Behavior Research Methods
2008, 40 (4), 1111-1128
doi: 10.3758/BRM.40.4.1111

Practical advice for conducting ethical online experiments and questionnaires for United States psychologists

KIMBERLY A. BARCHARD
University of Nevada, Las Vegas, Nevada

AND

JOHN WILLIAMS
University of Northern Iowa, Cedar Falls, Iowa

It is increasingly easy and, therefore, increasingly common to conduct experiments and questionnaire studies in online environments. However, the online environment is not a data collection medium that is familiar to many researchers or to many research methods instructors. Because of this, researchers have received little information about how to address ethical issues when conducting online research. Researchers need practical suggestions on how to translate federal and professional ethics codes into this new data collection medium. This article assists United States psychologists in designing online studies that meet accepted standards for informed consent, deception, debriefing, the right to withdraw, security of test materials, copyright of participants' materials, confidentiality and anonymity, and avoiding harm.

Online psychological research is inexpensive, can result in large sample sizes and high statistical power, and allows researchers to include participants from distant geographical areas (Birnbaum, 2004a; Reips, 2000). Across a wide range of variables, online studies lead to the same conclusions as laboratory studies (Krantz & Dalal, 2000), but they can also have greater external validity and generalizability than does laboratory research (Reips, 2000). Finally, the widespread availability of easy-to-use Web development software and programs designed specifically to create online surveys (see Table 1) makes creating and running online studies relatively easy, requiring little technical knowledge (Barchard & Pace, in press). For all these reasons, online psychological research is becoming relatively common. The purpose of this article is to provide psychologists with practical advice for conducting online studies in an ethical manner.

The number of online studies is large and increasing dramatically. In 2004, over 278 Internet studies were advertised on laboratory Web sites (Birnbaum, 2004a). On one site, Birnbaum (2004a) found a 425% increase from 1998 to 2003. In addition, there are Web page studies that are advertised in other ways, e-mail studies, and observational studies in which researchers join already existing groups, and these types of studies have also been increasing. Given the cost and time savings of collecting data electronically, online research will likely continue to increase in popularity.

Online studies differ in many ways from in-person studies conducted in research labs. For example, data are often sent electronically from the participant's computer to the researcher's computer, whereas in many in-person studies, the participant completes measures on paper. Without careful consideration of the implications of such methodological differences, researchers who are new to online research (and the number of such researchers increases each year) are likely to design studies that fail to meet accepted standards (Mathy, Kerr, & Haydin, 2003).

Fortunately, the ethical issues facing online psychological research are the same as the issues faced by in-person psychological research, and therefore, the same ethics guidelines can assist us. This article will focus on the guidelines that apply to most psychological research in the United States: Chapter 45 of the Code of Federal Regulations (CFR), Part 46: Protection of Human Subjects (CFR 46, 2001); Title 17, Copyright Laws (Copyright Law, 2003); and the American Psychological Association's (APA's) Ethical Principles of Psychologists and Code of Conduct (American Psychological Association, 2002). Not all laws and codes are relevant to ethical issues, and no one ethical system (e.g., utilitarianism, etc.) is adopted by all United States researchers; we have selected these laws and codes because they apply to all psychologists doing research in the United States and are particularly relevant to ethical issues in online research. This article goes beyond previous discussions on creating ethical online studies (e.g., Birnbaum, 2004b; Ess, 2002, 2007; Ess & the Association of Internet Researchers, 2002; Frankel & Siang, 1999; Kraut et al., 2004; Nosek, Banaji, &

K. A. Barchard, kim.barchard@unlv.edu

Table 1
Computer Programs for Creating Online Studies

Program	Developer	Available From
Easy-to-Use Web Development Software		
Amaya (free)	W3C	www.w3.org/Amaya/
Authorware 7	Adobe	www.adobe.com/products/authorware/
Dreamweaver CS4	Adobe	www.adobe.com/products/dreamweaver/
First Page 2006	EvrSoft	www.evrsoft.com/
Flash CS4	Adobe	www.adobe.com/products/flash/
SharePoint Web Designer 2007	Microsoft	office.microsoft.com/en-us/sharepointdesigner/default.aspx
Expression Web 2	Microsoft	www.microsoft.com/expression/
Programs Specifically Designed to Create Online Surveys and/or Web Experiments		
EventHandler 4.0c	UbiDog Productions	www.event-handler.com/
LiveCycle Designer ES	Adobe	www.adobe.com/products/livecycle/designer/
mrInterview	SPSS	www.spss.com/mrinterview/
SurveySolutions/EFM	Perseus Development Corporation	www.perseus.com/
SurveyMonkey	SurveyMonkey.com	www.surveymonkey.com/
The Survey System	Creative Research Systems	www.surveysystem.com/
SurveyWiz (free)	Birnbaum	psych.fullerton.edu/mbirnbaum/programs/surveyWiz.htm
WEXTOR (free for educational and noncommercial uses)	Reips & Neuhaus	psych-wextor.unizh.ch/wextor/en/

Greenwald, 2002; Peden & Flashinski, 2004; Wood, Griffiths, & Eatough, 2004) by including the APA Ethics Code and U.S. Copyright Laws and by providing specific steps for addressing each ethical issue. Psychologists should keep in mind that their local institutional review board (IRB) or administrative unit may require that additional steps be taken to meet the standards presented here or may require adherence to additional standards.

A single article cannot adequately address the ethical issues facing every possible type of online study. Online research includes questionnaires and tests, interviews, and naturalistic observation and can be conducted through Web pages, e-mails, chat rooms, bulletin boards, and graphics-based simulations (Kraut et al., 2004). It includes topics as wide-ranging as online shopping (Byrom & Medway, 2004), psychometric equivalence (Buchanan, Johnson, & Goldberg, 2005; Meyerson & Tryon, 2003), drug dealing (Coomber, 1997), hate crimes (Glaser, Dixit, & Green, 2002), sexsomnia (Mangan & Reips, 2007), and eating disorder support groups (Walstrom, 2004). This article focuses on one common type of online psychological research, in which legally competent adults are explicitly invited to participate in research. Examples of such studies can be found on the University of Mississippi's (2000) PsychExperiments Web site, Hanover College's (2008) Psychological Research on the Net Web site, the Social Psychology Network's (1996–2008) social psychology research Web site, and two Web sites at the University of Zurich: the Web Experimental Psychology Lab (Reips, 1995–2008) and the Web Experiment List (Reips, 2001–2008).

One relatively common type of online study poses few ethical challenges. This is a study in which anonymous participants complete rating scales that do not address any sensitive issues and that is advertised in such a way that the only people who will see the study advertisement are legally competent adults. This type of minimal risk study poses few ethical challenges and may be exempt from IRB review. However, many online studies do not fit this profile: Identifying information might be collected, sensitive questions might be asked, or the study advertisement might be seen by children or adults who are not legally able to provide consent. This article provides practical advice about how to design and run those types of studies and how to convince your local IRB that you have adequately addressed the ethical issues that are raised by your study design. We first will discuss the differences between such studies when they are conducted online and when they are conducted in person, and then we will discuss how to ensure that an online study is ethical. Wherever possible, we will include several suggestions that address a particular ethical issue, so that researchers can select the technique that is most effective for their particular research project, while minimizing the influence on data quality. These discussions may provide a model for how to think about ethical issues as technology changes over time.

DIFFERENCES BETWEEN ONLINE RESEARCH AND IN-PERSON RESEARCH

Online psychological research differs from in-person psychological research in many ways (Mathy et al., 2003), and many of these differences present challenges to designing an ethical study. The first obvious difference is that researchers usually have no direct contact with participants. Ethically, there are two benefits of lack of direct contact. It is easier to ensure complete anonymity, which may explain why online studies obtain higher response rates on sensitive questions (McCabe, 2004). And participants do not feel as much social pressure to stay, which increases their ability to discontinue participation if they become uncomfortable (Birnbaum, 2004b; Fricker & Schonlau, 2002; Kaplowitz, Hadlock, & Levine, 2004).

Lack of direct contact does, however, present three challenges to designing an ethical study. First, researchers cannot use visual and verbal cues to determine whether participants understand the consent form and debriefing or are upset by

their content. Second, researchers cannot provide immediate clarification if participants have questions about consent or debriefing. Third, researchers cannot easily verify that participants are legally old enough to consent. These challenges are not unique to online studies; they occur to various extents in mailed surveys, telephone surveys, and group testing sessions. This article discusses methods of meeting these challenges in the context of online research.

Differences between online studies and in-person studies also create challenges for obtaining high-quality data and valid results. For example, researchers are concerned about drop out rates and the representativeness of Internet samples. However, this article will focus exclusively on ethical issues. We recommend Birnbaum (2004b), Birnbaum and Reips (2005), Curran, Walters, and Robinson (2007), Dickinson, Arnott, and Prior (2007), Frankel and Siang (1999), Granello and Wheaton (2004), Kraut et al. (2004), and Reips (2002a, 2002b) for strategies for meeting methodological challenges in online studies.

The second main difference between online research and in-person research is that online research is often advertised more widely. Some online research is advertised to participants in one location (e.g., employees of one company, participants in the local subject pool), but much online research is advertised to anyone who wants to participate or to people with specified characteristics (e.g., schizophrenia, plays soccer) who live in any location. When a study is advertised over a large geographic area, this presents an ethical challenge, because it may be more difficult for participants to receive clarification. Although e-mail will usually be an option, in-person visits, phone calls, and postal mail may be inconvenient or expensive.

Another frequent difference between online and in-person studies is the method of responding. To answer questions, online participants use computer equipment (usually a keyboard and mouse), whereas many in-person studies use paper forms and verbal answers. Computerized responding presents two ethical challenges. First, it is more difficult to obtain signatures to indicate consent. Second, some people do not know how to effectively navigate Web pages, e-mail programs, and other online environments; they may become confused about how to do things and may not recognize security risks.

Finally, the fourth main difference is that in most online studies, participants' responses are electronically transferred from their computer to the server to the researcher's computer, whereas in most in-person data collection, either the data do not need to be transferred at all (i.e., the testing is done right in the lab, either on paper or on a computer), or the data are hand-carried from the testing location to the lab. Electronic data transfer presents an ethical challenge to protecting confidentiality, especially with the increased frequency of electronic information theft. Although the authors do not know of any cases of psychological study data being compromised via electronic transmissions, this article will discuss below how threats to confidentiality can occur—even in apparently anonymous surveys—at the respondent's computer, the server, and the researcher's computer and during data transfer.

ENSURING ETHICAL TREATMENT IN ONLINE RESEARCH

To ensure ethical treatment of participants in online studies, researchers must consider ethical issues that are the same as those they address for in-person studies but must adapt their methodology to fit the new environment. We will provide practical advice addressing eight ethical issues: informed consent, deception, debriefing, the right to withdraw, security of test materials, copyright of participants' materials, confidentiality and anonymity, and avoiding harm. We hope this discussion will assist researchers and IRBs in better understanding these ethical issues, provide practical tools for addressing these issues today, and model how to think about and address these issues as technology changes over time.

Informed Consent

Obtaining consent. The Code of Federal Regulations distinguishes between asking participants if they consent and documenting that consent. In many online studies, asking participants if they consent is easy, but documenting that consent is difficult, because the Code (CFR 46.117) requires a signature. We will begin by discussing which studies require informed consent, and then we will discuss the issue of documentation. A summary of our recommendations regarding informed consent is given in Table 2.

Although most institutional IRBs require informed consent, sometimes psychological studies can be conducted without it, according to the Code of Federal Regulations and APA Ethics code. The Federal Code (CFR 46.101) states that research is exempt from IRB review (and therefore, it is not necessary to obtain or document consent) if the study involves the use of educational tests, survey procedures, or interview procedures, unless the participants can be identified and disclosure of responses would harm the participants. The APA Ethics Code allows researchers to dispense with informed consent when permitted by federal law and, thus, is no more restrictive than the Federal Code. This means that much online psychological research can be conducted without asking for consent and without documenting consent—at least according to the Federal Code and the APA Ethics Code. The local IRB may be more restrictive. Some IRBs never grant exempt status, some grant exempt status in all cases allowed by the Federal Code, and some grant exempt status for only some of the cases allowed by the Federal Code. Researchers should check with their local IRBs to see whether their study is exempt, in which case informed consent is not required. Finally, even when informed consent is required, the IRB can waive the requirement for some of the standard elements of informed consent [CFR 46.116(c), 46.116(d)]; researchers must check with their local IRBs to determine whether they can use an abbreviated consent form.

When informed consent is required, the consent form must be clear and written in language understandable to the participant (APA Ethics Code, section 3.10; CFR 46.116). When the researchers and participants have no direct contact, the researchers must design the consent process

Table 2
Informed Consent

Essential[a]	Essential for Some Online Studies[b]	Additional Recommendations
	Informed Consent	
	If the research is conducted or supported by any federal department or agency, obtain approval from the local IRB before beginning data collection with human subjects.	
	If the IRB determines that the study is not exempt, obtain informed consent, write the consent form in a way that is clear and understandable to participants, and provide an opportunity for participants to ask questions and receive answers.	
	Documenting Consent	
	Unless the local IRB waives this requirement, document informed consent with a signature.	If documentation of informed consent is needed, we recommend a paper signature.
	If documentation of informed consent is required, collect this documentation before data collection begins.	If documentation of informed consent is not needed, we recommend that researchers provide partial documentation using "I consent" and "I do not consent" buttons, or by having participants e-mail to express interest, or by having participants answer questions about the study.
	If documentation of informed consent is required only for participants who want it, provide participants with a method of signing and returning the consent form but allow participants to begin the study before documentation is received.	If participants have poor computer skills or below-average language fluency, we recommend that researchers provide partial documentation of informed consent, using one of the methods above.
		If participants have poor computer skills, we recommend that researchers provide phone contact information.
		If the study is more than minimal risk, we recommend that researchers assess comprehension of consent information and make it easier for participants to ask questions.
Avoid recruiting children.		If exclusion of children is very important, we recommend that the Web site ask participants their age and direct children away from the Web site.
		If exclusion of children is critical, we recommend that the researcher obtain proof of age.
Avoid recruiting adults who cannot legally consent.		If the study requires the assessment of a person's capacity to legally consent, we recommend that the researcher provide higher levels of contact and consider in-person testing.

[a]Required by the Code of Federal Regulations and/or the APA Ethics Code for all online studies that were designed for legally competent adults and that qualify as human subjects research. [b]Required by the Code of Federal Regulations and/or the APA Ethics Code for some online studies. Each item indicates which studies it applies to.

carefully to ensure that the participants understand the information given (Kraut et al., 2004; Mathy et al., 2003). We recommend that researchers use simpler language than they would during an in-person study and avoid idioms, unless they know in advance that all potential participants will have high language fluency. In addition, if researchers are recruiting from a population that is likely to include people with disabilities, they should design their study materials to conform to W3C Web Content Accessibility Initiative Guidelines (Web Content Accessibility Guidelines Working Group, 1994–2007), by incorporating such features as adjustable text size and text labels for all graphics. If researchers are designing studies for older adults, we also recommend that they consider these accessibility guidelines, because many older adults have disabilities. (Andrew, Foley, McLellan, & Turnbull, 2004, report that 54.3% of people aged 65 and older in the United States have a disability.) Older people are also less likely to be computer literate and more likely to have motor and cognitive impairments (Dickinson et al., 2007), which should be considered when designing consent procedures. See Dickinson et al. for a discussion of computer research with older adults, and see Curran et al. (2007) for a discussion of online research with older adults and people with disabilities.

Documenting consent. The Code of Federal Regulations [CFR 46.117(a)] usually requires researchers to document consent with a signature on a written form. A written signature is easily and routinely obtained in laboratory settings. Unfortunately, if signed documentation of consent is needed in an online study, this will be inconvenient, because clicking on a button that says "I consent" is not legally equivalent to a written signature. When documentation of consent is needed, we recommend that researchers continue to use paper signatures. Participants can print, sign, and mail the consent form. Digital signatures can be legally substituted for written signatures (Electronic Signatures Act, 2000); however, digital signatures are no more conve-

nient than paper signatures when consent is documented, because each individual using a digital signature first needs to prove his or her identity to the entity that grants the digital signature. Thus, digital signatures do not represent a viable alternative to paper consent forms at this time. More in-depth discussions of digital signatures can be found in Youd (1996) and American Bar Association (2005).

Fortunately, many psychological studies do not need to document consent with a signed consent form. The Code of Federal Regulations [CFR 46.117(c)] states that IRBs may waive the signature requirement under two circumstances. The first circumstance is when "research presents no more than minimal risk and involves no procedures for which written consent is normally required outside of the research context." Most online studies in the United States probably fall into this category, which is why IRBs can justify waiving the requirement of documentation of informed consent and allow studies to proceed without a written signature. The second circumstance is when "the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality." Under this circumstance, the Federal Code allows each participant to decide whether they want to sign a consent form. Online researchers could tell participants that they may print, sign, and mail the consent form. This second circumstance appears to be rare in psychology. Most online studies can justify omitting documentation of consent, either because they are exempt from IRB review (and so informed consent is not required) or because they are minimal risk and the study involves no procedures for which informed consent is required outside of a research context. Some IRBs require researchers to submit a request for a waiver of documentation of informed consent for all online studies; check with your local IRB.

The Code of Federal Regulations does not state whether researchers need to receive consent documentation before participants begin the study. We make the following recommendations. When documentation is required for all participants, researchers should receive documentation first, to ensure that it is complete. After receiving documentation, researchers can give the participants access to the study. If documentation is optional (e.g., when participants decide whether they want to sign the consent form), the participants should be allowed to begin the study immediately, thus allowing the participants to complete the study in one session.

The local IRB may require informed consent and documentation of consent, even when the Code of Federal Regulations and the APA Ethics Code do not. Fortunately, the IRB may accept alternatives to a signature. Here are three possible alternatives. One easy method of documenting consent is to allow participants to indicate that they do not want to participate, as recommended by Mathy et al. (2003). The consent form can ask participants to choose between two options—"I consent" and "I do not consent"—and these responses can be sent to the database or collected from server log files. Because this is so easy, researchers may wish to offer a no-consent option (and discuss the purpose of this option with their IRBs) in all studies in which this is feasible. The inclusion of the no-consent option demonstrates that the researcher knows the importance of documentation and is attempting to obtain the best documentation possible. A second method of documenting consent is to ask participants questions about the consent form to check understanding (Pace & Livingston, 2005). This method will be discussed in greater detail below. Finally, researchers can document consent by directing participants to the study only after they e-mail to ask to participate (University of New Hampshire Institutional Review Board for the Protection of Human Subjects in Research, 2005).

Regardless of the stringency of the local IRB, we recommend that researchers document consent (e.g., by including a no-consent option) whenever participants may have poor computer skills or below-average fluency in the language used. For example, if a study of older adults is advertised using printed newsletters, the researcher may not be able to safely assume that every potential participant knows how to use the "Back" button or address bar to exit the study without consenting. This study could provide two methods of exiting every Web page: One method indicates that the person consents or wishes to continue participating; the other method allows the person to exit the study.

Many minimal risk studies, however, do not require documentation of consent, according to the APA Ethics Code and the Code of Federal Regulations. If studies are minimal risk, involve no procedures for which consent is normally required outside the research context, and are advertised on research-dedicated Web sites, IRBs may be satisfied that people who completed the study consented to participate. Visitors to those sites are probably very familiar with Web browsers and will have no difficulty in exiting an online study if they decide not to participate. Thus, even when studies require informed consent, they may not require written documentation of that consent, and thus it is possible to run these studies online.

For studies that are more than minimal risk, we are hopeful that legally acceptable online documentation of consent may be possible in the future. In our opinion, the current requirement of a written signature is too restrictive. The Code of Federal Regulations requires a written signature in order to document consent to participate in a research study. However, written signatures are not always required in other industries that carry comparable or greater levels of risk, such as online banking and commerce. For example, to transfer money from one bank account to another, customers can choose between two options, "transfer money" and "cancel"; and before using new software, customers can indicate acceptance of the license agreement by changing the selection from "do not accept" to "accept" and then clicking "continue." The online research community appears to be moving toward a consensus regarding the steps needed to document consent, borrowing methods that are used by online banking and commerce. We hope that such methods—deliberate, voluntary, online actions—will be accepted as documentation of informed consent in the Code of Federal Regulations at some point in the future.

Ensuring understanding. To ensure that participants understand what they are consenting to, they must

have the opportunity to ask questions and receive answers [APA Ethics Code, sections 3.10 and 8.02a; CFR 46.116, 46.116(a)(7)]. Because researchers are not present in online studies, studies that require consent need to build a question-asking opportunity into the consent process. At a minimum, researchers must provide contact information before asking participants if they consent and must reply to questions in a timely manner. We recommend that additional question-asking opportunities be given if the study has more than minimal risk.

Some researchers would argue that only minimal risk studies should be conducted online. We believe that this is too restrictive, and studies that are more than minimal risk can be conducted online if the researcher takes two additional steps to ensure understanding. First, we recommend that researchers make it easier for participants to ask questions. They could do this in at least two ways. The study could be available only when the researcher is available to answer questions, either by phone or in a chat room (Nosek et al., 2002). Although this would require the researcher to schedule time for running the study, as is the case with in-person studies, it may still be more convenient for the researcher to run such a study online, because participants can be geographically spread out. Alternatively, participants could be asked to e-mail the researcher to indicate that they consent and to ask any questions that they have, before the researcher gives them access to the study materials.

For studies involving more than minimal risk, we recommend that researchers take one additional step to ensure understanding: assess comprehension. Neither the Code of Federal Regulations nor the APA Ethics Code directly addresses the issue of understanding. However, the APA Ethics Code (section 3.04) does state that psychologists should avoid or minimize harm to research participants, and we believe that ensuring understanding is critical for studies that have more than minimal risk. Therefore, if a study involves more than minimal risk, we recommend that researchers embed questions about the process, benefits, and risks of the study in the consent form, as has been suggested by Frankel and Siang (1999) and Stanton and Rogelberg (2001). If potential participants answer the questions incorrectly, they can be given additional information. Because Web pages can dynamically interact with participants, ensuring participant comprehension may be easier in online studies than in some in-person studies (particularly group testing sessions). Making a Web page dynamically interact with users requires a Web-based programming language such as PHP, ASP, PERL, Java, or JavaScript. Learning a programming language can be time consuming initially, but programming greatly increases the flexibility of online studies.

If a study is minimal risk, however, we do not recommend that researchers ensure comprehension by asking participants questions during the consent process. This is not done during minimal risk in-person paper-based studies, and such additional steps should be added to online studies only if they are needed to ensure ethical treatment of participants. Implementing unnecessary additional steps may hinder or bias online research.

Excluding children. In the U.S., 18 is the age at which legal consent can be obtained. Other countries may have different age limits. Children can assent to participate in research, but they cannot legally consent (CFR 46.408). Consent must come from their parents or legal guardians. When studies have not been designed to obtain parental consent, researchers can take several steps to reduce the chance that children will participate. First, researchers can advertise in adult-oriented venues that will not appeal to children (Nosek et al., 2002). Second, researchers can present the studies themselves in ways that will not appeal to children. For example, they can avoid using cartoons (Nosek et al., 2002). A third strategy can also be used if these first two are considered insufficient. Near the beginning of the study, we recommend that researchers include a neutrally worded question that asks participants their age. If the participants are too young, direct them away from the study. To forestall them from returning and lying about their age, send them to an innocuous but interesting page, without saying that they cannot participate. If all three of these strategies are implemented, most minors will probably be excluded. However, none of these solutions can guarantee the exclusion of every minor. When excluding children is critical (e.g., studies that use sexually explicit material or age-restricted substances like tobacco or alcohol), preselected participants or in-person testing should be used, and proof of age (e.g., visual examination of birth certificate or driver's license) should be required whenever there is any doubt. If it is not feasible to obtain a visual inspection of proof of age in an online study and if it is not feasible to run the study in the laboratory, it is always an option to not run the study for ethical reasons. However, remember that the vast majority of laboratory studies do not require proof of age, and so most online studies will not require it either.

There are research questions where children should be included as research participants. In those cases, consent is obtained from the legal guardian of the child, and the child provides assent to the research. However, we would like to emphasize that changes to the consent procedures do not address all of the differences between research designed for legally consenting adults (addressed in this article) and research designed for children. The researcher needs to take into account children's verbal and cognitive limitations in every aspect of the design and conduct of the study. See Reips (1999) and Flicker, Haans, and Skinner (2004) for two alternative approaches to Internet research with children.

Excluding adults who cannot consent. A variety of conditions can impair someone's decision-making capacity and thus impair their ability to consent to research. These include substance abuse disorders, mental retardation, dementia, schizophrenia, and depression (National Bioethics Advisory Commission, 1998). Two approaches can be used to exclude people who cannot legally consent. The first approach is to avoid recruiting them. Thus, researchers can avoid advertising on Web sites and news groups that are designed for these groups and can avoid describing their study in ways that will attract such participants (e.g., "The Schizophrenia Study"). This is the approach that is already taken by the vast majority of online studies.

The second approach is to assess someone's capacity to provide informed consent; this may be necessary if

researchers are deliberately recruiting people who may have impaired cognitive abilities. Assessment of decision-making capacity is multifaceted (Roberts & Roberts, 1999). We argue that some aspects of this assessment could probably be done in an online study with no direct contact. For example, after reading information about the study, participants could answer comprehension questions. However, we argue that other aspects of the assessment cannot be conducted without direct contact. These include whether the participants are making a rational and deliberate decision and whether the participants understand the consequences of the decision within the context of their personal values, circumstances, and history (National Bioethics Advisory Commission, 1998; Roberts & Roberts, 1999). We therefore recommend that higher levels of contact be used for studies that require assessment of decision-making capacity. To facilitate research on these populations, we strongly recommend research on the evaluation of decision-making capacity and ability to legally consent. Such research may be difficult to conduct, because it may need to use participants who have legal guardians and populations of those who are recognized as sometimes being unable to legally consent. Yet such research is vital if online data collection is to use mentally ill participants.

Deception

Frankel and Siang (1999) have argued that deception cannot be justified in online studies, but we disagree. When researchers use deception, the APA Ethics Code requires that they explain the deception to the participants (section 8.08). In online studies, participants may not read and understand the debriefing information, and researchers may have difficulty addressing emotional turmoil (Kraut et al., 2004). Therefore, Frankel and Siang stated that it would be difficult to justify using deception in any online study. However, if the deception consisted solely of disguising the true purpose of the research or omitting some details, the risks might be minimal, even if some participants skipped the debriefing. We recommend that researchers and IRBs weigh the possible harm from inadequate debriefing against the benefits of conducting the research. In general, deception that can be justified for other methods with limited contact (such as group testing) can probably be justified for online studies.

Deception may also be easier to justify if researchers ensure that almost everyone receives the debriefing (see Table 3). For example, researchers can ask participants for consent to minor deception or for consent to withhold some details about the study and can tell the participants that they will be fully debriefed at the end. This may increase the probability that the participants will read the debriefing, and we recommend that researchers use this technique whenever feasible. The next section will discuss several additional strategies for ensuring that participants will read the debriefing.

Debriefing

Providing opportunities to debrief. Although the Code of Federal Regulations does not require researchers to debrief participants, the APA Ethics Code (section 8.08) requires that "psychologists provide a prompt opportunity for participants to obtain appropriate information about the nature, results, and conclusions of the research, and

Table 3
Deception and Debriefing

Essential	Essential for Some Online Studies	Additional Recommendations
Provide an opportunity for participants to obtain information about the study—for example, by providing contact information or answers to common questions at the end of the study.	If the study involves deception, explain the deception to participants during the debriefing. If the study involves deception, researchers must take reasonable steps to correct participants' misconceptions and thus must take reasonable steps to ensure that all participants receive debriefing information. See additional recommendations.	Although debriefing is not required by the Federal Code or APA if a study involves no deception, we recommend that all studies provide debriefing that describes the study in more detail than was given in the consent form. If ensuring understanding of debriefing information is critical, we recommend that researchers provide in-person debriefing. If the study involves deception or ensuring understanding of debriefing information is important for some other reason, we recommend that researchers assess understanding of debriefing information through the Web site and follow up incorrect responses with clarification. If the risks caused by deception are more than minimal, we recommend that researchers take extra steps to ensure that everyone receives debriefing. For example, we recommend that researchers ask for consent to minor deception or consent to withhold some details and tell participants they will be fully debriefed at the end. Researchers can also provide "Quit the study" links that go to debriefing; collect e-mail addresses and send debriefing e-mails; or make the study available only when the researcher is available to answer questions.

they take reasonable steps to correct any misconceptions that participants may have of which the psychologists are aware." Thus, all psychological research needs to provide opportunities to debrief.

For in-person studies, participants can ask their questions directly. However, online studies need to build in methods of obtaining additional information. This can be relatively easy. Researchers can provide contact information again at the end of the study and answer questions within a few days (see Table 3). Alternatively, researchers can provide answers to common questions at the end of the study. However, dropouts who close the browser window or who switch to another Web site will not read debriefing information that is given at the end of the study. Because dropout rates tend to be high in online studies, additional steps should be used if complete debriefing is important.

The following are some additional ways to provide debriefing. First, each page can include a "Quit the study" link that takes participants to a page with contact information and other information about the study, so that people who quit the study still receive debriefing. Second, the researcher can use JavaScript to create a popup debriefing window, if a participant closes the browser window before finishing the study. Third, some online experiment Web sites (e.g., genpsylab-wexlist.unizh.ch/) provide archives for debriefing information and require researchers to provide this information. Fourth, as Nosek et al. (2002) suggested, researchers can make the study accessible only when they are available in a chat room to answer questions. Fifth, researchers can collect e-mail addresses and send debriefing e-mails. If that option is chosen, researchers should explain that debriefing e-mails will be sent, to avoid breaches of confidentiality that may occur if participants provide e-mail addresses that they share with other people. This gives the participants the opportunity to provide a private e-mail account or to leave their e-mail address blank. As well, it is important to note that spam filters may block the reception of the debriefing e-mail. In order to minimize spam filter interference, researchers should use individualized subject lines and differing text within the body of the message. For most online studies, these steps are optional, because debriefing is not critical. However, providing detailed debriefing information to all participants may be critical for some studies involving deception or for studies conducted in participant pools with a mandatory educational component.

Ensuring understanding. Ensuring that participants read and understand debriefing information is more difficult in online studies than in in-person studies. When researchers believe that participants could be harmed if they are not fully debriefed, we recommend in-person debriefing. This way, researchers can ensure that participants receive the information and can use both verbal and nonverbal cues to check understanding. For example, if a study involved bogus negative personal feedback, in-person debriefing could ensure that the participants understood that the feedback was bogus.

For most psychological studies, debriefing is not critical. Those studies can be run online even though some people will skip the debriefing. First, if the debriefing is purely educational, researchers can run studies online without worrying about participants who skip debriefing. Neither the Code of Federal Regulations nor the APA Ethics Code requires that researchers ensure understanding of educational information. Second, if it is relatively important that participants understand debriefing information, studies can be run online with a few modifications. For example, if studies use minor deception, researchers must take reasonable steps to correct participants' misconceptions (APA Ethics Code, section 8.08). Under those circumstances, we recommend that researchers test participants' understanding of debriefing information and follow up incorrect responses with clarification through the Web site. Because Web sites can provide immediate feedback, ensuring understanding may be easier in online studies than in some types of in-person research, such as group testing. In general, if a study can be run with group testing and group debriefing, we argue that the researchers and IRB have determined that it is not critical that debriefing information be read and understood and, therefore, the study may be run online.

Right to Withdraw

Withdrawing participation. Participants have the right to withdraw at any time [CFR 46.116(b); APA Ethics Code, section 8.02]. In person, participants may feel social pressure to continue participating, because they want to be polite or researchers say that they need data. In contrast, participants feel little pressure to remain in online studies—an ethical advantage of online research (Reips, 1997, 2000).

Participants with poor computer skills may experience difficulty in withdrawing. They may not know how to exit by closing the window or using the address bar or back button. If some participants are likely to have poor computer skills, researchers should provide a simple method of withdrawing, such as "Quit the study" links on each page (see Table 4). This is particularly important if participants must answer every question before the computer lets them submit their responses. For example, participants might be required to give contact information so they can receive research credit or payment, and in some studies, participants are required to answer every question, so that the researcher obtains complete data and scale scores are valid. Whenever participants are required to answer questions before they can submit their responses, participants who do not know how to exit a page on their own may feel compelled to answer questions that they do not want to answer. If such participants will be recruited for the study, a simple method of withdrawing should be provided as part of the study itself.

Withdrawing data. When participants withdraw, they may also want to withdraw their previous responses. Neither the Code of Federal Regulations nor the APA Ethics Code explicitly states whether the right to withdraw participation implies the right to withdraw previously submitted data. In our opinion, the importance of data withdrawal depends on the study and why the participants withdraw. If the participants withdraw because they no longer want to continue the experience (e.g., they are

Table 4
Right to Withdraw

Essential	Essential for Some Online Studies	Additional Recommendations
	Withdrawing Participation and Obtaining Rewards	
Allow participants to withdraw from the study.	If informed consent is needed, tell participants the consequences of withdrawing from the study. If a study provides a partial or complete reward for partial completion of the study, collect the information that is needed to give that reward (such as name) at the beginning of the study.	If some participants are likely to have poor computer skills, we recommend that researchers provide simple methods of withdrawing from the study, such as "Quit the study" links.
	Withdrawing Data	
	If a study provides methods of withdrawing data that have been submitted, tell participants the consequences of withdrawing their data (and how to withdraw their data).	If participants are likely to withdraw because they find the study objectionable or because they are uncomfortable providing certain information to researchers, we recommend that researchers provide participants with a method of withdrawing their previously submitted data.

bored or fed up), allowing data withdrawal may not be important (and those participants may also be unlikely to read and answer questions about data withdrawal). However, we argue that participants should be given a method of indicating that their previous responses may not be used, if they withdraw because new information makes them find the study objectionable (e.g., explanation of deception) or because they are uncomfortable providing certain information to the researchers (e.g., confidential or emotionally sensitive information). The data withdrawal option should be presented after the new information or emotionally sensitive questions, as was done by Göritz (2006), or as part of the debriefing, as has been suggested by the University of New Hampshire Institutional Review Board for the Protection of Human Subjects in Research (2005).

In a paper-based study, withdrawing data is simple: If a participant says that he or she wants to withdraw the data, the pieces of paper are simply shredded. In an online study, the researcher needs to build in methods of withdrawing the data. There are three methods of withdrawing data in an online study. First, if the data have not yet been submitted, a reset button can erase answers. Second, if the data have already been submitted, the participant can request that the data be withdrawn by answering a question about data withdrawal at the end of the section or the end of the study or by e-mailing the researcher. Third, with some database designs, the participant can remove the data from the database without the researcher ever seeing it. The participant answers a data withdrawal question, asking that the data be removed, and the database removes the data immediately. Whichever method is used, researchers should tell participants the consequences of withdrawing from the study, including the consequences of different methods of withdrawing [CFR 46.116(b)(4)]. For example, the consent form could tell participants that if they withdraw by clicking a "Quit the study" button, they will be asked whether they would like to withdraw their data, but if they withdraw by closing the browser window, the data they have already submitted will be analyzed. The consent form could also tell participants to e-mail the researcher if they want to withdraw their data but were unable to use the data withdrawal option because of a computer malfunction or lost Internet connection.

Rewards. Psychologists sometimes give partial or complete rewards in return for partial completion (e.g., to protect students, clients, and subordinates from negative consequences of withdrawing; APA Ethics Code, section 8.04). The information needed to give these rewards (e.g., name or student number) must be collected at the beginning of online studies to protect participants' right to withdraw. Collecting this information at the beginning of the study also increases compliance in providing such information, which allows researchers to give participants their promised rewards (Frick, Bächtiger, & Reips, 2001).

In addition, psychologists must avoid offering excessive rewards that are likely to coerce participation (APA Ethics Code, section 8.06) or discourage participants from withdrawing. Although many online studies provide no reward or payment for participation and most payments are small (Peden & Flashinski, 2004), at least some studies provide lotteries for relatively large amounts (Musch & Reips [2000] reported one study with a lottery for $1,224). Researchers need to consider whether lotteries for larger amounts represent excessive rewards, depending on the type of participant being recruited.

Security of Test Materials

Test integrity. Psychologists are obligated to protect test integrity (APA Ethics Code, section 9.11). If test items are widely available, some test takers might know the answers and be able to fake a high or low score. To reduce the exposure of tests used in online research, researchers can control who sees their Web site. First, researchers can use password protection and control who receives the password. This is probably the most effective method of reducing test exposure. Many servers have built-in password protection, and free password protection systems are available on the Internet. Second, researchers can use a robots.txt file to tell search engine robots not to list their pages. Then, if someone asks search engines such as Google or Yahoo to find one of the tests used in the study,

the study pages will not be listed. See PHD Software Systems (1996–2002) or Koster (2008) to create a robots.txt file. Third, researchers can insert the following line into the header of the first page of their Web site:

<meta name="robots" content="noindex, nofollow">.

Like the previous technique, this prevents search engines from indexing that page and from following links to the rest of the study. If researchers use these techniques, only people responding to study advertisements will find study Web sites and the tests contained therein.

Copyright of test materials. Copyright holders have the exclusive right to decide when their works will be displayed publicly (Copyright Law, 2003, section 106). Legally, copyrighted materials can sometimes be used in research without infringing on copyright, depending on the proportion of the copyrighted work being used and how the use would affect its market value (section 107, Fair Use). However, we argue that openly publishing entire psychological tests on the Internet substantially affects their market value and, therefore, this does not constitute fair use. Including entire tests in e-mail studies can also affect market value, because e-mails are often forwarded to large numbers of people. Regardless of legal and financial considerations, we believe that copyright holders have the ethical right to say how their materials will be used. Thus, we conclude that researchers are both legally and ethically required to ask copyright holders for permission to include tests in e-mail and Internet studies, and if the copyright holders place restrictions on how the test can be used, researchers must adhere to those restrictions.

In our experience, copyright holders are rarely willing to allow researchers to openly display their tests in online studies. Online researchers therefore have three options. First, they can use public domain tests. For example, in the personality domain, a large set of scales is available through the International Personality Item Pool (ipip.ori.org). Second, they can write new tests. Writing new tests is time consuming and is usually not recommended if good tests of the desired constructs already exist. Third, researchers can address the concerns of copyright holders, in order to gain permission. Researchers often want to use established and validated tests in their research, both to ensure the quality of their studies and to allow comparisons with other studies. Thus, although these requests are often refused, it is valuable to discuss the steps researchers can take to try to obtain permission.

To obtain permission to use copyrighted tests in online studies, it is helpful for researchers to understand why copyright holders refuse this permission. In our experience, copyright holders refuse permission for three reasons, all of which are related to the fact that it is impossible to completely prevent participants from copying study materials in an online study. First, if a test is not free, the copyright holder is likely to refuse permission to use the test in an online study, because other people may find and then use the test without paying. In our experience, copyright holders for paid tests usually refuse permission to use a test in an online study unless an online version of the test already exists. In that case, the publisher usually requires the researcher to use the publisher's version of the online test.

Second, even when a test is free, copyright holders may refuse permission because they worry that their test might be used improperly. When instructions, items, response scales, or scoring are done improperly, the results obtained from this error-laden test are interpreted as reflecting badly on the original. To ensure that the test is used properly, many copyright holders place restrictions on who has access to the items. Publishing the test on the Internet as part of an online study makes the test items available to everyone and thus poses a threat to test integrity.

Finally, copyright holders sometimes express concern that test users may obtain the test items and answers in advance, thus invalidating their scores. This is especially likely to be a concern for tests used in employment or educational contexts, because test takers are motivated to obtain good scores. Once again, publishing the test as part of an online study makes the test items widely available, thus threatening the confidentiality of the items and their answers.

Given these concerns, how can a researcher obtain permission to use a copyrighted test in an online study? The researcher can modify the studies so that materials are not displayed so openly. First, the researcher can restrict access to the study, and second, the researcher can make it more difficult to copy the test. To reduce the number of people who can access the study, the researcher can use the robots.txt file, the robots meta-tag, and password protection, as described above. If password protection is being used, some researchers might argue that copyrighted materials are not being publicly displayed and, therefore, permission is not required. However, we argue that this depends on how many people are given the password, and we recommend asking permission anyway.

Although it is impossible to completely prevent participants from copying test materials, several strategies can be used to make it more difficult. Researchers can offer to implement one or more of these strategies, to try to obtain permission to use a test in an online study. First, researchers can prevent participants' computers from storing copies of the Web pages. See Birnbaum and Reips (2005) or Adobe (2008) on preventing Web page caching. Second, researchers can make it more difficult for most users to print, copy and paste, or use the print screen function, by inserting the following lines of html into the top of their Web page:

<body onload=setInterval("window
.clipboardData.clearData()",20)>

<body ondragstart="return false"
onselectstart="return false">

<body oncontextmenu="return false;">

<style media="print">body {display: none} </style>

These commands work if participants are using Internet Explorer 5 or later (about 72% of users) and have not disabled JavaScript (about 95% of users; The Counter, 2008). Third, to make it more difficult to save the Web page or to view and print the html code, researchers can open the study in a window without menus. See Burns (2008) or

JavaScript Kit (1997–2008) to do this using JavaScript. Fourth, researchers can present items one at a time, using a Web-based programming language like PHP, ASP, or PERL, or even by writing each page separately using plain html. Fifth, researchers can switch from software that creates html files (e.g., Macromedia Dreamweaver or Microsoft FrontPage) to software with built-in security features. For example, Adobe LiveCycle Designer, Macromedia Flash, and Macromedia Authorware all have built-in methods of presenting items one at a time and of preventing copying, printing, and saving. Learning new software is often time consuming; however, once researchers are familiar with the new software, it may be as easy to use as their current software. Finally, if necessary, researchers can supervise participants while they are viewing testing materials and never give the participants the study Web site address and password. This will prevent the participants from hand-copying the test.

Some combination of the procedures above may be sufficient to obtain permission from copyright holders. If the copyright holder grants permission, the researcher should faithfully reconstruct all aspects of the original test as closely as possible (title, instructions, response scale, items, formatting) and should display the copyright notice. In our experience, copyright holders are likely to grant permission to use a test in an online study if the items have been published in a journal article, dissertation, or book and some of the steps above are taken to protect test security. Even under these circumstances, some copyright holders will refuse permission. This is understandable, because the Internet represents a much wider distribution of the test items than do most academic media. If researchers are unable or unwilling to implement the security procedures that copyright holders require, or if the copyright holder refuses to grant permission under any circumstances, the materials may not be used in online studies. It is the researcher's responsibility to obtain permission to use copyrighted materials in research and to candidly discuss how tests will be administered and what security procedures will be used. Copyright restrictions are often inconvenient to online researchers, but copyright is a legal issue as well as an ethical one, and it cannot be ignored for researchers' convenience.

In addition, researchers must protect the security of copyrighted materials when sharing these materials with others. Conducting research online makes it easy for other researchers to view, use, and vary study materials, because the study address and password can be included in publications. However, if there are copyrighted materials in the study and the copyright holder does not want all readers to have access to them, the study materials should be edited to protect the copyrighted tests. For example, if the third Web page contained a copyrighted test, that page could be edited to give just the name of the test and the publisher's contact information. See Table 5 for a summary of our recommendations regarding test security.

Copyright of participants' materials. In some studies, researchers analyze participants' artwork, photographs, videos, poetry, or stories. If the researcher wants to include these materials in their manuscripts or presentations, they need to protect participants' copyright (see, e.g., Ess, 2007; Eysenbach & Till, 2001). Some participants will want their materials displayed and will want their names attached to the materials. Others may grant permission for their materials to be displayed but will not want their names attached. Others may refuse permission. If a researcher wants to present words or pictures that participants created, they need to incorporate a mechanism for obtaining permission. For example, they could ask for contact information and then contact those participants whose materials they want to use. Alternatively, they could ask all the participants for permission to reproduce their works and whether they want their name attached.

Researchers should keep in mind possible conflicts between protecting participants' copyright and protecting their confidentiality (see, e.g., Ess, 2007). If the copyrighted materials were publicly displayed (e.g., in a book or art exhibit), researchers would automatically give credit to the artist. However, when copyrighted materials are shared privately, as they may be during a study, researchers should not assume that the artists want their artworks or names included in publications. When there is a conflict between protecting participants' copyright and protecting participants' confidentiality, we recommend that the participants' wishes govern.

Confidentiality and Anonymity

Keeping data secure. Psychologists must maintain the confidentiality of research data (APA Ethics Code, section 4.01). For in-person paper-based studies, security and confidentiality are maintained by restricting access and separating identifying information. First, completed materials are personally transported by the researcher from the data collection site to a locked location (such as a lab), and only people who need these materials are given access. Second, if identifying information is collected, it is separated from other study materials. For example, signed

Table 5
Security of Test Materials

Essential	Essential for Some Online Studies	Additional Recommendations
Protect test integrity by reducing the exposure of test items.	If the researcher wants to use copyrighted tests in e-mail or Internet studies, ask copyright holders for permission to include tests and candidly discuss how tests will be administered and what security procedures will be used. If copyright holders place restrictions on the use of their tests, obey these restrictions.	We recommend that researchers use robots.txt or robots meta-tag to tell search engines not to list pages, and password protect their Web sites when this will not interfere with data collection. If researchers want to publish participants' artwork or creative work, we recommend that they ask permission and follow participants' wishes about publishing participants' names.

consent forms are separated from questionnaires. Identifying information from consent forms is rarely entered into the computer, and when it is, it is usually put in a file separate from the study data.

For online data collection, protecting confidentiality requires the same two steps, but these steps are implemented differently, because data are collected, transferred, and stored electronically. For each step, the required security measures vary on the basis of the data, as with paper-based data collection. If the study involves identifying information, greater security is needed than if the data are anonymous, and if the study collects sensitive information (e.g., criminal activities, opinions on moral issues), greater security is needed than if the data are innocuous. See Table 6 for a summary of our recommendations for confidentiality and anonymity.

The first step, restricting access, requires physical and electronic security of both the server used to collect the data and the computer to which the researcher downloads the data (usually the researcher's office computer). On the server, system administrators protect the physical and electronic security of the data. Physically, the server and its backups should be in an environment with access limited to authorized individuals. Electronically, system administrators should follow industry standards for protecting the electronic security of the servers. In addition, researchers must protect the security of the data on the server by prohibiting external access to unprotected files and directories. Data files should be password protected, and the folders that contain data files should contain index .html files to prevent participants (and others) from seeing listings of all the files (Reips, 2002a). Finally, researchers should consider choosing a server with an operating system that is less vulnerable to outside attacks (see Reips [2002a] for a comparison of operating system vulnerability). See University of New Hampshire Institutional Review Board for the Protection of Human Subjects in Research (2005) for a list of 10 questions to ask about server security.

On the researcher's computer, the researcher protects the physical and electronic security of the data. Physically, the computer and its backups should be kept in a secure location with limited access. Researchers must ensure that the computer itself is not stolen or accessed by unauthorized people, because passwords can often be broken and can be circumvented using a system recovery boot-disk on Windows operating systems (93.2% of Internet users are using Windows operating systems; The Counter, 2008). Electronically, researchers should maintain current virus protection, apply critical updates to operating systems and software, use a firewall, use good passwords, and avoid opening suspicious e-mail attachments. Researchers should give assistants access to only the specific files they need and should give them only the type of access they need. For additional advice about maintaining computer security, see the Carnegie Mellon University (2002) Web site. Advice about computers changes rapidly. Researchers should follow the security advice from their system administrators. In our opinion, these routine security procedures will be sufficient for online studies that do not collect sensitive information or identifying information. However, researchers should check with their local IRBs to ensure that these routine security procedures are sufficient.

Table 6
Confidentiality and Anonymity

Essential	Essential for Some Online Studies	Additional Recommendations
Restrict physical and electronic access to data on researcher's computer.	If violations of confidentiality could harm participants, warn participants about these threats.	If identifying information is collected, we recommend that researchers separate it from other study materials as soon as possible.
Restrict physical and electronic access to data on server.	If sensitive information is being collected using e-mail, ensure that participants use encrypted e-mail or warn participants about threats to confidentiality when using e-mail and offer an alternative method of participating.	If identifying information cannot be separated from sensitive information during data collection, we recommend that researchers encrypt the data during transfer from the participant's computer to the server and from the server to the researcher's computer.
Keep abreast of threats to computer security.		If identifying information cannot be separated from sensitive information once data collection is complete, we recommend that researchers keep the data in a locked location that is not Internet accessible.
Accurately tell participants whether data will be anonymous or not.		If it is essential to collect data that are likely to inspire hacking (e.g., social security numbers, credit card numbers), we recommend that researchers use the very highest data security standards.
Avoid collecting data that will inspire hacking, unless it is absolutely essential.		If sensitive information is being collected using computers that are used by multiple people, we recommend that researchers prevent page caching and avoid the "get" method of form submission.
		If some participants are likely to have poor computer skills and data are being collected by e-mail, we recommend that researchers warn participants about the threats to confidentiality when multiple people use the same e-mail account.

If identifying information is collected, the second step must also be taken: Identifying information should be separated from other study materials and stored in a different location. Identifying information, such as a name or e-mail address, may be needed to indicate consent, provide debriefing or payment, or assign credit. This information should be put in a separate database on the server, as discussed by Peden and Flashinski (2004) and Schmidt (1997), or for more protection, it can be placed on a separate server. The easiest method of doing this is to collect identifying information on a Web page separate from the main study materials, so that each Web page sends the data to a different database. Separate Web pages and databases can be implemented easily if the study is developed using any standard Web development program (see the top half of Table 1). When the identifying information is transferred to the researcher's computer, it should be put in a separate folder or removed from the hard drive entirely. If identifying information is kept separate from the study data, then if the data are accessed by someone without proper authority, the data themselves will at least be anonymous. In addition, if the sensitive data is made anonymous, colleagues and research assistants will not know the identity of the participants.

Identifying information might be present in online studies without researchers' realizing it. Combinations of variables can sometimes be used to identify individual participants, particularly if a study is limited to a small group of people (this has, in fact, occurred in studies run by each of the authors). For example, the combination of sex, age, and ethnicity might reveal the identity of some participants if a study uses employees of a single company or students in a single class. Even in large samples, combinations of variables can identify individuals. In August 2006, AOL posted the search queries of 657,000 customers on the Internet (Barbaro & Zeller, 2006). Although they replaced user names with numbers, these data were not entirely confidential. The *New York Times* was able to identify one Georgia woman on the basis of her search queries. In some cases, researchers can design their studies so that no combination of variables will identify participants. If this is not possible, these variables can be collected using separate Web pages and databases and can be combined with other data only after removal from the server.

Identifying information can also be present without a researcher's realizing it if Internet Protocol (IP) addresses are recorded. Whenever a computer connects to the Internet, it is assigned a unique IP address. Some online studies record IP addresses, and these can sometimes be used to identify individual computers and individual users (see, e.g., American Registry for Internet Numbers, 1997–2007). Furthermore, Internet service providers (ISPs) can often trace individual users by combining IP addresses with date and time, even when computers are assigned different IP addresses each time they connect to the Internet (e.g., dial-up connections and computer labs). Researchers should therefore check whether IP addresses are being recorded automatically in their data set. If IP addresses are being recorded but are not needed, researchers can at least delete them before saving the data on their own computer. Researchers also sometimes record IP addresses deliberately, to help control for multiple submissions or invalid submissions or to match data from the same participant over different Web pages. However, there are other ways of accomplishing the goals that IP addresses are used for, and researchers may sometimes prefer to make their studies completely anonymous.

If IP addresses are being recorded, we agree with Granello and Wheaton (2004) that researchers should not claim that their studies are completely anonymous. If the study does not collect any other identifying information, the participant might mistakenly perceive the study as completely anonymous, and so we recommend that the researcher explicitly state in the consent form that IP addresses are being collected and can sometimes be used to trace individual users. This is a controversial issue in online data collection, though: Many researchers argue that IP addresses in theory might be used to identify individuals but that this is quite difficult and in practice very unlikely. Nonetheless, warning participants about the possibility of being identified through their IP address might be particularly important if the participants are likely to use ISPs that are run by their workplaces and the study includes sensitive information regarding their work life.

In some cases, it may be impossible to separate identifying information from other data. Perhaps IP addresses are being collected automatically, or the data are inherently identifying (e.g., describe how your political career has impacted your family life). If the study contains sensitive information, researchers should take additional steps to protect confidentiality. What steps are needed will depend on when identifying information is joined to sensitive data. If identifying information is joined to sensitive data when data are first collected, the data need to be protected during the original data collection. One recommendation is to label items in a way that is meaningless to anyone but the researcher (Nosek et al., 2002). For example, a multiple-choice question can use options like

```
<input type="radio" name="Item3" value="b">
```

rather than

```
<input type="radio" name="How often have you
stolen a car?" value="More than once">.
```

However, because a data thief could reconstruct the data by looking at the items on the original Web page, this strategy is not sufficient. Instead, we recommend that data be encrypted for transmission from the participants' computer to the server, so that if data are intercepted, the content cannot be read (Kraut et al., 2004; Nosek et al., 2002). The most common encryption method is a secure sockets layer (SSL; VeriSign, 1995–2008). Make sure that your server allows an SSL if that level of protection is needed.

In addition, when identifying information is stored with sensitive information on the server, server security is essential. The institution whose server is being used should have a full-time specialist devoted to server security or should have contracted the services of such a specialist. These days, maintaining server security requires a computer se-

curity specialist, and we therefore do not recommend that researchers run their own servers if they will be collecting sensitive information that can be traced to participants. Researchers should instead use institutional servers that are well protected by security specialists or should embed their servers within a network that is protected by such specialists. Some researchers argue that thieves are not motivated to steal our research data and we therefore do not need specialists to ensure server security. We disagree. Just as we would not leave sensitive identifiable data sitting in the hallway where anyone could look at it, we should not leave such data on a server that is vulnerable to attacks from the Internet. Although thieves are unlikely to seek out our research data, computer hackers do routinely probe for vulnerabilities and are likely to gain access to servers that are not adequately protected. When sensitive information is connected to identifying information, researchers must do all they can to protect confidentiality.

If identifying information cannot be separated from sensitive data when data are being downloaded from the server and stored on the researcher's computer, two additional steps should be taken. First, data should be encrypted during transfer (e.g., by using Secure FTP [Taylor, 2002] or Kerberos [Massachusetts Institute of Technology, 2005]). If data are not encrypted, Stanton and Rogelberg (2001) recommended that researchers warn participants that the Internet is too uncontrolled to ensure confidentiality. Second, once data have been downloaded, identifying information should be separated from sensitive data. If this is impossible, data should be stored in a location that is not Internet accessible (e.g., a computer not connected to the Internet or a CD in a locked filing cabinet). If researchers cannot implement these security procedures, they should not collect sensitive identifiable data over the Internet; instead, they should collect the data in person, either on paper or on computers that are not connected to the Internet.

For some studies, even encrypted data transfers are not sufficient. Although most online studies are unlikely to inspire deliberate hacking attempts (Birnbaum, 2004b), some types of information are more sensitive than others and more likely to inspire hacking. In particular, social security numbers, credit card numbers, and passport numbers might be targeted for identity theft. Researchers should avoid collecting such information unless it is absolutely essential. For example, if social security numbers are used as employee or student numbers, researchers should try to identify participants without using these numbers. If it is essential that such information be collected in an online study (e.g., a study on credit ratings might need social security numbers), the very highest security standards should be used. At this time, the highest standards are those adopted by online banking services and are detailed in the Payment Card Industry (PCI) Data Security Standards. These standards were originally jointly developed by Visa and MasterCard and are now set by the PCI Security Standards Council (2008). These 12 standards address both server security (e.g., firewalls) and data use (e.g., limiting access to data) and include detailed implementation requirements.

Regardless of study content, security issues can also be raised by the data collection method. When several people use the same computer, this creates additional concerns about confidentiality. First, Web browsers often save Web pages, and these pages can contain participants' responses. If sensitive information is being collected, we recommend that researchers prevent page caching. See Birnbaum and Reips (2005) or Adobe (2008) for prevention methods. Second, browsers often save Web page addresses, and if data are submitted using the "get" method, participants' responses may be saved in the Web page address (see Reips, 2002a). We recommend that researchers avoid this method of submission. Third, businesses often have a legal right to review information stored on company computers. This would include cached pages, Web addresses, and business and personal e-mails. If answers could be damaging to participants if seen by their employer, researchers should warn participants about this threat to confidentiality and may want to suggest that they complete the study at home or use an alternative method of responding (e.g., print the questions and mail them).

Conducting online research via e-mail creates additional concerns regarding confidentiality, because most e-mails contain identifying information. When e-mails are sent from one server to another, they can be intercepted with relatively little technological skill. Encrypted e-mails and better security features by ISPs have reduced concerns regarding unauthorized reading of e-mails. However, many commonly used e-mail services (e.g., Gmail, GMX, Yahoo! Mail) do not use encryption (Tschabitscher, 2008). Therefore, if sensitive information is being collected in an e-mail study, we recommend that researchers either ensure that all respondents use encrypted e-mail (which may be possible if participants are preselected) or warn potential participants of this security issue and offer an alternative method of responding (e.g., use a Web page, or print and mail the survey). Even if encrypted e-mail is used, confidentiality issues still exist if multiple people use one e-mail account, because other people can see the sent mail (Frankel & Siang, 1999). If some participants may have poor computer skills and may be unaware of this issue, or if sensitive information is being collected, we recommend that researchers warn potential participants of this security issue and offer an alternative method of responding. Because encrypted e-mail is rare, e-mail studies should usually be avoided if confidentiality is a concern.

Computer hardware and software are ever-changing, and therefore, threats to confidentiality in online studies will continue to evolve. To ensure that researchers keep abreast of security threats, they can consult security standards developed in the broader computer industry. One helpful resource at this time is the Payment Card Industry (PCI) Data Security Standards (PCI Security Standards Council, 2008). Although researchers are not required to meet these standards and will not need to implement this level of security except in the most sensitive of studies (i.e., medical records with identifying information in an HIV-positive population), periodically consulting these or

later-developed industry guidelines will help researchers identify and address new security issues.

In this section, we have discussed security procedures that can be used to collect sensitive data. In our opinion, these additional procedures are not usually necessary if no sensitive information is being collected or if this information is not joined to identifying information. Many online studies are either completely anonymous or collect no sensitive information and so will not require any of these special procedures.

Establishing identity. To protect confidentiality, sometimes researchers must establish participants' identities. For example, researchers might want to access confidential data in another location (e.g., medical, financial, employee, or student records) or to quote participants in publications and so must ensure that they are receiving permission from the correct person. There are two ways to establish identity online. The first method is asking participants additional questions for which only they should know the answers. This method is often used for online and phone banking and can also be used in research. For example, the first author recently asked students for permission to access their official student records and asked the students to provide both their student numbers and their names. Because student numbers are confidential, when a participant knows Jane Smith's student number, this strongly suggests that the participant is Jane Smith.

The second method of establishing identity online is sending individualized invitations. The researcher can preselect potential participants, create a database that lists study IDs with contact information (probably e-mail addresses), and send invitations and IDs to potential participants. When data are received, researchers can compare the IDs with the database to ensure that they match. There are two variations on this approach. The manual method is simple but time consuming. The participants are told their ID and are asked to type it in, and the researcher checks the database to ensure that they match. The automated method is more elegant. IDs are embedded in links given in the e-mail invitations, so that the participants do not have to type them, and a computer program automatically checks IDs against the database. To automate invitations and matching, researchers must write programs that send and receive information from databases, using languages like PHP, ASP, or PERL. The automated method may be inconvenient for the first study, but once a researcher has learned one of these languages, this method may be relatively easy to implement in future studies.

Neither of these two methods of establishing identity is infallible. If this is critical, then in-person testing with proof of identification should be used. However, we believe that few psychological studies fall into this category.

Avoiding Harm

Psychologists must attempt to avoid and minimize harm to research participants (APA Ethics Code, section 3.04). Many risks can be anticipated and minimized (e.g., confidentiality, invasion of privacy, drug treatment side effects). However, it is difficult to determine whether research has harmed participants in unexpected ways when researchers have no direct contact with the participants, as is usually the case in online research. If the researcher believes that there is a significant possibility of unintended harm in a particular study if little or no direct contact occurs, we recommend that the researcher increase the amount of contact or consider conducting the research in person. For example, if researchers were worried that participants might make unwise financial decisions after participating in an online study involving a stock market simulation, the researchers could provide detailed debriefing, references to Web sites and books on financial issues, and follow-up e-mails or phone calls to the participants who are particularly at risk. See Table 7 for a summary of our recommendations for avoiding harm.

Some groups of people are more likely to be harmed than others, and additional steps should be used to protect their welfare. The Code of Federal Regulations [CFR 46.111(b)] defines the following as vulnerable populations: children, prisoners, pregnant women, and people who are mentally disabled or economically or educationally disadvantaged. We recommend that studies involving these groups have higher levels of contact so that unintended harm can be prevented and detected. Researchers should provide multiple methods of contact (e.g., phone or address, as well as e-mail) and should provide more information about potential risks. We also recommend that researchers pretest their study materials with people from the target population, to determine whether modifications are necessary to avoid unintended harm. Reips (2002b) recommends pretesting all studies to ensure clear instructions for all participants. Finally, if researchers believe that asking for informed consent may itself harm participants, they should refrain from conducting the study.

In addition, research involving people with mental disorders may need additional steps to avoid unintended harm. Although the Code of Federal Regulations does not identify people with mental disorders as a vulnerable population, recent in-person research shows that people with mental disorders are twice as likely to become anxious when answering questions regarding their mental and physical health and are four times more likely to perceive interview questions as invading their privacy (Boothroyd, 2000). These adverse reactions are more common when participants perceive consent procedures as inadequate (Boothroyd, 2000). Although participants may be less concerned about invasion of privacy in an online study, these risks may still be an issue. Therefore, if a study asks about symptoms of mental illness and may be completed by some participants with mental illnesses, we recommend that these risks be clearly described, and Boothroyd suggests that researchers include examples of sensitive questions in the consent form. In addition, researchers should address participants' emotional discomfort. Boothroyd gave participants a toll-free number to contact the researchers. Researchers can also tell participants how to obtain free mental health services, or they can provide qualified professionals who are available by phone or in an online chat room.

Table 7
Avoiding Harm

Essential	Essential for Some Online Studies	Additional Recommendations
Attempt to avoid or minimize harm to research participants.	If the research involves vulnerable populations (children, prisoners, pregnant women, people who are mentally disabled, or people who are economically or educationally disadvantaged), take extra steps to avoid unintended harm.	If participants are from vulnerable populations, we recommend that studies involve higher levels of contact; that researchers provide their phone number and address, as well as e-mail address; and that the consent form include more information about the potential risks of the study.
	If participants have mental illnesses and the study asks about symptoms of mental illness, address participants' emotional discomfort.	If participants are from vulnerable populations, we recommend pretesting with people from the target population.
		If participants have mental illnesses and the study asks about symptoms of mental illness, we recommend that the consent form warn participants that these questions will be asked and might cause anxiety or feelings that their privacy has been invaded.
		If the study is designed for people who are likely to have poor computer skills, we recommend that researchers minimize harm by following the recommendations under informed consent, the right to withdraw, confidentiality, and debriefing.
		If the study will be advertised openly on the Internet and interception of study materials or answers could result in severe social or legal consequences for some participants, we recommend that researchers forewarn potential participants about such content by using informative study titles and descriptions and provide detailed information regarding threats to confidentiality.

Because of the lack of direct contact in online studies, additional steps may also be needed when participants have poor computer skills. For most online studies, researchers can assume a certain level of competence with computers and the Internet. However, some people who use the Internet lack essential skills and knowledge (e.g., use of the back button, address bar, underlined links, and free e-mail accounts). If some people who will see the study advertisement are likely to lack these skills, researchers should consider modifying their study. We suggested possible modifications in the sections on informed consent, the right to withdraw, debriefing, and confidentiality. When deciding what modifications are needed, researchers should consider the type of participant (e.g., age, occupation), how participants are recruited (e.g., newspaper, Web site), and therefore what skills all the participants will have. For example, a researcher studying retirement transition for steel workers, using advertisements in the company newsletter, might not be able to safely assume that all potential participants have adequate Internet skills. If researchers modify the study to accommodate people with poor computer skills, they should pretest study materials with members of the target group who have poor computer skills, to determine whether the modifications were successful.

If an online study is widely advertised, researchers should consider whether their study poses additional risks for participants from other countries and cultures. Activities, words, and pictures that are mundane in the researcher's country may be distressing or illegal in the participant's country (e.g., abortion, marijuana use, euthanasia, prostitution, same-sex marriage). Even within North America, there are variations in what is legal and what is illegal from one state to another and from the United States to Canada. We recommend that researchers forewarn potential participants of such content by using informative study titles and descriptions. If interception of the material could result in severe social or legal consequences for some participants, researchers should provide detailed information regarding threats to confidentiality. In addition, researchers should keep in mind that concepts that are central to ethical issues (e.g., confidentiality, privacy) vary between different cultures (Ess, 2005); indeed, the fundamental approach that is taken to ethical issues (e.g., minimum required protections vs. cost–benefit analysis) also varies between cultures (Ess, 2007). We therefore strongly encourage researchers who use open advertisements to consult the recommendations of the Association of Internet Researchers regarding international issues (Ess & the Association of Internet Researchers, 2002).

FINAL THOUGHTS

In this article, we have emphasized the differences between online studies and in-person studies, by focusing on online studies in which participants have no direct contact with the researcher. However, in some cases, online studies are much more similar to in-person laboratory studies, because they have relatively high degrees of direct contact. For example, studies conducted through instant messaging or in a chat room have high degrees of contact, although most of the visual and auditory cues of an individually administered in-person study are still missing. Online studies can also be administered during individual in-person appointments, during which researchers show participants how to use the computer. In this situation,

although testing materials may be on the Internet, many ethical issues can be addressed in the same way as during in-person paper-based studies. Finally, as Internet video cameras become more common, research may use interactive video-and-audio sessions with participants around the world; distance education and distance medical services already take advantage of these technologies. When there is more contact between researchers and participants, there are fewer differences between online and in-person studies, and fewer differences in how to deal with ethical issues. Each study should be considered separately to determine how best to address each ethical issue.

Ongoing discussion of ethical issues in online research is critical for three reasons. First, legislation and guidelines are sometimes ambiguous when applied to these new data collection environments, so that it is not clear how studies should be designed and implemented. By discussing these issues, researchers can clarify how to interpret and implement ethical principles. Second, new ethical issues will arise, because researchers will begin collecting data in environments that do not exist today and because changes in technology will create new risks in existing environments. Researchers will need to develop strategies for these new data collection environments. Third, participants will change. Over the next decade or two, the composition of Internet users may change drastically as computers become less expensive and more common in areas where they are currently limited. For these three reasons, it is critical that online researchers and IRB members discuss ethical issues with each other and continue to discuss the steps needed to conduct ethical research in these changing environments. We welcome feedback, comments, and dialogue on these issues.

AUTHOR NOTE

We thank Glen Scott of IBM and Michael Shutt of UNLV computing services for suggestions regarding technical issues. We also thank the following psychologists and online researchers for their comments on earlier drafts of the manuscript: Daniel Allen, UNLV; Alexis Kennedy, UNLV; Paul G. Stiles, University of South Florida; and several anonymous reviewers. Correspondence concerning this article should be addressed to K. A. Barchard, Department of Psychology, University of Nevada, P.O. Box 455030, 4505 S. Maryland Parkway, Las Vegas, NV 89154-5030 (e-mail: kim.barchard@unlv.edu).

REFERENCES

Adobe (2008). *How to prevent caching of swf files.* Retrieved September 29, 2008, from www.adobe.com/go/tn_14743.

American Bar Association (2005). *Digital signature guidelines tutorial.* Retrieved September 29, 2008, from www.abanet.org/scitech/ec/isc/dsg-tutorial.html.

American Psychological Association (2002). Ethical principles of psychologists and code of conduct. *American Psychologist*, **57**, 1060-1073.

American Registry for Internet Numbers (1997-2007). *ARIN WHOIS database search.* Retrieved September 29, 2008, from ws.arin.net/whois.

Andrew, R., Foley, R., McLellan, D., & Turnbull, R. (2004). *ASP Web development with Macromedia Dreamweaver MX 2004*. London: Apress.

Barbaro, M., & Zeller, T., Jr. (2006, August 9). A face is exposed for AOL Searcher No. 4417749. *New York Times*.

Barchard, K. A., & Pace, L. A. (in press). Evaluating the effectiveness of collaborative computer-intensive projects. *Interactive Learning Environments*.

Birnbaum, M. H. (2004a). Human research and data collection via the Internet. *Annual Review of Psychology*, **55**, 803-832.

Birnbaum, M. H. (2004b). Methodological and ethical issues in conducting social psychology research via the Internet. In C. Sansone, C. C. Morf, & A. T. Panter (Eds.), *Handbook of methods in social psychology* (pp. 359-382). Thousand Oaks, CA: Sage.

Birnbaum, M. H., & Reips, U.-D. (2005). Behavioral research and data collection via the Internet. In R. W. Proctor & K.-P. L. Vu (Eds.), *The handbook of human factors in Web design* (pp. 471-492). Mahwah, NJ: Erlbaum.

Boothroyd, R. A. (2000). The impact of research participation on adults with severe mental illness. *Mental Health Services Research*, **2**, 213-222.

Buchanan, T., Johnson, J. A., & Goldberg, L. E. (2005). Implementing a five-factor personality inventory for use on the Internet. *European Journal of Psychological Assessment*, **21**, 115-127.

Burns, J. (2008). *New window: No title bar.* Retrieved September 29, 2008, from www.htmlgoodies.com/beyond/javascript/article.php/3471181.

Byrom, J., & Medway, D. (2004). Cyber solutions to remote problems? Online trading in British overseas territories—A review and research agenda. *International Review of Retail, Distribution, & Consumer Research*, **14**, 71-82.

Carnegie Mellon University (2002). *Home computer security.* Retrieved September 29, 2008, from www.cert.org/homeusers/HomeComputerSecurity/.

Code of Federal Regulations, Part 46: Protection of Human Subjects of 2001, 45 U.S.C.A. §46. Retrieved September 29, 2008, from www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm.

Coomber, R. (1997). Using the Internet for survey research. *Sociological Research Online*, **2**. Retrieved September 29, 2008, from www.socresonline.org.uk/2/2/coomber.htm.

Copyright Law of the United States of America of 2003, U.S.C.A. §106 *et seq*. Retrieved September 29, 2008, from www.copyright.gov/title17/circ92.pdf.

The Counter (2008). *Statistics for March, 2008*. Retrieved September 29, 2008, from www.thecounter.com/stats/.

Curran, K., Walters, N., & Robinson, D. (2007). Investigating the problems faced by older adults and people with disabilities in online environments. *Behaviour & Information Technology*, **26**, 447-453.

Dickinson, A., Arnott, R., & Prior, S. (2007). Methods for human–computer interaction research with older people. *Behaviour & Information Technology*, **26**, 343-352.

Electronic Signatures in Global and National Commerce Act (2000). 15 U.S.C.A. §101. Retrieved September 29, 2008, from frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf.

Ess, C. (2002). Introduction: Special issue on Internet research ethics. *Ethics & Information Technology*, **4**, 177-188.

Ess, C. (2005). "Lost in translation"?: Intercultural dialogues on privacy and information ethics. *Ethics & Information Technology*, **7**, 1-6.

Ess, C. (2007). Internet research ethics. In A. Joinson, K. McKenna, T. Postmes, & U.-D. Reips (Eds.), *The Oxford handbook of Internet psychology* (pp. 487-502). Oxford: Oxford University Press.

Ess, C., & the Association of Internet Researchers (2002). *Ethical decision-making and Internet research: Recommendations from the aoir ethics working committee.* Retrieved September 29, 2008, from aoir.org/reports/ethics.pdf.

Eysenbach, G., & Till, J. (2001). Information in practice: Ethical issues in qualitative research on Internet communities. *British Medical Journal*, **323**, 1103-1105.

Flicker, S., Haans, D., & Skinner, H. (2004). Ethical dilemmas in research on Internet communities. *Qualitative Health Research*, **14**, 124-134.

Frankel, M. S., & Siang, S. (1999). *Ethical and legal aspects of human subjects research on the Internet.* Washington, DC: American Association for the Advancement of Science.

Frick, A., Bächtiger, M.-T., & Reips, U.-D. (2001). Financial incen-

tives, personal information and dropout in online studies. In U.-D. Reips & M. Bošnjak (Eds.), *Dimensions of Internet science* (pp. 209-219). Lengerich, Germany: Pabst.

FRICKER, R. D., & SCHONLAU, M. (2002). Advantages and disadvantages of Internet research surveys: Evidence from the literature. *Field Methods*, **14**, 347-367.

GLASER, J., DIXIT, J., & GREEN, D. P. (2002). Studying hate crimes with the Internet: What makes racists advocate racial violence? *Journal of Social Issues*, **58**, 177-193.

GÖRITZ, A. S. (2006). The induction of mood via the WWW. *Motivation & Emotion*, **31**, 35-47.

GRANELLO, D. H., & WHEATON, J. E. (2004). Online data collection: Strategies for research. *Journal of Counseling & Development*, **82**, 387-393.

HANOVER COLLEGE (2008). *Psychological research on the net.* Retrieved September 29, 2008, from psych.hanover.edu/research/exponnet.html.

JAVASCRIPT KIT (1997-2008). *Windows and JavaScript.* Retrieved September 29, 2008, from www.javascriptkit.com/javatutors/window1.shtml.

KAPLOWITZ, M. D., HADLOCK, T. D., & LEVINE, R. (2004). A comparison of Web and mail survey response rates. *Public Opinion Quarterly*, **68**, 94-101.

KOSTER, M. (2008). *A standard for robot exclusion.* Retrieved September 29, 2008, from www.robotstxt.org/wc/norobots.html.

KRANTZ, J. H., & DALAL, R. (2000). Validity of Web-based psychological research. In M. H. Birnbaum (Ed.), *Psychological experiments on the Internet* (pp. 35-60). San Diego: Academic Press.

KRAUT, R., OLSON, J., BANAJI, M., BRUCKMAN, A., COHEN, J., & COUPER, M. (2004). Psychological research online: Report of board of scientific affairs' advisory group on the conduct of research on the Internet. *American Psychologist*, **59**, 105-117.

MANGAN, M. A., & REIPS, U.-D. (2007). Sleep, sex, and the Web: Surveying the difficult-to-reach clinical population suffering from sexsomnia. *Behavior Research Methods*, **39**, 233-236.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY (2005). *Kerberos: The network authentication protocol.* Retrieved September 29, 2008, from web.mit.edu/kerberos/.

MATHY, R. M., KERR, D. L., & HAYDIN, B. M. (2003). Methodological rigor and ethical considerations in Internet-mediated research. *Psychotherapy: Theory, Research, Practice, Training*, **40**, 77-85.

MCCABE, S. E. (2004). Comparison of Web and mail surveys in collecting illicit drug use data: A randomized experiment. *Journal of Drug Education*, **34**, 61-72.

MEYERSON, P., & TRYON, W. W. (2003). Validating Internet research: A test of the psychometric equivalence of Internet and in-person samples. *Behavior Research Methods, Instruments, & Computers*, **35**, 614-620.

MUSCH, J., & REIPS, U.-D. (2000). A brief history of Web experimenting. In M. H. Birnbaum (Ed.), *Psychological experiments on the Internet* (pp. 61-87). San Diego: Academic Press.

NATIONAL BIOETHICS ADVISORY COMMISSION (1998). *Research involving persons with mental disorders that may affect decisionmaking capacity.* Retrieved September 29, 2008, from bioethics.georgetown.edu/nbac/capacity/TOC.htm.

NOSEK, B. A., BANAJI, M. R., & GREENWALD, A. G. (2002). eResearch: Ethics, security, design, and control in psychological research on the Internet. *Journal of Social Issues*, **58**, 161-176.

PACE, L. A., & LIVINGSTON, M. M. (2005). Protecting human subjects in Internet research. *Electronic Journal of Business Ethics & Organizational Studies*, **10**, 35-41.

PCI SECURITY STANDARDS COUNCIL (2008). *Payment card industry (PCI) data security standard, version 1.1.* Retrieved September 29, 2008, from www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

PEDEN, B. F., & FLASHINSKI, D. P. (2004). Virtual research ethics: A content analysis of surveys and experiments online. In E. A. Buchanan (Ed.), *Readings in virtual research ethics: Issues and controversies* (pp. 1-26). Hershey, PA: Information Science Publishing.

PHD SOFTWARE SYSTEMS (1996-2002). *Robots.txt tutorial*. Retrieved September 29, 2008, from www.santarosa.edu/~dpearson/mirrored_pages/SearchEngineWorld.com/robots_tutorial.htm.

REIPS, U.-D. (1995-2008). *The Web experimental psychology lab*. Retrieved September 29, 2008, from www.psychologie.unizh.ch/sowi/Ulf/Lab /WebExpPsyLab.html.

REIPS, U.-D. (1997). Das psychologische experimentieren im Internet [Psychological experimenting on the Internet]. In B. Batinic (Ed.), *Internet für Psychologen* (pp. 245-265). Göttingen: Hogrefe.

REIPS, U.-D. (1999). Online research with children. In U.-D. Reips, B. Batinic, W. Bandilla, M. Bosnjak, L. Gräf, K. Moser, & A. Werner (Eds.), *Current Internet science: Trends, techniques, results.* Zürich: Online Press.

REIPS, U.-D. (2000). The Web experiment method: Advantages, disadvantages, and solutions. In M. H. Birnbaum (Ed.), *Psychological experiments on the Internet* (pp. 89-117). San Diego: Academic Press.

REIPS, U.-D. (2001-2008). *The Web experiment list.* Retrieved September 29, 2008, from genpsylab-wexlist.unizh.ch/.

REIPS, U.-D. (2002a). Internet-based psychological experimenting: Five dos and five don'ts. *Social Science Computer Review*, **20**, 241-249.

REIPS, U.-D. (2002b). Standards for Internet-based experimenting. *Experimental Psychology*, **49**, 243-256.

ROBERTS, L. W., & ROBERTS, B. (1999). Psychiatric research ethics: An overview of evolving guidelines and current ethical dilemmas in the study of mental illness. *Biological Psychiatry*, **46**, 1025-1038.

SCHMIDT, W. C. (1997). World-Wide Web survey research: Benefits, potential problems, and solutions. *Behavior Research Methods, Instruments, & Computers*, **29**, 274-279.

SOCIAL PSYCHOLOGY NETWORK (1996-2008). *Online social psychology studies.* Retrieved September 29, 2008, from www.socialpsychology.org/expts.htm.

STANTON, J. M., & ROGELBERG, S. G. (2001). Using Internet/Intranet Web pages to collect organizational research data. *Organizational Research Methods*, **4**, 200-217.

TAYLOR, L. (2002). *Secure FTP 101*. Retrieved September 29, 2008, from www.intranetjournal.com/articles/200208/se_08_14_02a.html.

TSCHABITSCHER, H. (2008). *Top 16 free email services.* Retrieved September 29, 2008, from email.about.com/cs/freeemailreviews/tp/free_email.htm.

UNIVERSITY OF MISSISSIPPI (2000). *PsychExperiments: Psychology experiments on the Internet*. Available at psychexps.olemiss.edu/.

UNIVERSITY OF NEW HAMPSHIRE INSTITUTIONAL REVIEW BOARD FOR THE PROTECTION OF HUMAN SUBJECTS IN RESEARCH (2005). *Guidelines for conducting Web-based survey research*. Retrieved September 29, 2008, from www.unh.edu/osr/compliance/support/internet_research.pdf.

VERISIGN (1995-2008). *SSL information center.* Retrieved September 29, 2008, from www.verisign.com/ssl/ssl-information-center/index.html.

WALSTROM, M. K. (2004). Ethics and engagement in communication scholarship: Analyzing public, online support groups as researcher/participant-experiencer. In E. A. Buchanan (Ed.), *Readings in virtual research ethics: Issues and controversies* (pp. 174-202). Hershey, PA: Information Science Publishers.

WEB CONTENT ACCESSIBILITY GUIDELINES WORKING GROUP (1994-2007). *How to meet WCAG 2.0: A customizable list of WCAG 2.0 requirements (success criteria) and techniques* [Draft]. Retrieved September 29, 2008, from www.w3.org/WAI/WCAG20/quickref/.

WOOD, R. T. A., GRIFFITHS, M. D., & EATOUGH, V. (2004). Online data collection from video game players: Methodological issues. *CyberPsychology & Behavior*, **7**, 511-518.

YOUD, D. (1996). *What is a digital signature? An introduction to digital signatures.* Retrieved September 29, 2008, from www.youdzone.com/signature.html.

(Manuscript received August 21, 2007;
revision accepted for publication March 27, 2008.)