Empirical Software Engineering, 6, 329–341, 2001.

Protecting Research Subjects, Employees and Researchers: Implications for Software Engineering

JOAN E. SIEBER* jsieber@csuhayward.edu
California State University, Hayward, CA 94542, USA

"What's the big deal? They're not doing lobotomies."
– the author's officemate

Abstract. Human subjects research entails risks for subjects and, to a lesser extent, for researchers. This paper introduces the common types of risks to subjects of empirical software engineering research, and how risk can be a function of the context in which the research is conducted. Risks for researchers are also discussed. Government regulation of the ethics of human subjects research is introduced using the example of the Common Rule that governs much human subjects research taking place in the United States.

Keywords: Empirical software engineering, human subjects research, intellectual property, research risks, Common Rule

1. Introduction

Empirical software engineering research using human subjects is not very risky, but neither is it risk-free. If ethics is not considered in the planning and conduct of the research, harm can come to many of the stakeholders involved. For example harm can come to:

- Individuals, companies, and researchers from academia if their intellectual property is not protected.
- Software engineers who participate or choose not to participate in research.
- Students who are asked to serve as subjects.

This paper begins by introducing the types of risks and vulnerabilities involved in empirical software engineering research using human subjects. Following this section, the types of subjects most commonly used in empirical software engineering studies are identified and the types of harm that can occur to them are illustrated. The regulation of human subjects research is illustrated by reviewing the main ele-

*From September 2001 to November 2001, Joan Sieber will be serving as Program Director of Societal Dimensions of Engineering, Science and Technology in the Division of Social and Economic Sciences. Email: jsieber@nsf.gov

ments of the United States' Common Rule. US federal regulations also mandate that Institutional Review Boards (IRBs) oversee researchers' compliance with the Common Rule. IRBs require researchers to submit a protocol describing the ethical issues raised by their research and how the researchers plan to deal with those issues. The IRB reviews this protocol to determine whether the proposed research complies with the Common Rule. Both the structure and function of IRBs and the typical content of a research protocol are discussed.

2. Risks, Contexts and Vulnerabilities

There are various kinds of risks involved in research. Moreover, particular situations are risky in relation to the context and to the particular vulnerabilities of the subjects involved. Understanding the relationship of risk and vulnerability to context is crucial both to identifying risk and to ameliorating or preventing it. For example, analysis of open source, per se, is not risky, nor is having one's open source analyzed, per se, risky. Persons become vulnerable in relation to specific contexts. A slight change in context or procedure can reduce or eliminate risk, as when the authors of open source are given an opportunity to decline to have their source code examined.

Risk refers to the possibility of some harm, loss, or damage. The main forms of risk in research are described below, though not exhaustively. Any new technology, research question or context might bring with it new risks. Nonetheless, an examination of some of the typical risks connected with research will begin to sensitize empirical software engineering researchers to some of the kinds of ethical issues they will need to recognize and resolve. To facilitate this recognition, the relevance of each type of risk to empirical studies of software engineering is highlighted.

Inconvenience, such as boredom, frustration, and wasting of time that the subject would prefer to spend otherwise. In the case of software engineers serving as research subjects, note that wasting their time constitutes an expense for their employer. In the case of classroom studies, consider that students have paid a substantial sum of money to receive an education. For students, also, a waste of time constitutes a waste of money.

Psychological risk, such as worry about criticism of one's work, loss of reputation, embarrassment, breach of confidentiality. The possibility of the perceived risky event is worrisome to the subject even if the probability of its occurrence is actually slim or non-existent. People are often uncomfortable about being observed or interviewed and often feel that they are not only being observed but also being evaluated. In workplace studies, employees may fear that there is a hidden agenda motivating the study. Such fear would cause stress to study participants. In classroom studies, students may worry about whether and how their participation (or non-participation) in the experiment will affect their grade.

Social risk, such as disapproval by one's peers, or stigmatization because of information that was revealed. This can arise more readily in workplace studies since the subjects and their co-workers will often know each other and will sometimes provide information about each other's professional conduct. For example, employees may disclose that the processes they follow deviate from those mandated by company policy.

Economic risk, such as loss of intellectual property, loss of employment, loss of opportunities for professional advancement, or loss of revenue. In workplace studies, there is a chance that managers would use information gleaned to make decisions about individual employees. Therefore, loss of employment or advancement constitutes a significant risk for subjects taking part in workplace studies. Students participating in classroom studies risk not receiving an adequate education. For example, they may be forced to use an experimental software engineering toolkit developed by a professor, rather than an industry standard toolkit. The lack of knowledge of, and experience with the industry standard toolkit can adversely affect the student's employment opportunities. A company may lose revenue or intellectual property rights as a result of a study's publication. For example, a metrics paper discussing the relationship between bugs and programming experience could be exploited by a competitor to malign the source code of the company that hosted the study. This could result in loss of revenue for that company.

Legal risk, such as a lawsuit or subpoena of data. There are several forms of legal risk in empirical studies of software engineering, though the rate of occurrence of legal problems seems quite low. Researchers assume some legal risk if they exaggerate their capabilities or those of their technologies. Researchers could also face legal action if their study somehow harms the company or individuals, as described above. If a company under study produced a system that ultimately resulted in injuries, the researcher's data may be subpoenaed to determine, for example, whether the company was following and applying all the relevant standards.

Physical risk, such as injury, is unlikely to result from empirical software engineering research.

The *context* that is critical to creating most of these risks is lack of *autonomy* of subjects. *Autonomy* means ability to control one's own fate, make one's own decisions, or protect one's own interests. To function autonomously, subjects need to be told "what they are getting into," i.e., what is going to happen, what risks may arise, etc. if they decide to participate in the research. When subjects are not properly informed of the nature of the research and of the risks it poses to them, they lack the necessary information to make appropriate autonomous decisions. For example, if the performance of employee subjects will be videotaped and later shown to managers or at a conference, subjects need to know that information about them will be disseminated before they agree, or decline, to participate in the research.

Risks or harms will also arise from invasion of privacy or from breach of confidentiality. Moreover, in empirical studies of software engineering, harm can often

involve loss of intellectual property. Consequently, it is useful to researchers to have a clear understanding of the concepts of *privacy*, *confidentiality* and *intellectual property*. Although these are common words in the vocabulary of most readers, their exact meaning is remarkably obscure.

Privacy refers to a person's (or a company's) interest in controlling the access of others to oneself. People do not necessarily wish to be left alone, but they do want to control the conditions under which others examine their behavior and attitudes. Privacy is protected in the research context partly by informed consent—voluntary, non-coerced consent for a researcher to obtain information about oneself.

Confidentiality refers to data (not to persons) and to agreements between the researcher and the subject concerning how the data will be managed and who will have access to it. Such agreements typically are part of the informed consent. The agreement is not necessarily that the data will not be disclosed but will instead specify the conditions and perhaps the means of disclosure.

Intellectual property is valuable knowledge that a person or company has produced. Like other forms of property, it may be protected by law, via non-disclosure agreements. Legal risk is incurred by both the researcher and subjects if they do not take the hosting company's intellectual property interests into consideration. Before intellectual property is developed to a point where it is protected by a patent or copyright, the owner of the property must take steps to demonstrate that it is private property which others may not disclose or use. If a competitor steals intellectual property and produces a patented product before the legitimate owner can do so, the legitimate owner could successfully sue by proving that all reasonable steps were taken to protect the property from disclosure. For this reason, when private intellectual property is revealed to a researcher or to participants in the context of research, the researcher or subjects should sign a non-disclosure agreement.

Researchers from academia may also own intellectual property. For example many empirical software engineering researchers develop software engineering tools. The researchers introducing these tools in a company for a field test place their intellectual property at risk if they do not obtain non-disclosure agreements from the company and the subjects. Similarly, researchers should obtain non-disclosure agreements from student subjects or colleagues who are asked to try out or review tools.

A non-disclosure agreement used in research might be as follows:

> During this study, you will work with an unannounced product. The information you acquire relating to this product, including but not limited to the appearance, nature and function of the product, is the confidential information of [intellectual property owner]. This proprietary information is disclosed to you only for purposes of your participation in this study, and you may not use it for any other purpose or disclose it to anyone. Because this agreement does not protect your ideas, please do not disclose confidential or proprietary information belonging to you or any other party.

At issue is not whether a researcher or a subject is likely to use the information for commercial purposes, but whether all reasonable steps have been taken to protect the intellectual property, in case a lawsuit should arise.

Typically, employees have already signed a blanket non-disclosure statement at the time of employment; hence employee-subjects need not sign an additional non-disclosure agreement to protect the employer's intellectual property. However, researchers developing a tool or methodology that they wish to protect will need to have their subjects sign a non-disclosure agreement.

Vulnerability is contextual. For example, a poor graduate student would not be vulnerable, and in fact would be quite fortunate, if offered a considerable amount of money to answer a simple survey or to test safe equipment. On the other hand, the same graduate student would be vulnerable if offered a large sum of money to test dangerous equipment. Thus, vulnerability should not be thought of as residing in the person alone, but in the person in relation to the particular research context. Several kinds of vulnerability in certain research contexts are as follows.

Subordination—being under the authority of another. Superiors should not recruit research subjects who are their employees, as their own employees cannot easily decline to participate. In addition, professors should not recruit their own students as subjects. They can have someone else recruit them, as long as the student's decision to participate remains confidential. Alternatively, professors can recruit students from another professor's class. Care must be taken to assure employees and students that no one expects them to participate—that they should do exactly as they wish with no overriding sense of obligation. They should be further assured that their decision to participate or not occurs outside of the scrutiny of others.

Vulnerability to inducements—taking unwanted risks in order to obtain a reward. Inducements (e.g. payment, gifts) can be provided as long as they do not constitute an excessive benefit. Whether a benefit is excessive or not depends on the normal range of benefits accessible to the subject. Consequently, researchers are unlikely to be able to offer any excessive benefit to software engineers. Students should not be offered inducements so great that they become willing to take risks that they would otherwise refuse to take.

Organizational vulnerability—belonging to a group that may place one at risk when one participates in research. Software engineers are at risk of revealing industrial secrets.

3. Research Subjects

At this point, the reader may be asking "Who or what counts as a research subject in *this* discussion of research risk and vulnerability?" The more usual notion of a subject is someone with whom the researcher interacts. Here we examine issues connected with two kinds of subjects with whom the researcher might interact: employees and students.

3.1. Employees as Subjects

Employees are particularly vulnerable subjects since they are typically part of a small community where significant psychological, social and economic damage could result from information they disclose in the course of research. Hence it is important that all research using employees as participants obtain their informed consent. The consent process should:

- Caution the employee to avoid volunteering sensitive information of an incidental nature.
- Describe how the data will be analyzed and presented, e.g., to the project, the company, or to outsiders.
- Indicate the extent to which the information will be reused for different research purposes or shared with others.

Subjects must explicitly consent to the presentation of data, including videotapes of subject performance on prototypes or in interviews, at conferences or to collaborators. This detail concerning use or dissemination should be included in the consent statement. Unless there is explicit agreement that the data may be shown to others, researchers should ensure the confidentiality of employee data by removing all unique identifiers if possible, storing the data under lock and key, and destroying the raw data after it is no longer needed.

Approaches to recruitment are particularly sensitive. When co-workers or supervisors directly recruit employee-subjects it may be difficult or embarrassing to decline to participate. When subjects are needed from among employees, it is advisable for a general announcement to be issued via company e-mail or mailboxes or at a company meeting, so that no one feels pressure to participate.

Collection of sensitive data and use of deceptive research methods are particularly problematic when researchers use colleagues as research subjects, or when researchers from academia have long-term relationships with employees of a host company—a relationship that extends beyond a single study. The effects on subsequent interactions with colleagues and employees should be considered. Of particular concern is the importance of keeping research information private from the company's or university's Human Resources Department. No research data should be used for administrative purposes to which the subject has not consented.

3.2. Students as Subjects

Similar issues arise when students are research subjects because, like employees, students are subordinates. The student's vulnerability arises from their relationship to the professor who has control over their grades. Consequently, students will often feel pressure to participate in their professor's research even if they are assured that

participation is voluntary. To reduce this pressure, researchers can employ recruitment and experimental procedures that preserve the student-subject's anonymity, such as making a general announcement via e-mail, and having graduate students, rather than the professor, interact with the students.

Reciprocity exists in all human relationships irrespective of whether the initiator considers it. The researcher who respects the privacy and autonomy of potential student-subjects will receive thoughtful and respectful research participation in return. Valid data with little error variance will be obtained. The respect that is shown through non-coercive recruitment and informed consent procedures, considerate scheduling of research participation, and thoughtful, useful feedback and discussion will be reciprocated in other ways as well. For example, students will communicate to one another what an interesting and positive experience it was to participate in the professor's research. By the same token, students who feel exploited may express their disdain,through thoughtless or even spiteful responses in the research setting, and through negative comments to peers about the exploitative actions of their professor.

4. Government Regulation of Human Subjects Research

Many of the ideas discussed so far are part of the human research regulations of many countries. In this final section, we examine the regulations governing human subjects research in the United States. This section briefly describes the origin and elements of the Common Rule, and describes the functioning of IRBs which are mandated to review research proposals to ensure that the ethical dimension of the research has been properly considered, consistent with federal requirements.

4.1. The Common Rule

During the last two decades, various United States federal agencies (e.g., Department of Education, Department of Justice) developed their own regulations of human research, some basic parts of which resembled, but differed slightly from, Department of Health and Human Services (DHHS) basic regulations. To achieve greater regulatory uniformity, the federal government recently brought all 17 of its departments[1] under the basic part (45 CFR 46, Subpart A) of DHHS's regulations, which became known as the Common Rule. Software companies seeking federal funding (e.g., from the National Science Foundation) are also subject to the Common Rule governing research on humans.

The Common Rule is an imperfect and evolving document. When 45 CFR 46, Subpart A was originally drafted in the early 1970s, it was directed primarily at biomedical research. Social and behavioral scientists, and especially cultural anthropologists and oral historians have continually complained that these regulations are a poor fit with their research. Not surprisingly, IRBs that evaluate social and

behavioral research sometimes must engage in creative interpretation of the regulations in order to evaluate social/behavioral protocols in a reasonable way. This creates difficulty and concern for IRBs, as they are charged with following the regulations, and their institutions are subject to sanctions for violations.

The full text of the Common Rule can be found at http://ohrp.osophs.dhhs.gov/. The item 'OHRP Policy and Assurances Page' leads to 'Regulations: 45 CFR 46' of which Part A is the Common Rule. It is recommended that the reader scan the Common Rule, print it out, and file it away for future reference. Since it is written in regulatory legalese, its main parts are rephrased here in more user-friendly language.

The Common Rule sets forth minimal requirements. Individual IRBs may require more, but not less. Researchers should contact their own IRB to find out its requirements and procedures. Typically IRBs welcome inquiries by researchers who are in doubt about whether the activity they plan to undertake is considered research and requires IRB review.

The Common Rule describes how an IRB is set up in compliance with federal law, when and how an IRB may expedite review of a protocol (e.g., have it reviewed by one or two experienced IRB members rather than the whole committee), what records the IRB must keep, and various other matters described subsequently herein. First, however, we turn to what a researcher submits to the IRB, namely the research protocol, including the informed consent procedure. All researchers receiving funding from these agencies must comply with the common rule or risk losing their funding. Understandably, empirical software engineering researchers may have concerns about how to interpret the regulations to fit their particular research circumstances. The biomedical, social and behavioral sciences have faced similar questions, as they have expanded their research to new kinds of problems. Their venues for answering such questions may be of interest to empirical software engineering researchers.

Questions concerning the regulations and suggestions for interpreting them to fit one's research may be addressed to a variety of sources. If the problem is a simple one that other, more experienced IRBs or researchers have solved, it might be raised via the IRB discussion group (McWirb) to which one may subscribe, by e-mailing mcwirb@mcwirb.org. There, one learns how others have reasoned about such problems, and handled similar issues. McWirb is a forum for disagreements as well as for problem solving, however most of its subscribers are not attuned to the kinds of issues confronting empirical software engineering researchers. Consequently, it would be prudent for software engineers to develop a separate discussion group to deal with issues unique to their research. They might then seek confirmation from McWirb and from the Office for Human Research Protection at http://ohrp.osophs.dhhs.gov/ about the adequacy of the solutions they have crafted.

4.2. The Research Protocol

The research protocol is the official account, submitted by the researcher to the IRB, stating the intended research methods and procedures. At minimum, it includes a

brief discussion of the research problem and hypotheses, how benefit is maximized and risk minimized, how autonomy (i.e., freedom to decide for oneself) of subjects is respected, and how informed consent is obtained. The wise researcher regards it as a planning tool (like a research proposal), rather than as last minute paper work. Researchers who are in doubt about appropriate ways to protect human subjects might submit a draft of their protocol to the IRB or to an individual IRB member to solicit suggestions or assistance.

If the project is simple and involves little risk, the protocol might consist of a one- or two-page statement and a consent form. The following description of the research protocol is based on the assumption that empirical software studies will tend to be simple and low risk. More complex studies would require more detailed protocols providing more information about both the researcher the nature of the risks involved, and the protections of subjects that will be employed; see Sieber (1992) or the IRB Handbook at http://ohrp.osophs.dhhs.gov/ for information appropriate to more complex research.

The protocol might consist of the following elements:

A cover sheet that includes the principal investigator's name, phone number or e-mail address, and the projects' intended starting and ending dates.

A description of the research, including the purpose, method, design, and location of the research, and written permission of the person in charge of the location, if appropriate.

The number and nature of subjects to be studied (e.g., employees, community members, students, and, where relevant, their age, gender, or other special characteristics that form the basis of subject selection).

A description of possible risks (e.g., inconvenience or discomforts, invasion of privacy, disclosure of confidential information, financial risk) and steps that will be taken to reduce or minimize risks.

A description of inducements or benefits to subjects. For example, will subjects be paid, or student-subjects be given credit?

Freedom of subjects to withdraw with impunity at any time is a right that must be respected. If the subject is not free to withdraw at any time, the protocol should explain why and state how autonomy is respected in the situation. For example, in a group research setting, it would greatly inconvenience other subjects and the researcher if one individual were to withdraw in the midst of a group discussion, but subjects wishing to remain silent on some issues should be free to do so.

An analysis of risks and benefits, if relevant, reveals whether risks are offset by the benefits that the research is designed to produce.

A description of the informed consent procedure should include how, where and by whom it is negotiated and how subjects will be debriefed. A copy of the informed consent statement should be appended to the protocol.

Relevant additional information, such as the consent form, any letters of permission, and interview or survey questions should be appended to the protocol. There may be relevant information that cannot be attached to the protocol, such as the experimental apparatus. One or more of the IRB members might examine the equipment or laboratory setup if that seems relevant to the IRB's understanding and evaluation of the project.

4.3. The Informed Consent

Informed consent means both (a) a specific agreement (often in written form) about the conditions of the research participation, and (b) on-going two-way communication between the researcher and subject[2] in which the subject is always free to raise questions or ask for clarification. The agreement must be *voluntary*, without threat or undue inducement. *Informed* means that the subject knows what a reasonable person in the same situation would want to know before consenting. *Consent* means explicit agreement. The University of Minnesota http://www.research.umn.edu/consent/ offers an excellent, self-programmed tutorial that teaches what is required in an informed consent document and includes quizzes to check understanding.

Informed consent requires clear communication—not legal jargon or technical detail. A written and signed consent form is usually employed. However, it is widely recognized that the most important part of the communication—the part that matters to subjects—is the researcher's *oral* communication with the subject. It behooves the researcher to communicate the elements of consent, orally, to the subject and to engage in open give and take in response to any questions or comments the subject may have. As any perceptive researcher will attest, it is the person who is talking to the subject—not the consent form—that communicates. The researcher should ensure that the subject is paying attention and understands. A monotone recitation of what is written in the consent form undoes whatever respectful language may be contained in the form.

The elements of consent as they are likely to pertain to empirical software engineering studies are:

1. A statement of what the study involves, its purpose, procedures to be followed (what the subject will experience—not necessarily details of the research design), and the likely duration of the subject's participation.
2. An explanation of any foreseeable risks or discomforts, and a description of any feedback or benefits to subjects. Special mention should be made about risks and related safeguards with respect to vulnerable subjects such as employees.
3. A description of how the confidentiality of data will be maintained, or whether the data will be anonymous (no names or other unique identifiers attached).

4. Mention of the subject's right to refuse without penalty, to withdraw from the procedure at any point, or to withdraw his or her own data at the end of the session.
5. Indication that the subject may keep a copy of the consent form.
6. Information on whom the subject may contact afterward about any questions or complaints. (Typically, one contacts the researcher with any questions, and some key person in the organization with any complaints.)

It may be appropriate to incorporate a non-disclosure agreement in the consent statement.

To help researchers plan their consent statement, templates are usually available from IRBs. Consult your IRB or its website to see if such templates exist. Even using templates, however, researchers must carefully consider what they are writing and how the IRB is likely to interpret their submission.

Debriefing is an important part of the consent process. After having completed their participation, the subjects should have a chance to ask questions, and the researcher should provide whatever information is deemed of interest to the subjects. In addition to providing answers and information, debriefing should also restore a positive frame of mind to subjects; e.g., in the case of those who performed poorly in the tasks given to them (Holmes, 1976). This is also a good time for the researcher to get a better understanding of why the subjects responded as they did. For example, how do the subjects' perceptions of the usefulness or usability of a product compare with those of the researcher? Sometimes the researcher learns as much from the debriefing as from the data.

4.4. The IRB

The IRB meets periodically to review research protocols submitted by members of that institution. The IRB chair or designee receives the protocols, sends them out for review, calls IRB meetings, and communicates the IRB's comments or approval to the researcher. Data collection involving human subjects may not commence until IRB approval is received. Typically the IRB chair and other members are available, informally, to answer questions from researchers, and to provide information.

4.4.1. Membership

The IRB consists of five or more members, including the chair. There may also be a staff person who maintains the IRB's files, and performs other clerical or administrative functions. The members are required by law to have:

> Varying backgrounds to promote complete and adequate review of research activities commonly conducted by the institution. The IRB shall be sufficiently

> qualified through the experience and expertise of its members, and the diversity of the members' backgrounds including consideration of the racial and cultural backgrounds of members and sensitivity to such issues as community attitudes, to promote respect for its advice and counsel in safeguarding the rights and welfare of human subjects. (45 CFR 46.107).

Summarizing the rest of 45 CFR 46.107, no IRB may consist solely of people of one gender or one profession. It must include at least one member whose primary concerns are in scientific areas, and one member in non-scientific areas. It must include at least one member who is neither affiliated with the institution nor an immediate relative of someone affiliated with the institution. No member may participate in review of a project on which he or she has a conflicting interest. The IRB may invite individuals with competence in special areas to assist in the review of issues which require expertise beyond that available on the IRB, but those individuals may not vote on the acceptability of the protocol.

4.4.2. Expedited Review

The Common Rule permits expedited review of some kinds of research involving minimal risk. A list of kinds of research eligible for expedited review appears at http://ohrp.osophs.dhhs.gov/ and is modified from time to time. Expedited review is permitted (a) for items appearing on the list at the discretion of the IRB, or (b) for review of minor changes in previously approved research. The IRB chairperson or one or more experienced reviewers designated by the chair may carry out the expedited review. Under expedited review, reviewers may approve or suggest minor changes, however disapproval may occur only after full review by the IRB. An IRB that adopts an expedited review policy must also create a method for keeping all members informed of research proposals which have been approved under the procedure.

5. Summary

Risk assessment and ethical problem solving are essential tools of empirical software engineering research involving human subjects. Research participants who are treated ethically are more likely to be cooperative and to yield valid data. For example, research involving the corporate sponsor's employees, or students, should thus be performed in ways that do not exploit these readily available subjects and cause ill will. Empirical software engineering researchers should be aware of the regulations that govern their behavior and act appropriately to follow these rules.

Acknowledgments

Grateful acknowledgment is due Interval Research Corporation for permission to use the ideas and policies developed by its Human Subjects Committee, of which the author served as chair from 1997 to 2000.

Notes

1. Like DHHS, some of the other departments had additional regulations which they retained in addition to the common rule. It is conceivable that in years to come software engineering will conduct research under funding from other federal departments. These departments and their regulations that contain the common rule are: Housing and Urban Development (24 CFR 60), Justice (28 CFR 46), Transportation (49 CFR 11), Veterans Affairs (38 CFR 16), Consumer Product Safety (16 CFR 1028), Environmental Protection (40, CFR 26), International Development (11 CFR 225), NASA (14 CFR 1230), NSF (46 CFR 690), Agriculture (7 CFR 16), Commerce (15 CFR 27), Defense (32 CFR 219), Education (34 CFR 99), Energy (10 CFR 745), Social Security (P.I. 103–296), and CIA (Executive Order 12333); the last three agencies also employ Subparts B, C and D of 45 CFR 46.
2. The reader will note that throughout this discussion, the term *subjects* rather than research participants has been used. Some would argue that this is a disrespectful term. However, it is the term used in the Common Rule, and it reminds us that the person studied typically has less power than the researcher and must be accorded the protections that render this inequality morally acceptable. In communication between the researcher and the subject, however, the term *research participant* is preferable.

References

Common Rule (45 CFR 46, Subpart A). http://ohrp.osophs.dhhs.gov/.

Institutional Review Board (IRB) Guidebook. http://ohrp.osophs.dhhs.gov/.

Holmes, D. 1976. Debriefing after psychological experiments: Effectiveness of post-experimental desensitizing. *American Psychologist* 32: 868–875.

Sieber, J. E. 1992. *Planning Ethically Responsible Research*. Newbury Park: Sage.

Joan E. Sieber is professor of Psychology, Emerita at California State University, Hayward, Hayward, CA 94542. jsieber@csuhayward.edu. Her main research interests concern methodology of sensitive field research, and empirical study of how ethical problems arise in social and behavioral research. She is a fellow of the American Psychological Association, a frequent consultant to industry-based researchers, and serves on the faculty of Public Responsibility in Medicine and Research (PRIM&R), Boston.