surveys. *American Sociological Review, 43,* 144–162.

Singer, E., Hippler, H., & Schwarz, N. (1992). Confidentiality assurances in surveys: Reassurance or threat? *International Journal of Public Opinion Research, 4,* 256–268.

Smith, T. W. (2002, May). *An experimental comparison of knowledge networks and the GSS.* Paper presented at the annual conference of the American Association for Public Opinion Research, St. Petersburg Beach, FL.

Sproull, L., & Faraj, S. (1995). Atheism, sex, and databases: The net as a social technology. In B. Kahin & J. Keller (Eds.), *Public access to the Internet* (pp. 62–81). Cambridge, MA: MIT Press.

Sproull, L., & Kiesler, S. (1991). *Connections: New ways of working in the networked organization.* Cambridge, MA: MIT Press.

Tourangeau, R., Couper, M. P., & Steiger, D. M. (2003). Humanizing self-administered surveys: Experiments on social presence in Web and IVR surveys. *Computers in Human Behavior, 19,* 1–24.

Trice, A. D. (1987). Informed consent: VIII. Biasing of sensitive self-report data by both consent and information. *Journal of Social Behavior and Personality, 2,* 369–374.

Turkle, S. (1997). *Life on the screen.* New York: Touchstone Books.

U.S. Department of Commerce. (2002). *A nation online: How Americans are expanding their use of the Internet.* Washington, DC: U.S. Government Printing Office.
Walther, J. B., & Parks, M. R. (2002). Cues filtered out, cues filtered in: Computer-mediated communication and relationships. In I. M. L. Knapp & J. A. Daly (Eds.), *Handbook of interpersonal communication* (3rd ed., pp. 529–563). Thousand Oaks, CA: Sage.
Webb, E. J., Campbell, D. T., & Swartz, R. D. (1999). *Unobtrusive measures.* Newbury Park, CA: Sage.
Williams, K. D., Cheung, C. K. T., & Choi, W. (2000). Cyberostracism: Effects of being ignored over the Internet. *Journal of Personality and Social Psychology, 79,* 748–762.
Williams, K. D., Govan, C. L., Croker, V., Tynan, D., Cruickshank, M., & Lam, A. (2002). Investigations into differences between social- and cyberostracism. *Group Dynamics, 6,* 65–77.
Yee, N. (2003, September 5). *The Norrathian Scrolls: A study of EverQuest.* Retrieved December 19, 2003, from http://www.nickyee.com/eqt/home.html