

Psychological Research Online: Opportunities and Challenges

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

Abstract

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 rapidly changing nature of technology, norms, and online behavior means that the risks and safeguards against them will differ from those characterizing traditional research and will themselves change over time. This paper 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 the challenges.

Send comments and editorial correspondence to:

Robert Kraut
HCI Institute
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh PA 15213
robert.kraut@cmu.edu
412 268-7694

Psychological Research Online: Opportunities and Challenges

*Robert Kraut, Judith Olson, Mahzarin Banaji,
Amy Bruckman, Jeffrey Cohen, Mick Couper,*

The Internet as a research vehicle presents both opportunities and challenges for psychological research. In 1985, only 8.2% of US households had a personal computer, and the Internet as we now know it, with its rich array of communication, information, entertainment, and commercial services, did not exist. Since then, this exotic technology has become domesticated and is now used by the majority of Americans for personal and economic reasons (Cummings & Kraut, 2002). By September of 2001, 66% of the US population used a computer at home, work, or school, and the vast majority of these, 56% of the US population, also used the Internet (U. S. Department of Commerce, 2002).

The Internet and the widespread diffusion of personal computing have the potential for unparalleled impact on the conduct of psychological research. For example, the Internet has changed the way scientists collaborate, by increasing the ease with which they can work with geographically distant partners (Walsh & Maloney, 2002) or share information (e.g., <http://www.socialpsychology.org/>). In this article we will focus on the way the Internet is changing the process of empirical research.

The Internet presents empirical researchers with opportunities. It lowers many of the costs associated with collecting data on human behavior, can host online experiments and surveys, allows observers to watch online behavior, and offers the mining of archival data sources. For example, online experiments can collect data from thousands of participants with minimal intervention on the part of experimenters (B. A. Nosek, M. Banaji, & A. G. Greenwald, 2002a). Internet chat rooms and bulletin boards provide a rich sample of human behavior that can be mined for studies of communication (Nardi & Whittaker, 2001), 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, 1995), distributed collaboration (Hinds, 2002), and identity-switching (Turkle, 1997), which are interesting in their own right and have the potential to challenge traditional theories of human behavior.

At the same time, the Internet raises substantial challenges in terms of quality of data and the treatment of research participants. For example, researchers often lose control over the context in which data are procured when subjects participate in experiments online. Insuring informed consent, explaining instructions, and conducting effective debriefings may be more difficult than in the traditional laboratory experiment. Observations in chat rooms and bulletin boards raise difficult questions about risks to participants, including privacy and lack of informed consent. This article will discuss both the advantages of this new mode for psychological research as well as the challenges that it poses to data quality and the protection of research participants.

After discussing the opportunities and challenges of conducting online research, we close with recommendations in light of these challenges, directed toward both the researcher and the Institutional Review Boards that oversee the protection of human research subjects. We focus our attention primarily on online experiments, surveys, and observation of naturally occurring online behavior, because these are the major types of research conducted currently by psychologists who use the Internet. Furthermore, these methods have obvious parallels in the off-line (non-Internet) world that can be used as yardsticks by which to compare the online methods.

Opportunities of Internet research

The Internet can have 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.

Making empirical research easier

Compared to other modes of collecting data, the Internet can make observational research, self-report surveys, and random-assignment experiments easier to conduct. This ease derives largely from two properties of Internet research: economy and access.

Subject recruitment. Use of the Internet decreases the cost of recruiting large, diverse, or specialized samples of research participants for either surveys or online experiments. Many researchers attract volunteers by posting announcements at relevant web sites and distribution lists. This technique can provide a large a diverse sample at low cost. For example, in four years, Nosek, Banaji, and Greenwald (2002b) collected a data set of over 1.5 million completed responses in tests of implicit attitudes. (See Sidebar 2). A survey on online behavior collected data from 40,000 respondents from many countries (Wellman, Quan Haase, Witte, & Hampton, 2001), simply by putting a link to the survey on a National Geographic website. On a smaller scale, the research reported in Sidebar 4 (Williams, Cheung, & Choi, 2000) conducted a pair of online experiments about ostracism, with over 1,500 participants from over 60 countries. And those conducting usability tests of websites can merely post “try this new page and give us your reactions” on a busy website and get thousands of responses within hours.

One can post a research opportunity at service sites that specialize in advertising the availability of 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, Inc. (<http://www.surveysampling.com>) are available to aid in selecting a sample. Alternately, one can invite participation by sending personalized electronic mail messages to active participants 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 do not need access to introductory psychology classes to recruit research subjects and often do not need grant money to pay them.. The Internet has opened research to those with fewer

resources. 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, published findings about the psychology of playing online multi-player games, based on 19 surveys he directed to players of the Internet game EverQuest between September 2000 and April 2001, collecting over 18,500 responses from approximately 3,300 players. However, a corollary of this open access is that those with minimal training and supervision can conduct and publish research, some of which might be of low quality. Yee's research results, for example, are available on his own website (www.nickyee.com) but have not been published in any peer-reviewed venue. Regardless of the quality of this research, his intense polling of a single population has polluted this data source for researchers who may be more qualified. In this sense, the tragedy of the commons has now threatens psychological research (Hardin, 1968). In another case, an undergraduate, Martin Rimm, published a study in the *Georgetown Law Review* (Rimm, 1995) reporting on the prevalence of pornography, using research methods that have been heavily disputed (Thomas, 1996).

Observing social behavior. The Internet provides scientists interested in social behavior with many archives of communication, from online groups in discussing topics as diverse as medical support, hobbies, popular culture, and technical information (e.g., see the newsgroups archives at <http://groups.google.com/groups> or the collections of email-based distribution lists at <http://tile.net/lists/>). 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).

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 ordinarily difficult to study in controlled settings because of the difficulty of bringing subjects back to the laboratory many times. Research in social psychology on groups larger than three or four are again difficult to study in the laboratory. Studying large groups over time merely compounds these problems. The Internet has provided a new venue for such long-term research on large groups. For example, Baym (1998) was able to explore the way groups develop a sense of community over an extended time period, by examining the use of an electronic mail distribution list about soap operas. Similarly, Butler (2001) was able to study the impact of participation on the attraction and retention of group members, by creating an archive of all messages sent to 206 online groups over a three-month period. Finally, Bos et al. (2002) examined the development of social capital by having groups of up to 24 play a game on the Web, in which individuals exchanged favors at anytime they wished for a month.

In contrast to conducting observational research in face-to-face settings, for example in a classroom or playground, where the researcher's presence may contaminate the phenomenon under study, researchers can be less obtrusive when conducting observation online. Conducting research online, Bruckman (1999) was able to study the influence of groups on long-term learning, by tracking 475 children learning a programming language

over a five-year period. Furthermore, because the participants in online groups type in their own comments and dialogue, the researcher no longer needs to transcribe the data. The researcher can use simple programs to perform content analyses, examining, for example, differences in different age groups or the ways boys and girls use the tools they are given (Bruckman, 1999).

Access to other archival data. The records of individual behavior on the Internet can provide a source of detailed, unobtrusive data for other phenomena besides social behavior (Webb, Campbell, & Swartz, 1999). The detailed transaction logs that people leave when using the Internet for a wide variety of activities provide a wealth of potential data for study. These include browsing behavior, application use, purchasing behavior, file uploads and downloads, subscription to communication forums, email sending, and a host of other digital transactions. For example, both academics and market researchers have used the Internet as a source of data about individual preference and choice (Montgomery, 2001). Others have used the history of uploads and downloads of music files to document the extent of social loafing and the rarity of altruistic behavior online (Adar & Huberman, 2000). These records include information about sequences of behavior, not only their quantity. Because most online transactions have detailed time stamps, one can analyze sequences of behavior, observing how events early in a sequence influence those occurring later. For example, Hoffman, Novak, and Duhachek (2002) used the time sequence of online behavior to model the concept of psychological flow (Csikszentmihalyi & Csikszentmihalyi, 1988), and Kraut and his colleagues (Kraut, 1999) used records of Internet users' email traffic to document changes in the geographic dispersion of social networks over a two-year period.

Automation and experimental control. One of the benefits of online research is that it allows a degree of 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 participant. Unlike traditional laboratory experiments or telephone surveys, where each new participant must be encountered, instructed and supervised by a person, most online experiments and surveys are automated with a low marginal cost: a human experimenter does not need to give instructions, introduce the experimental manipulation, and or collect the data. Cobanoglu, Warde, and Moreo (2001) estimate that marginal, unit costs for postal mail survey are \$1.93, compared to a marginal cost of close to zero for a Web-based survey, although fixed costs for the Web are higher. The differentials are much higher for interviewer-administered surveys (telephone or face to face), as one is paying for interviewers' time for every contact attempt and completed interview. Practitioners estimate that the per-completed interview costs for telephone surveys range from \$40 to well over \$100.

Consider how Web surveys are changing the nature and economics of questionnaire-based research. With conventional, paper-based questionnaires, transcription of survey answers is an expensive and potentially error-prone process. The questionnaires themselves are relatively inflexible, either forcing a common sequence of questions for all respondents or requiring confusing instructions for skipping blocks of questions (Dillman, 2000). Survey organizations have long used computer-assisted interviewing

(CAI) for both in-person or telephone interviewing to overcome these problems (Couper & Nicholls, 1998). Interviewers enter data as they ask questions, and the software can customize the next question based on prior answers and other considerations. Internet surveys provide similar advantages to CAI systems, while eliminating the interviewer. Many software packages now exist that can create complex online questionnaires, where the data are written directly to a database. (See Crawford, 2002 for a review. <http://www.asc.org.uk/> maintains a list of software for online surveys).

Using these techniques, the researcher has greater control over the data-collection setting compared with executing a mailed survey. The researcher, for example, can constrain response alternatives with menus or dialog boxes and conduct checks as the questionnaire is being completed to identify missing or inconsistent data. By requiring respondents to submit their surveys incrementally, the researcher can obtain partial data even from those who fail to complete an entire questionnaire. This helps the researcher obtain a measure of biases in the sample and systematic differences between those who complete the survey and those who drop out.

Automation also means that the assignment of subjects to experimental conditions within a questionnaire is a trivial exercise. The assignment can be based on subject characteristics or on responses to earlier items. The possibility of control and the potential size of the subject sample allow researchers to conduct large and complex experiments within a single study (See Sidebar 1). User metrics such as response latencies, changed answers, backing up, or other behaviors can be captured, permitting richer analysis of the process of the experiment and variations in its execution across subjects. The Implicit Attitude Test, described in Sidebar 2, uses reaction times to measure attitudes more subtly than traditional verbal attitude measures.

Examining new social phenomena

Up to this point, we have emphasized some of the opportunities of using the Internet as a research modality to increase the efficiency of studying traditional psychological phenomena. The Internet is also an important phenomenon in its own right. Like the telephone, television, and automobile before it, personal computers and the Internet are new technologies being adopted by a majority of Americans, with the potential to change the way they live their lives. Just as psychologists have long been interested in the way that television influences child development, prejudice, and violent behavior (Huston et al., 1992), so too psychologists are now examining the impact of the Internet (e.g., R. Kraut et al., 1998; McKenna & Bargh, 2002; Wellman & Haythornthwaite, 2003).

The Internet is used extensively for interpersonal communication. Starting with landmark research by Hiltz and Turoff (1978) and by Sproull & Kiesler (1991), psychologists have examined how computer-mediated communication differs from other communication modes in influencing social interaction. More recently, psychologists have been especially interested in the longer-term impact of computer-mediated communication. They examine how time spent on email and in chat rooms contrasts with other Internet applications and its impact on social involvement and its psychological consequences (e.g., Kraut et al., 2002; McKenna, 1998).

The Internet is also the location for psychological and social phenomena that, if not entirely new, are rare in other settings. For example, although distributed work has existed for centuries (O'Leary, Orlikowski, & Yates, 2002), highly interdependent workgroups whose members are geographically distributed are a relatively recent phenomenon, made possible by improvement in computing and telecommunications, including the Internet. These new forms of working have caused researchers to re-examine how shared context and trust, often taken for granted in face-to-face settings, have their influence on group performance (e.g., Olson & Olson, 2000; Rocco., 1998). The challenge of designing ways to improve coordination and communication forces us to rethink taken-for-granted conceptions of the world. For example, researchers are now deconstructing the concept of face-to-face interaction, to understand how its individual components can influence communication (e.g., Kraut, Fussell, Brennan, & Siegel, 2002). Others have examined the nature of commitment to very large groups (e.g., Moon & Sproull, 2000). Yet others have examined how the Internet allows individuals to assume and play with alternate personal identities, which may differ from their real-world persona in gender, age, or other normally static properties (e.g., Turkle, 1997).

Challenges of Internet research: Data quality

The preceding section highlighted the ways in which online research can reduce the cost of psychological research on traditional topics and open up new phenomena to the psychologist's lens. However, these opportunities sometimes entail risks to both the quality of the research itself and to the human subjects who participate in it. In this section we discuss concerns about data quality associated with conducting research online.

Sample biases

Although the majority of Americans now have access to the Internet, they are by no means representative of the nation as a whole. While the large differences between Internet users and non-users in terms of gender, income, and age that existed in the 1990s have shrunk, people with and without computers still differ on many demographic and social dimensions. For example, Internet users are more likely to be white, to be young, and to have children than the nation as a whole (U. S. Department of Commerce, 2002). There is some evidence that they differ in psychological characteristics as well; users, for example, are both more stressed and extroverted than non-users (Kraut et al., 2002).

There is currently no sampling frame that provides an approximate random sample of Internet users, unlike the case of random digit dialing of telephone numbers, which provides an approximate sample of the U.S. population. The problem of representativeness is compounded because many online surveys and experiments rely on opportunity samples of volunteers. As a result, it is not clear exactly how to go about the task of appropriate generalization. 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 participants, these self-selected samples are problematic (Couper, 2001; Robinson, Neustadtl, & Kestnbaum, 2002; Smith, 2002).

Even if a sampling frame of all Internet users could be constructed, or in specialized populations where such frames exist (students at selected colleges, subscribers to an online service, registrations at a website, etc.), problems of non-response may threaten the generalizability of the findings. 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, 2001; Fricker & Schonlau, 2002). The problem of biased sample selection for surveys is especially problematic for longitudinal or panel designs. It is more difficult to maintain contact with respondents in online surveys than in telephone or mail surveys because email address change much more frequently than phone numbers or postal addresses.

Control over the data-collection setting

Previously, we noted that conducting research online *enhances* control for random assignment of participants to conditions and for the selection and ordering of questions in a questionnaire. On the other hand, the researcher typically has less control over the environment in which the research is conducted than in other experimental settings.

As Nosek, Banaji and Greenwald (2002) note, in the laboratory, the experimenter stage-manages the physical environment, controlling to a degree the participant's visual, auditory, and social stimuli. Moreover, in the laboratory, an experimenter can verify some of the identities that participants claim, can tailor instructions to ensure that each participant understands them, can monitor participants' behavior to ensure that they are involved and serious, can make appropriate decisions about retaining or removing participants once a study has commenced, can assess the effect of the research experience on them, and can intervene if the researcher perceives undesirable effects. While an experimenter may not perform many of these actions in any particular laboratory experiment, they represent options when designing and executing the research. When the researcher decides to conduct an experiment online, many of these actions are not possible or are more difficult to put into effect.

The anonymous nature of the Internet may encourage some people to participate for the express purpose of damaging data. This could involve multiple submissions by the same individual, widespread dissemination of the URL for the purposes of flooding the site, and other nefarious behaviors designed to undermine the integrity of the research. There are some technical protections for this, such as the use of cookies or tracking IP addresses to guard against multiple responses, if the survey or experiment is an open one. Nevertheless, these solutions are not perfect, especially when computers are shared, as among students in a university computer lab. If the research is by invitation only with respondents given IDs and passwords or individually tailored URLs, one can exert better control over participation.

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, in the experiments described in Sidebar 4 (Williams et al.,

2000; Williams et al., 2002), Williams and his colleagues report substantially higher dropout rates than they have observed conducting similar research in the laboratory. Withdrawal from the experiment undermines the value of random assignment of subjects to an experimental condition. The fact that such behaviors may more readily occur on the Internet is in itself an interesting topic for study, but for many research enterprises, such practices may at best add noise to the data and more likely damage the entire study.

In online communities that are the subject of naturalistic observation, anonymity also can have an effect. When people are not identified, they feel less accountable for their actions and are more likely to engage in deviant behavior (Sproull & Kiesler, 1991). While this is an interesting phenomenon in itself, it has the potential to generate misleading generalizations about behavior off-line from the behavior observed online.

Challenges of Internet research: Protection of human subjects

Conducting research online raises challenges in protecting human subjects as well as in protecting the quality of the data. We believe that online research is not inherently more risky than comparable research conducted through other venues, but that conducting research online may change the nature of the risk and the investigators' ability to assess it. Some of the challenges arise because fundamental concepts for assessing informed consent and risk, such as the nature of individual identifiability or public behavior, become ambiguous when research is conducted online. Other challenges arise because of the researcher's reduced control over the research environment, discussed previously, which makes it more difficult to insure participants' identity or to assess their reactions to the research situation.

The basic ethical principles underlying research involving human subjects are contained in the Belmont Report, prepared by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research in 1979. These include:

- 1) **Respect for Persons:** Individuals should be treated as autonomous agents who can make informed decisions to become or refuse to become participants in research. Potential participants who are not capable of self-determination, because of diminished capacity (e.g., children or the mentally ill), need protection.
- 2) **Beneficence:** Researchers are obligated to secure the well-being of human subjects, maximizing possible benefits from their participation in research and minimizing harm.
- 3) **Justice:** The burdens of being a research participant and the benefits of the research should be fairly distributed.

These principles have been formalized into the Federal Policy for the Protection of Human Subjects (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 voluntary, informed consent before people participate in research and documenting their consent, and for the treatment of minors and other vulnerable populations. It established an oversight process called the Institutional Review Board (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 upon key concepts such as risk, expectations of privacy, pre-existing records, and identifiability, 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 Institutional Review Board needs to consider in determining whether the research needs to gain informed consent from a research participant and whether that consent must be documented. In a later section, we will explicitly discuss obtaining and documenting informed consent online. However, it should be clear from an examination of Figure 1 that assessing whether informed consent is required involves determining whether a research project is classified as human subjects research, whether the project is exempt from the Federal regulations, and whether an IRB can waive the consent requirement or its documentation.

Figure 1 about here

Figure 1 lists criteria for making these determinations, which are likely to change when research is conducted online². These criteria include the following:

- 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

¹ Federal regulations are published in the Code of Federal Regulations (CFR). Each of the Federal agencies and departments that have adopted the Common Rule has published it with different CFR numbers (e.g., HHS’s regulations are published as 45 CFR 46). The content is identical for each. In referring to sections of the Common Rule in this document we will use the notation: CR§102(b), where the CR stands for the document (i.e., the Common Rule), and the code following the § stands for a part number and letter subsection.

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

Conducting Internet research increases the ambiguities in assessing each of these criteria. We expand on these ambiguities in following sections, illustrating them with the case of online communication forums, like chatrooms and listservs.

In addition, when conducting research online, researchers need to contend with changes in the technology, the ways the technology is typically used, and the norms surrounding this use, because this context is integral to assessing anonymity, privacy, risk and the like. For example, the concept of minimal risk depends upon a comparison of the risk associated with research participation to risk in everyday life. The concept of privacy depends upon participants' reasonable expectations about whether others will be allowed access to information about them. As online behavior and norms change, the nature of minimal risk and the very concept of privacy themselves change.

Identifiable versus anonymous information

Determining whether an individual is identifiable or anonymous has implications for the risks participants are exposed to, whether the research is exempt from Federal human-subjects regulations, and whether the research even involves human subjects at all. 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. However, in observations of naturally occurring online behavior, the very nature of anonymity versus identifiability is ambiguous.

Consider the question of whether a researcher can quote dialog from an online conversation, identifying excerpts by the pseudonyms by which participants identify themselves. Many participants in a chat room use a pseudonym (e.g., IAmCute or FloridaSnowbird2000) to simultaneously mask and express their identities. As such, the choice of a pseudonym itself represents data of which the scientific audience may need to be aware (See Bassett & O'Riordan, in press for a fuller discussion). The use of pseudonyms does not guarantee anonymity and may not prevent participants from being identified. Internet users may choose online pseudonyms that contain part or all of their real names. Additionally, in the online conversation, participants often disclose information that publicly links their pseudonym to their real identities (Frankel & Siang, 1999). In some cases, where an unusual name or rare demographic category (e.g., a female professor over 50 in information systems at the University of Michigan Business School) exists, small amounts of information can lead to identification of the respondent. In email-based discussion forums, known as list servers, participants' identifiers invariably include their electronic mail addresses, making it easy to trace and contact them. Moreover, many Internet users employ the same pseudonym for an extended period of time and at multiple Internet sites. Consequently, they care about the reputation of that pseudonym. Thus disclosing information from a purportedly "anonymous" pseudonym in many cases has the potential to identify and to harm its owner.

Public versus private behavior

Some have argued that scientists can record Internet-based communication without the knowledge or consent of participants, because this constitutes unobtrusive observation of unidentifiable people in public places (Herring, 1996). According to the federal regulations [CR§102(f)], research involves human subjects only if data is collected through interaction with a subject or if it collects “identifiable private information”. The regulation bases its definition of “private information” on the “reasonable expectation” of privacy. Expectations about privacy are likely to be shaped by a number of features of online settings. In Yahoo Groups (<http://groups.yahoo.com/>), for example, participants’ expectations of privacy are likely to be influenced by whether archives of their conversations are open to the public or only to available only to members, even though researchers can easily become members with access to the archives. In other case, the presence of explicit policies posted on websites or online discussions are likely to influence expectations of privacy. For example, one text-based virtual reality environment announced at its login screen:

“NOTICE FOR JOURNALISTS AND RESEARCHERS: The citizens of LambdaMOO request that you ask for permission from all direct participants before quoting any material collected here.”
(<telnet://lambda.moo.mud.org:8888>)

People are also likely to have higher expectations of privacy if the discussion is among a small, stable group rather than a large one with substantial turnover in membership. In general, in an online setting, participants may often have expectations of privacy because they cannot see the “eavesdroppers.” In a face-to-face setting like a cafe, the presence of an idle stranger (who happens to be an anthropologist with a hidden tape recorder) is likely to be noticed, and people may adjust their behavior accordingly. In a chatroom, however, a lurker, that is, a person who reads messages, but doesn’t contribute them, is much more likely to go unnoticed.

According to Waskul and Douglass, “the blurring of public and private experience is particularly characteristic of on-line research” (Waskul & Douglass, 1996). Whether a person conversing online can reasonably expect the communication to be private depends upon legal regulation, social norms, and specific details of implementation, all of which are changing. Researchers and IRBs need to explicitly decide whether communication among individuals on an electronic mail distribution list, such as the soap-opera distribution list studied by Baym (1993), or an Internet chatroom, such as the sexually-oriented ones studied by Bull and McFarlane (2000), is public behavior. In these settings, people disclose opinions and facts that they would likely not disclose in a physical public location. Their perceptions and expectations are often that the encounter includes only other participants in the chat room who are simultaneously present.

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

between individuals are considered protected communication. However, this 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.” It is also not illegal in the case that “the electronic communication system . . . is configured so that such electronic communication is readily accessible to the general public.” (18 USC § 2511(2)(g)(I))

Whether behavior should be considered public or private also depends upon changing features of technology. For example, many websites often automatically create logs showing the Internet Protocol (IP) address of the machines that someone used to 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 know the identify of its users. However, IP addresses did not translate into individual identifiers in the earlier minicomputer era, when many people had accounts on a single computer, or now, if the system uses dynamic IP addresses in which one of a fixed number of addresses is assigned to a machine on the fly. In the case of dynamic IP addresses, tracing the address only identifies the machine pool, not the actual machine or its user.

Ambiguities in defining “existing public” records

According to federal regulation, research is exempt from IRB regulations if it consists of the collection of existing and publicly available data, documents, and records CR§46.101(b)(4). Existing public records include newspaper articles, letters to the editor, birth announcements, public voter lists, and telephone books. The rules concerning the use of such data were constructed, however, in the world prior to the existence of the Internet. Now, the distinctions are often fuzzy both about (a) whether something can be said to “exist” prior to the study or (b) whether the record is indeed “public.” For example, when individuals interact, browse and buy online, their behavior often leave traces (i.e., records that are amenable to study by researchers). Yet, at times, there is ambiguity about the status of these traces as pre-existing records. Market research firms, such as Doubleclick (<http://www.doubleclick.com/>), have created technology that compiles a history of a single machine’s traversal of cooperating Internet sites, selling this information to its subscribers and using it to place targeted advertisements. One might argue that the widespread use of such technologies, often revealed in a website’s privacy policy, makes these transaction logs public records, even though many Internet users are unaware of them and consider their Web behavior private.

The issue continues to be complicated even when research participants voluntarily publish information online and know, in a sense, that the information is a public record. For example, many people post family pictures online, intending them for their family and friends. A recent college graduate created a personal web page with her resume, pictures of her sorority sisters and members of her families. When asked who she thought was looking at this website, she replied, “Well, see I don’t think anybody would look at it unless I told them it was there. So I kind of view it, I guess, as the same thing as like if you, if someone came over to your house. . . . You might show them your photo albums of your family, your friends, or your cat, or whatever.” Technically, these photos and her

resume, including her name and address, were a matter of public record, and the poster should have realized this. In the interview just described, however, the poster considered the records private, like a photo album in one's living room. For researchers who comb the Internet for scientifically relevant data, it is not clear whether the use of such data is ethical. It is an enduring record, but in the expectation of the person who posted it, the record may be private. It may be that in the future, better education about the scope and access of information available on the Internet will align the assumptions of various parties more closely with each other.

Risk to Subjects from Internet Research

Both general ethical principles and federal regulation require that the risks to subjects from participating in research should be minimized. When the Belmont Report was first developed, after the disclosure of the Tuskegee syphilis experiments (Center for Disease Control), the major concern was for the risks of physical injury or death associated with medical studies. Risks, however, also include social, psychological, economic, and legal outcomes, which are more typical of behavioral research.

Evaluation of risk must weigh both the magnitude and the probability of harm to the subjects against the value of the research outcome to the individual and society. Research that results in unreliable or invalid data can have no benefit and, as such, is not worth any risk it may pose to participants. As indicated in Figure 1, researchers have a different set of options available to them when conducting minimal risk research as opposed to research with greater risk. For example, when conducting minimal risk research, they can request the waiver of informed consent or its documentation, and IRBs can conduct expedited reviews when evaluating such research. 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..." (CR§102.(i)).

Internet research involves two potential sources of risk:

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

The nature of the potential risks varies with the particular research method used (observation, experiments, surveys, etc.) and the particular implementation decisions made within a choice of method. For example, it is easier to anonymize data in quantitative surveys and experiments than in observations of online conversations, where participants may reveal information about themselves. The risk to subjects if they leave a research setting before receiving debriefing information is greater for deception studies (because of lack of informed consent) than in many online communication forums or surveys. We examine the risks associated with various research genres in more detail below.

Harm as a consequence of participation in online research

Much online research involves minimal risk. It exposes participants to innocuous questions and benign or transient experiences with little lasting impact. In general, online research is no more risky than any offline surveys, experiments, or observations. In some respects, it may be less risky, because the reduced social pressure (Sproull & Kiesler, 1991) in online surveys or experiments compared to their face-to-face counterparts makes it easier for participants 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).

Although risk in online settings is typically low, the actual risk depends upon the specifics of the study. For example, some questions in a survey or feedback from an experiment may cause participants to reflect on unpleasant experiences or to learn something unpleasant about themselves. Banaji, Greenwald, and Nosek's research on implicit attitudes, for instance, provides some participants with feedback that they may have prejudices of which they were unaware (See Sidebar 2). Similarly, participating in a survey may make a respondent confront unpleasant or disturbing issues (e.g., suicide, feelings of loss, cancer symptoms, etc.), which can lead to distress. 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 participants. For example, Williams' research on ostracism deliberately exposed participants to situations in which they were socially excluded (See Sidebar 4). Theory predicted and the data confirmed the negative effects of exclusion. A cost/benefit analysis of the gains to knowledge and the human condition generally versus the costs to the individual participants are no different here than in medical research or in traditional psychological research.

Although not explicitly covered in the common rule, research participants may be harmed if the welfare of the online groups in which they participate is damaged by the research. Consider the case of online social-support groups, such as Breast Cancer Support (<http://bcsupport.org/>), where people who confront a common problem share information, empathy and advice. Research may damage communication and community in those forums. King (1996) quotes 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. I certainly don't feel at this point that it is a "safe" environment, as a support group is supposed to be, and I will not open myself up to be dissected by students or scientists. I'm sure I'm not the only person who feels this way" (See Eysenbach & Till, 2001 for similar concerns). When conducting cost-benefit analysis for research, investigator and IRB alike must anticipate these subtle consequences of their decisions.

Debriefing

APA ethical guidelines (American Psychological Association, 2002) call for debriefing participants—providing an explanation of the nature, results, and conclusions

of the research, delivered 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 participant, they are to take reasonable steps to ameliorate the harm.

In addition, since many psychology experiments, including those conducted online, recruit subjects from psychology classes, they have an obligation to make the experience educational. Even when subjects are not students, educating participants should be considered a public good. Debriefing is a way to give something back to the public, affirming the Belmont Report's principle of justice.

Studies online have the advantage that researchers can post debriefing materials at a website, and can automatically update these material as new data and results come in. By providing participants with a code, debriefing materials can be tailored to particular experimental conditions and be made personally relevant.

As suggested earlier, however, debriefing in online research may be difficult. The absence of a researcher in the online setting makes it difficult to assess a participant's state, and therefore to determine whether an individual has been upset by a experimental procedure or understands feedback received. In contrast to a face-to-face setting, the online researcher is less likely to know if intervention is needed, how to adjust messages for a particular recipient, or how to fix problems caused by the research experience. In addition, participants in online research may leave the setting before receiving debriefing. Although it is hard to debrief a participant who leaves the session early, Nosek, Banaji and Greenwald (2002) have suggested some solutions:

- Subjects enter an email address before the study begins, so that at the end of the study debriefing material is emailed to them (although this undercuts the anonymity afforded by online research).
- A "leave the study" button, available at all times, brings up a debriefing statement when selected.
- When the subject closes the window, a new window appears with the debriefing statement, much as various advertisements appear after a window is closed in some websites.

Breach of confidentiality

Probably the greater risk of harm in online research comes not from the experience of participating, but from possible disclosure of personal information at a later time. Researchers must ensure adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data. The identifying information can include names, email addresses, partially disguised pseudonyms, or other distinguishing personal information.

Identifying information may be inadvertently disclosed either as the data is being collected, or, more commonly, when it is stored on a networked computer connected to the public Internet. Data in transit is vulnerable, for example, if a participant or automated process sends data to the investigator by electronic mail. The store-and-forward nature of electronic 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 email addresses. These risks can be avoided by not transmitting information that will permit identification or by separating this data from other research data. Although analogous risks can occur with paper forms, they are higher when data is shipped over the Internet, because of the openness of the networks and the possibility of automated pattern detection.

Greater risks result from outsiders gaining access to stored data files, either through deliberate hacking or because the investigator mistakenly distributed them. This risk is not unique to online research but is a challenge for all data stored on networked computers. Researchers should regularly check the permissions associated with computer directories. Directories can be password protected, and sensitive files can be encrypted. However, many investigators fail to take these precautions to protect their data.

The standard approach to dealing with problems of confidentiality is to separate personal identifiers from other data describing participants. Thus, one often keeps names and addresses in one file and data in a second, with an arbitrary code number to link the two files. Tourangeau, Couper and Steiger (In press, See Sdebar 2) illustrate some techniques used to maintain separation of identity from data in survey research involving sensitive data.

A special complication in maintaining a participant’s anonymity arises when an investigator conducting online research must match different pieces of information from the same respondent. For example, the HTML protocol, in which most Web surveys are authored, is stateless, meaning that it does not keep history from one page view to another. If an investigator separates questions from a survey into multiple pages, the HTML protocol does not automatically link the responses from a single respondent. To link the questionnaire, programmers sometimes use cookies, small text files stored on a respondent’s computer. There are a variety of other ways to keep track of a respondent’s answers across several Web pages, such as session cookies, which are stored in memory, hidden values embedded in the HTML, or environment variables such as IP address. As long as these techniques use an arbitrary code to link the questionnaire sections, they may pose fewer confidentiality threats than the use of cookies.

Paying online subjects for their participation may also link participants’ responses to their identities. 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, participants can redeem their certificates without revealing their identity.

The degree of concern over confidentiality should be directly related to the sensitivity of the data being collected. One should be less concerned when the information about the participants is innocuous (i.e., its revelation would bring no harm or embarrassment to participants) or if participants are anonymous (the participant cannot be identifiably linked to the information provided). Many online surveys and experiments fall into one or both of these categories. However, when participants are identifiable and the research involves data that places 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 e-commerce transactions, such as encryption and secure socket layer (SSL) protocols, are likely to be sufficient. Numerous tutorials exist describing the options (e.g., Garfinkel, Spafford, & Russell, 2002). The level of security (and the information conveyed to the respondent in that regard) should be appropriate to the risk. As research by Singer, Hippler and Schwarz (1992) demonstrates, overly elaborate assurances of confidentiality may actually heighten rather than diminish respondents' concern, causing participants to be less willing to provide sensitive information. In addition, using SSL potentially adds burden to the respondent, depending on their server settings and degree of interactivity required of the task. Some subjects may be excluded from participating because of the complexity required in interacting with the high level of encryption required.

Informed consent

Investigators must typically obtain voluntary informed consent from research participants, in which they freely agree to participate after they understand what the research involves and its risks and benefits [CR§116]. As indicated earlier, investigators conducting online research may have difficulties in establishing whether participants are truly informed or even whether they are who they purport to be. Children and other vulnerable groups such as the mentally handicapped 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 participants' identity is especially problematic, because it is so easy for children to pretend to be their parents. These problems necessarily raise the possibility that the consent will not be valid. Depending on the risk involved in the research, the researcher may either accept the possibility of uninformed consent or insist that a legally verified signature accompany the consent form. Getting informed consent online may not be suitable for high-risk studies.

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 (COPPA) (see <http://www.ftc.gov/ogc/coppa1.htm>). Among other constraints, this regulation applies particularly to operators of a website directed towards children or those who know they are collecting information from children. We believe that these restrictions apply to research projects designed to collect information from children. They 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.

Researchers can increase the likelihood that participants are granting truly informed consent or that they are who they purport to be. For example, it is possible to get better feedback from participants about whether they understand the consent statement by breaking a consent form into segments and requiring a 'click to accept' before continuing, or by administering short quizzes to establish that a participant understood one section before administering the next. Similarly, one can more reliably distinguish children from adults by having participants 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. Many of these techniques have been developed to deal with problems of fraud in electronic commerce applications (e.g., VeriSign's Authentication Service Bureau <http://www.verisign.com/products/asb/>) or for protecting online communications (e.g., Pretty Good Privacy <http://www.pgp.com>). They will be evolving in response to business and security needs.

However, these techniques often come at a cost to the participants. The extra effort is likely to reduce response rates, increase non-response to sensitive items (Singer, 1978) and possibly produce biased data (Trice, 1987). In addition, these techniques may require specialized technologies (e.g., 32-bit encryption) and knowledge, which may exclude some types of subjects from the research (e.g., those who haven't upgraded to the most recent browser or who live outside the United States). Therefore these techniques are appropriate only when there is more than minimal risk to the participant.

Federal human-subjects regulation requires that informed consent be documented by the use of a "...written consent form approved by the IRB and signed by the subject" [CR§117]. It is difficult to obtain legally-binding signatures online. However, Institutional Review Boards (IRBs) can waive the requirements for written documentation of informed consent for minimal risk research [CR§117(c)], and many IRBs permit research participants to click a button on an online form to indicate they have read and understood the consent form.

Table 1 lists methods of obtaining consent for Internet-based studies from strongest to weakest. The weakest method of consent, simple click to accept electronic forms, is most vulnerable to misrepresentation. There is no reliable way to know who is clicking, or whether a child or parent is the one clicking. As digital signatures become more commonly used, there may be new ways to obtain consent with relative ease. The table illustrates the tradeoffs inherent in each of these methods for obtaining consent. In particular, anonymity is often traded off when strong forms of consent are used, especially when documentation is kept.

Table 1 about here

Advice to researchers and institutional review boards

The Internet allows researchers to collect data in new ways and to observe phenomena that might be rare in other settings. Psychologists need to become educated in the possibilities and caveats, so that they can capture advantages of conducting online research while reducing risks to research quality or to human participants. In general, research on the Internet is not inherently more difficult to conduct or inherently riskier to participants than other, more traditional research styles. But because the Internet is a

relatively new medium for research, where online behavior, norms, technology, and research methods are all evolving, conducting online research raises ambiguities that have been long settled in more conventional laboratory and field settings. Until conducting online research becomes routine, it is likely to require more forethought and self-reflection than conventional research in the discipline. The sections below provide some guidance to researchers and the Institutional Review Boards, which monitor their conduct.

Start small

By opening up research populations, through sampling and observation of online groups, and by automating research processes, such as random assignment or survey distribution and collection, the Internet enables researchers to work with larger samples and more complex designs, potentially allowing them to examine more subtle psychological phenomena or higher-order statistical interactions. If one thinks of users of the Internet, the online groups they inhabit, and the conversations and transactions they leave behind as public goods available for researchers to study, then the very economies and ease of access that make the Internet an attractive research medium give rise to a dilemma of the commons (Hardin, 1968; Olson, 1971). Poor online research can potentially contaminate a large number of participants. Low quality academic research conducted online is having some of the same consequences as commercial electronic mail and telemarketing--undermined the ability of legitimate researchers to collect data online. Researchers should restrain themselves and supervise their students, so that they only consume resources appropriate to the importance of their research problem.

People who have run surveys and experiments online also recommend starting with small pilot projects to identify how online data collection methods differ from conventional ones. Nosek, Banaji, and Greenwald (2002), for example, recommend that a pilot project explicitly attempt to replicate a well-known phenomenon in the off-line setting (See Sidebar 2). Once comparability of subject behavior can be established, then new variables can be addressed with greater confidence.

Understand and guard against sources of poor data

One of the earliest considerations has to do with ensuring that the data collection effort is worth the cost and effort. Sampling biases, aberrant subject behavior from being anonymous, and protections against fraudulent data are all issues to be addressed before the study begins. Investigators can reduce fraudulent data by tracking IP addresses, putting cookies on participants' 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.

Use techniques for protecting human subjects commensurate with risks

No purpose is served when researchers or their IRBs place hurdles in front of research involving minimal risk. One should not use over-elaborate informed consent statements, encryption, digital signatures, or extensive assurances of confidentiality when risks are minimal, because these features discourage participation and are likely to harm the

quality of the data collected, but provide little benefit to human subjects. Instead, one can guard against risk with lower keyed approaches. Because experimenters get no feedback from participants, they need to pre-test instructions and informed consent statements so they are clear to the wide-ranging populations from which subjects may come. IRBs should waive documentation of informed consent, by agreeing to a “click to assent” button on websites. For low risk surveys and experiments, debriefing material can be customized to participants’ behavior and delivered as an updated set of Frequently Asked Questions. Because the most likely risk for data collected online is the breach of confidentiality, where research data is disclosed outside of the research context, investigators should use good data management practices to lessen this risk. In particular, stripping identifiers from data, storing identifiers and data in separate files, and auditing the security of data directories should be routine practice for all research involving human subjects.

On the other hand, 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 participant’s state or to respond to evidence of distress when conducting online research, deception experiments and research that exposes participants to stressful events may be problematic if conducted online. Researchers should consider screening respondents, either through sample selection or through preliminary data collection, to eliminate vulnerable populations. The greater freedom of participants to withdraw from online research is a mixed benefit. Compared to laboratory settings, they are more likely to leave before experiencing severe distress, but also before they can be adequately debriefed. To counteract early withdrawal, researcher can arrange their study so that participants 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 a 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. Under some circumstance, researchers might apply for a Certificate of Confidentiality (<http://grants.nih.gov/grants/policy/coc/index.htm>), allowing the investigator and others who have access to research records to refuse to disclose identifying information on research participants in civil, criminal, administrative, legislative, or other government proceedings.

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.

Understand the nature of human subjects risks in online research and possible solutions

The Internet as an environment through which to conduct research is in flux. The ambiguities in defining what is public behavior and in choosing the technologies to obtain informed consent and document it are but two cases in point. As Figure 1 illustrated, even a seemingly simple decision about whether data collection should be considered human subjects research becomes ambiguous when research is conducted online, based as it is on concepts such as identifiability, expectations of observation, and private information. In navigating these issues, researchers and Institutional Review Boards 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 upon conventions established by those who frequent support groups and upon 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” [CR§46.107]. We recommend that all IRB boards have technical consultants, who can be called upon when needed.

Because these issues of protecting data quality and human subjects in online research are new and because they involve recommendations that involve procedural or technical remedies, 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.

Summary

As it is changing interpersonal communication, commerce, and the distribution of information and entertainment, the Internet has the potential to change the conduct of psychological research as well. New psychological phenomena are emerging. Researchers can efficiently expand the scale and scope of research on traditional psychological topics. Yet these opportunities come at some risk both to the quality of research that is produced and to the human subjects of the research. Although these risks are real, they are not insurmountable. Foremost they require researchers and Institutional Review Boards to keep abreast of changes in online behavior, community standards, and available technology. They also require a degree of reflection about the research process that may not be necessary in more established domains.

Figure 1: Some factors relevant to Internet research influencing whether informed consent is required and must be documented.

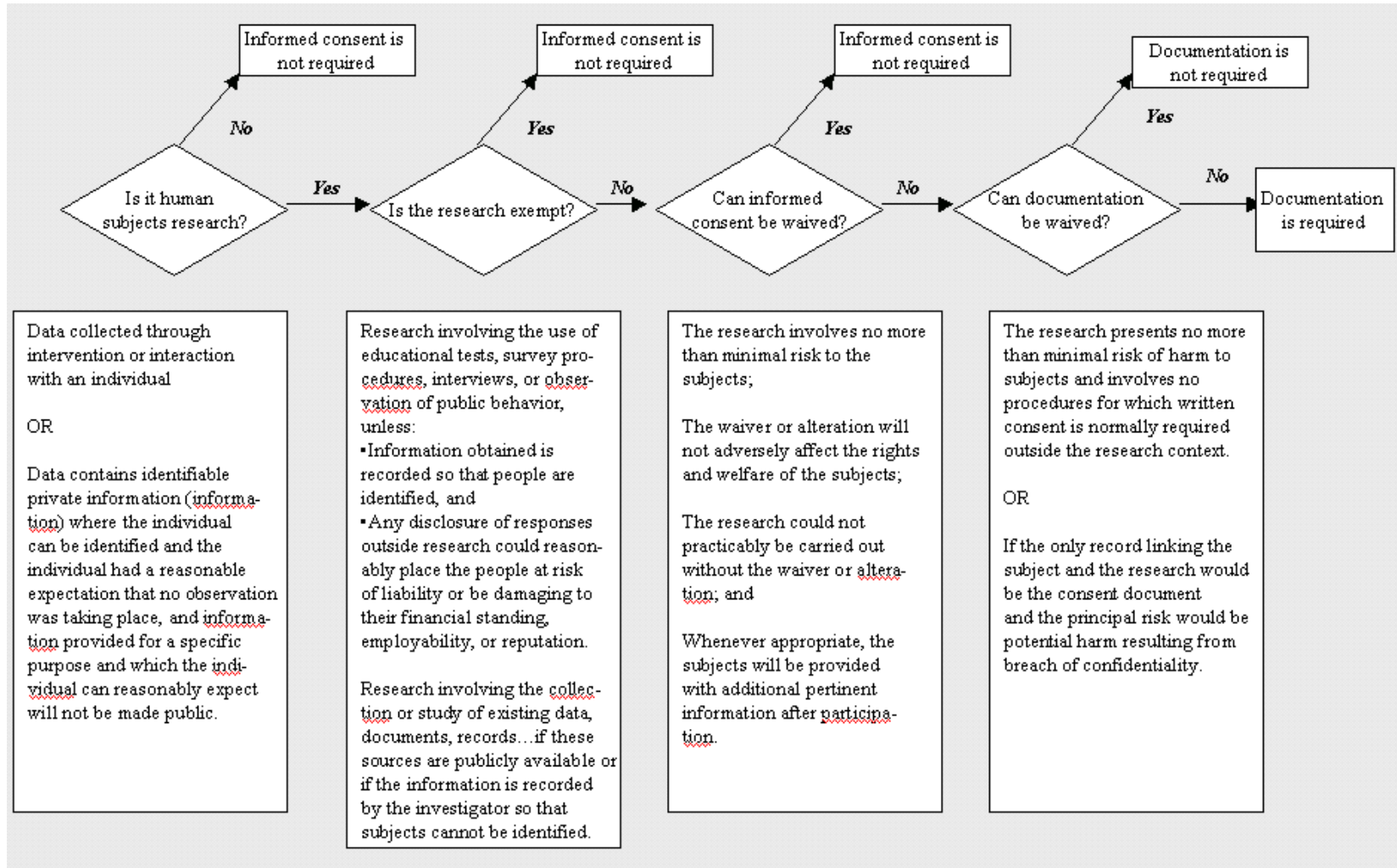


Table 1: How method of interaction influences the ability to protect the research participants.

Method of interaction between investigator and research participant	Research Issue					
	Insuring informed Consent	Documenting Informed Consent	Insuring Debriefing	Protecting Anonymity	Preventing Coercion	Ease and Cost of Interaction
Face-to-face dialog with signed forms	++	++	++	--	--	--
Telephone conversation	++	--	++	-	-	-
Postal mail	--	++	0	++		0
Electronic forms signed by verifiable digital signature.	--	++	0	--	?	++
Electronic forms signed by simple “click to accept” method.	--	+	0	++	++	++

Note: Cells represent a rough estimate of the value of interaction techniques against several criteria.
 ++ = very good; + = good; 0 = neutral; - = deficiencies; -- = serious deficiencies.

References

- Adar, E., & Huberman, B. A. (2000). Free Riding on Gnutella. *First Monday*, 5(10), NP.
- American Psychological Association. (2002). *Ethical principles of psychologists and code of conduct, Draft 7*. Washington, DC: American Psychological Association.
- Banaji, M. R. (2001). The nature of remembering: Essays in honor of Robert G Crowder
Implicit attitudes can be measured PB -, 2001 xix, 396. In H. L. Roediger, III & J. S. Nairne & e. al. (Eds.) (pp. 117-150).
- Bassett, E. H., & O'Riordan, K. (in press). Ethics of Internet research: Contesting the human subjects model. *Journal of Ethics and Information Technology, Vol 4*.
- 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(2), 147-165.
- Bruckman, A. (1999). The Day After Net Day: Approaches to Educational Use of the Internet. *Convergence*, 5(1).
- Bull, S., & McFarlane, M. (2000). Soliciting Sex on the Internet: What Are the Risks for Sexually Transmitted Diseases and HIV? *Sexually Transmitted Diseases*, 27(9), 545-550.
- Butler, B. (2001). Membership Size, Communication Activity, and Sustainability: A Resource-Based Model of Online Social Structures. *Information Systems Research*, 12(4), 346-362.
- Center for Disease Control. (June 19, 2001). *The Tuskegee Syphilis Study: A Hard Lesson Learned*. Retrieved Feb 17, 2003, from the World Wide Web: <http://www.cdc.gov/nchstp/od/tuskegee/time.htm>
- Cobanoglu, C., Warde, B., & Moreo, P. J. (2001). A Comparison of Mail, Fax and Web-Based Survey Methods. *International Journal of Market Research.*, 43(4), 441-452.
- Couper, M. P. (2001). The Promises and Perils of Web Surveys. In A. Westlake & W. Sykes & T. Manners & M. Rigg. (Eds.), *The Challenge of the Internet*. (Vol. 35-56). London: Association for Survey Computing.
- Couper, M. P. (2001). Web surveys: A review of issues and approaches. *The Public Opinion Quarterly*, 64(4.), 464-494.
- Couper, M. P., & Nicholls, W. L. I. (1998). The History and Development of Computer Assisted Survey Information Collection. In M. P. Couper & R. P. Baker & J. Bethlehem & C. Z. F. Clark & J. Martin & W. L. Nicholls II & J. O'Reilly (Eds.), *Computer Assisted Survey Information Collection*. New York: Wiley.
- Couper, M. P., Traugott, M. W., & Lamias, M. J. (2001). Web survey design and administration. *The Public Opinion Quarterly*, 65(2), 230-253.
- Crawford, S. (2002). Evaluation of Web Survey Data Collection Systems. *Field Methods*, 14(2), 226-240.

- Csikszentmihalyi, M., & Csikszentmihalyi, I. S. (Eds.). (1988). *Optimal experience: Psychological studies of flow in consciousness*. New York, NY, US: Cambridge University Press.
- Cummings, J. N., & Kraut, R. (2002). Domesticating computers and the Internet. *The Information Society, 18*(3), 1-18.
- Cummings, J. N., Sproull, L., & Kiesler, S. B. (2002). Beyond hearing: Where the real-world and online support meet. *Group Dynamics, 6*(1), 78-88.
- Dillman, D. (2000). *Mail and Internet surveys* (2nd ed.). New York: Wiley.
- Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *British Medical Journal, 323*(10), 103-105.
- Frankel, M. S., & Siang, S. (1999). *Ethical and Legal Aspects of Human Subjects Research on the Internet* (Available as: <http://www.aaas.org/spp/dspp/sfrr/projects/intres/report.pdf>). Washington, DC: American Association for the Advancement of Science (AAAS).
- Fricker, R. D., & Schonlau, M. (2002). Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature. *Field Methods, 14*(4), 347-365.
- 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*(1), 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.
- Hiltz, S., & Turoff, M. (1978). *The network nation: Human communication via computer*. Cambridge, MA: MIT Press.
- Hinds, P., & Kiesler, S. (Ed.). (2002). *Distributed work*. Cambridge, MA: MIT Press.
- Hoffman, D., Novak, T. P., & Duhachek, A. (2002). The Influence of Goal-Directed and Experiential Activities on Online Flow Experiences. *Journal of Consumer Psychology*.
- Horrigan, J. B., & Lee Rainie, D. (2002). *Getting Serious Online* (Report). Washington, DC: Pew Internet & American Life Project.
- Huston, A. C., Donnerstein, E., Fairchild, H. H., Feshbach, N. D., Katz, P. A., Murray, J. P., Rubinstein, E. A., Wilcox, B. L., & Zuckerman, D. (1992). *Big world, small screen: The role of television in American society*.
- King, S. (1996). Researching Internet Communities: Proposed Ethical Guidelines for the Reporting of Results. *The Information Society, 12*(2), 119-127.
- Kraut, R., Kiesler, S., Boneva, B., Cummings, J. N., Helgeson, V., & Crawford, A. M. (2002). Internet paradox revisited. *Journal of Social Issues, 58*(1), 49-74.
- Kraut, R., Mukhopadhyay, T., Szczypula, J., Kiesler, S., & Scherlis, W. (1999). Communication and information: Alternative uses of the Internet in households. *Information Systems Research, 10*(4), 287-303.
- 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*(9), 1017-1031.

- Kraut, R. E., Fussell, S. R., Brennan, S. E., & Siegel, J. (2002). Understanding effects of proximity on collaboration: Implications for technologies to support remote collaborative work. In P. Hinds & S. Kiesler (Eds.), *Distributed work* (pp. 137-162). Cambridge, MA, US: MIT Press.
- 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(4), 437-453.
- McKenna, K., & Bargh, J. (1998). Coming out in the age of the Internet: "Demarginalization" through virtual group participation. *Journal of Personality and Social Psychology*, 75(3), 681-694.
- McKenna, K., & Bargh, J. (Eds.). (2002). *Consequences of the Internet for Self and Society: Is Social Life Being Transformed?* (Vol. 58(1)): Society for the Psychological Study of Social Issues.
- 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 & Social Psychology*, 75(3), 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(1), 9-31.
- Milgram, S. (1963). Behavioral study of obedience. *Journal of Abnormal and Social Psychology*, 67(4), 371-378.
- Montgomery, A. L. (2001). Applying Quantitative Marketing Techniques to the Internet. *Interfaces*, 30(2).
- Moon, J. Y., & Sproull, L. (2000). Essence of distributed work: The case of the Linux Kernel. *First Monday*, 5(11), November.
- Nosek, B. A., Banaji, M., & Greenwald, A. G. (2002a). Harvesting implicit group attitudes and beliefs from a demonstration web site. *Group Dynamics*, 6(1), 101-115.
- Nosek, B. A., Banaji, M., & Greenwald, A. G. (2002b). Harvesting implicit group attitudes and beliefs from a demonstration web site. *Group Dynamics*, 6(1), 101-115.
- Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002). E-research: Ethics, security, design, and control in psychological research on the Internet. *Journal of Social Issues*, 58(1), 161-176.
- O'Leary, M., Orlikowski, W., & Yates, J. (2002). Distributed work over the centuries: Trust and control in the Hudson's Bay Company, 1670-1826. In P. Hinds & S. Kiesler (Eds.), *Distributed Work* (pp. 27-54). Cambridge Ma: MIT Press.
- Olson, G. M., & Olson, J. S. (2000). Distance Matters. *Human-Computer Interaction*, 15(2-3), 139-178.
- Olson, M. (1971). *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, Mass: Harvard University Press.
- Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organizational Science*, 11(4), 404-428.
- Rimm, M. (1995). Marketing Pornography on the Information Superhighway. *Georgetown Law Review*, 83(June), 1849-1934.
- Robinson, J. P., Neustadtl, A., & Kestnbaum, 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, FL.
- Rocco, E. (Ed.). (1998). *Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact*. Los Angeles, California, United States: ACM Press.
- Singer, E. (1978). Informed consent: Consequences for response rate and response quality in social surveys. *American Sociological Review*, 43(2), 144-162.
- Singer, E., Hippler, H., & Schwarz, N. (1992). Confidentiality Assurances in Surveys: Reassurance or Threat? *International Journal of Public Opinion Research*, 4(3), 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, & Keller, J. (Ed.), *Public access to the Internet*. Cambridge, MA: MIT Press.
- Sproull, L., & Kiesler, S. (1991). *Connections: New ways of working in the networked organization*: MIT Press.
- Sproull, L., & Kiesler, S. B. (1991). *Connections: New ways of working in the networked organization*. Cambridge, MA, US: The MIT Press.
- Thomas, J. (1996). When cyberresearch goes awry: The ethics of the Rimm "Cyberporn" study. *The Information Society*, 12(2), 189-198.
- Tourangeau, R., Couper, M. P., & Steiger, D. M. (In press). Humanizing self-administered surveys: experiments on social presence in web and IVR surveys. *Computers in Human Behavior*.
- Trice, A. D. (1987). Informed consent: VIII Biasing of sensitive self-report data by both consent and information. *Journal of Social Behavior & Personality*, 2(3), 369-374.
- Turkle, S. (1997). *Life on the Screen*. New York, 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.
- Walsh, J. P., & Maloney, N. G. (2002). Computer network use, collaboration structures, and productivity. In S. Kiesler (Ed.), *Distributed Work* (pp. 433-451). Cambridge, MA: MIT Press.
- Waskul, D., & Douglass, M. (1996). Considering the Electronic Participant: Some Polemical Observations on th eEthics of On-Line Research. *The Information Society*, 12, 129-139.
- Webb, E. J., Campbell, D. T., & Swartz, R. D. (1999). *Unobtrusive measures*. Newbury Park, CA: Sage.
- Wellman, B., & Haythornthwaite, C. A. (Eds.). (2003). *The Internet in Everyday Life*. New York: Blackwell Publishers.
- Wellman, B., Quan Haase, A., Witte, J., & Hampton, K. (2001). Does the Internet increase, decrease, or supplement social capital? Social networks, participation, and community commitment. *American Behavioral Scientist*, 45(3), 436-455.

- Williams, K. D., <kip@psy.mq.edu.au>. (2002, June 5). Debriefing in the Cyberostracism experiment. Email to Robert Kraut <robert.kraut@cmu.edu>.
- Williams, K. D., Cheung, C. K. T., & Choi, W. (2000). Cyberostracism: Effects of being ignored over the Internet. *Journal of Personality & Social Psychology*, 79(5), 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(1), 65-77.
- Williams, K. D., Wheeler, L., & Harvey, J. A. R. (2001). Inside the social mind of the ostracizer. In et al. (Ed.), *The social mind: Cognitive and motivational aspects of interpersonal behavior* (pp. 294-320): , 2001 xvi, 444.

Sidebar 1: Protecting Identities In An Online Survey

The Internet (and particularly the Web) vastly extends the power of experimental manipulations. This is especially true in the case of experiments or surveys. For example, Tourangeau, Couper & Steiger (In press) conducted a series of experiments on the effect of social presence in Web surveys on the answers provided to sensitive question, including both socially desirable and socially undesirable behaviors. The topics included attitudes towards gender equality, drug and alcohol use, diet and exercise, voting and church attendance, impression management, and so on. For example, one study varied whether the respondent saw a picture of a male researcher, a female researcher or a logo of the study. In addition, some respondents received feedback based on previous answers, while others did not.

The sample was obtained through Survey Sampling, Inc. (SSI), a vendor of mail, telephone and Internet samples, which maintains a list of over 7 million Internet users who have expressed willingness to receive such surveys or related materials. SSI sent the invitation to a sample of 15,000 members of this list, directing them to the researchers' URL, and providing each with a unique login and password. In this way the respondents' identities were unknown to the researchers and access to the survey was restricted to those who were invited. Equal numbers of male and female participants were selected and the random assignment of respondents to treatment was stratified by gender. Over 3,481 respondents logged into the survey site, and 87.5% (3,047) of these completed the survey. Several such surveys could be conducted in the time it would take to conduct one laboratory study of more limited scope and higher cost.

Incentives were delivered by SSI, again without revealing the respondent's identity to the researchers. This was done by delivering to SSI a list of the IDs of those who completed the survey. In this way the identifying information and the respondent data were kept completely separate in two different locations and by two different organizations. At no time did the researchers have access to respondents' e-mail addresses or any other identifying information. And at no time did the sample vendor have access to any of the survey responses.

While the results showed few effects of the social presence manipulation on the likelihood of reporting socially sensitive information, this example points to the advantages of the Internet as a forum for research on topics such as this. A study of this magnitude and complexity could not be undertaken using traditional survey methods (e.g., telephone or face to face) or laboratory-based experiments. Furthermore, responses to a variety of highly sensitive questions were collected in a controlled experiment without compromising the confidentiality of participants.

Sidebar 2: Online Experiments

After several years of studying implicit social cognition in traditional laboratories, Greenwald, Banaji, and Nosek developed a website to collect data about implicit attitudes for both research and educational purposes (B.A. Nosek et al., 2002a). The site is currently reachable at <http://implicit.harvard.edu>. Drop-in respondents participate in a task lasting approximately 5 minutes to gain insight into the workings of implicit attitudes and stereotypes. This site uses The Implicit Association Test (IAT; Greenwald, McGhee, & Schwartz, 1998) to collect response latencies to measure the strength of association between a concept (e.g., a social group such as “elderly” and “young,”) and an attribute, (e.g., an evaluation such as good-bad) or a stereotype such as slow-fast. The test rests upon the assumption that people will be faster to respond to a concept-attribute pair that reflect their attitude or stereotype (e.g, elderly-slow) than one that does not (e.g., elderly-fast or young-slow) (See Banaji, 2001 for further explanation.) Since the site opened in September 1998, participants have completed over 1.5 million tasks that capture some aspect of attitude or stereotype involving self, other individuals, or social groups (B.A. Nosek et al., 2002a). The site is now separated into a demonstration site that collects little personal information and provides an educational experience within a short period of time and a research site, which demands a more time and request more personal information, including an email address.

Data quality concerns involved required the investigators to develop an applet that could measure reaction time data via the Web. They could not use a remote server to present stimuli and collect response times, because network congestion and routing decisions would have introduced substantial error into the response latencies. To assess the validity of their new procedures, the investigators initially placed online only tasks that had been extensively tested in the laboratory, to make sure that the new procedures and subject populations produced results consistent with laboratory data based on college students.

The major benefit of collecting data online was the very large sample size it produced with minimal marginal costs. In the first two years, the website collected over 400,000 tests in the race task alone.

- The large sample size yields highly stable data.
- The large sample size allowed the investigators to develop new algorithms to score the Implicit Attitude Tests. They could develop the new algorithms on substantial sub-samples and test on new sub-samples.
- The large sample size produced new findings from relatively rare populations (e.g., young girls with special interest in math and science) or other specialized populations of interests (e.g., minorities) and to investigate the consequence on attitudes of both planned events, such as the 2000 national election, and unpredicted ones, such as attacks on the World Trade Center on September 11, 2001.

This research illustrates several ways to protect the welfare of human subjects. This website collected no personal information other than broad demographic data. IP addresses were separated from the data prior to analyses. Although perhaps not necessary, the researchers used a secure server to store the data, even though this protection excluded some participants. The tests involved no deception. They were advertised as an opportunity for participants to measure their hidden biases, and the informed consent statement warned potential participants that they could learn about disturbing aspects of themselves. “If you are unprepared to encounter interpretations that you might find objectionable, please do not proceed further.” Participants clicked on an “I wish to proceed” link to take the tests.

Debriefing took the form of a series of frequently asked questions and answers (FAQs), along with links to supporting research and related work. Because, in online experiments, participants could leave a site before encountering the debriefing information, this site automatically redirected a participant’s browser to the debriefing pages if a participant terminated a session for almost any reason.

The site also provided an email address for correspondence. The investigators learned the value of a complete FAQ archive early in the history of the site. As they added FAQs in response to emailed queries, participants dramatically reduced the number of questions they sent to the investigators.

In its primary lapse in protecting human subjects, the site made no provisions for screening out children or other vulnerable populations.

Sidebar 3: Protecting Identities in Chatroom Research

Research on chat rooms and other Computer Mediated Communication (CMC) environments is often ethically problematic, when the researcher creates a record of otherwise ephemeral communication. However, it can be conducted ethically, even in forums concerning highly sensitive subject matter.

One example is research by Bull and McFarlane (2000), which examined conversations in Internet chat rooms to understand how the Internet is used to find sex partners and the risks such activity poses for sexually transmitted diseases (STD). Data in selected chat rooms was collected through passive observation; observers did not interact with participants. The authors observed 175 discussions in chat rooms with sexual content. Each observation lasted from 30 minutes to two hours. They found evidence that people find sex partners online and as a result, appear to engage in sexual activities that put them at risk for STDs, including HIV. The study concludes that the Internet facilitates risky sexual contact in the same way that it facilitates shopping and research: it makes everything faster, easier, and more accessible.

Activity in these chat rooms was highly sensitive and if disclosed outside of the research setting, could put participants at legal risk. The participants were frequently discussing sex acts, which were illegal in some jurisdictions even among consenting adults. Research records could be vulnerable to court subpoena. To protect human subjects, Bull and McFarlane first obtained a certificate of confidentiality (Bull and McFarlane, 2000)³. A certificate of confidentiality gives the researcher the right to refuse to turn over such data to anyone, including courts and law enforcement officials.

Furthermore, the researchers destroyed the link between participants' identities and the conversational data. After chat log files were collected, the researchers coded the conversations for instances of behaviors of interest. They subsequently destroyed the original logs. In the final published study, the authors included several pseudonyms through which users identified themselves online. It may have been preferable for the authors to have changed the pseudonyms, since they often serve as persistent identifiers and could be traced back to the user's real names.

³ The Public Health Service Act 301 (d), 42 USC 241 (d) provides Certificates of Confidentiality, which can be requested from the Secretary of the Department of Health and Human Services. They afford special protection in cases where it is deemed [necessary?appropriate?]. This certificate gives the researcher protection from being "compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding to identify such individuals." Eligible [?] research areas involve sexual attitudes and preferences, alcohol and drug use, illegal conduct, mental health, medical records, genetic make-up, or information that if released could be damaging to financial standing, employability, or reputation, or lead to social stigmatization or discrimination. Research on the Internet is especially appealing with these topics because there is no coercion, and responses can be anonymous. The appropriate use of a Certificate of Confidentiality would grant the investigator the right to protect participants, and its use does not require that the research be federally funded. For more information visit: <http://ohrp.osophs.dhhs.gov/humansubjects/guidance/certconpriv.htm>

With these precautions, the researchers successfully protected their subjects, while obtaining research data that provided valuable insight into public health issues. On the other hand, these precautions degraded the scientific value of the data. For example, other researchers could no longer reanalyze the data to extend or challenge conclusions. Nor could the authors reanalyze the data for test new hypotheses. In this case, a better compromise might have been for the authors to anonymize logs by removing names, pseudonyms, email addresses, and other identifying details, but otherwise keeping the logs intact.

The difficult question for research on otherwise ephemeral communication is how to decide what degree of precautions is necessary. This will vary depending on the nature of the forums being studied—both their publicness and the sensitivity of the topics being discussed. For example, in chat rooms on less controversial topics, participants frequently flirt with each other and may form strong personal relationships (McKenna, Green, & Gleason, 2002). Records created of such activity could be vulnerable to subpoena in divorce cases. Whether researchers should request a certificate of confidentiality, destroy logs, or anonymize the data depends upon their informed judgments on the likelihood and severity of negative consequences to participants to participants if the records were disclosed, through subpoena or other mechanisms.

Sidebar 4: Protecting Participants in Online Deception Experiments

As discussed in the text, conducting deceptions experiments online may be problematic, because of problems of monitoring reactions and conducting debriefing.

Williams and his colleagues (2001) have conducted a series of online experiments examining the impact on participants of being ostracized or excluded. In their basic paradigm, participants play an online ball-toss game with other putative participants, who in reality are computer programs. Participants are given controls that allow them to direct the ball to either of the other two putative players and believe other players have similar controls. The experiments compare an involvement condition, in which participants receive the ball, to an ostracism condition, in which they are excluded. Across several studies, ostracism had negative psychological consequences. Compared to the included participants, excluded ones reported lower self-esteem, less sense of belonging to their group, and more negative moods, for example.

In Experiment 2 (reported in Williams et al., 2001), 501 participants initially accessed the experiment's website. Over 50% of the initial participants, however, failed to complete the experiment. In Experiment 1 in the same paper, the dropout rate was 13%. Other experiments in this series have had dropout rates of less than 10% (Williams, 2002, June 5). Dropout rates in online research are typically higher than those for comparable laboratory experiments. This difference in dropout rates illustrates both strengths and weakness of online research. Because participants feel less compelled to stick with online experiments than laboratory ones, their behavior gives credence to the language in most informed consent procedures—that participants are free to discontinue at any time without consequence.

On the other hand, if the reasons for are associated with the experimental conditions, high dropout rates undercut the value of random assignment of participants to conditions and are a threat to the internal validity of the research. After dropouts, the participants in different conditions will no longer be equal on measured and unmeasured variables. In the Williams experiment, dropouts were distributed evenly across experimental conditions. The authors attribute the high dropout rate to telecommunication delays and technical problems, rather than to discomfort with the experimental procedures.

The experimental procedure for the Williams et al. experiments took participants to a debriefing page, which explained the phenomenon of ostracism, the deception and the need for it. Because, by definition, researchers cannot offer true informed consent during deception experiments, they have a special obligation to debrief participants in this type of research. If participants dropped out of the experiment early, they would not reach the debriefing page, with its explanations. Because researchers have an obligation to provide subjects with “additional pertinent information after participation CR§116(d4),” the loss of subjects before debriefing in deception experiments is especially problematic.

While Williams (Williams, 2002, June 5) reports that over 90% of participants who start recent experiments continue all the way through, including the debriefing, other online experiments do not seem to show the same concern for debriefing. For example,

in an experiment by Glaser and colleagues (2002), experimenters entered Internet Relay Chat rooms operated by racist organizations and enticed participants to react to different types of threats posed by a minority member—marriage, job competition, or housing. Even though the experimenters did not provide participants with a description of the research before engaging them in the manipulation, they seemed to have made no effort to debrief them after the fact. We consider this a breach of the researchers' ethical responsibilities.