Cornell University
Office of Research Integrity and Assurance
Human Research Participant Protection Program

SOP 16: COMPUTER- AND INTERNET-BASED HUMAN PARTICIPANT SURVEY RESEARCH

1. Subject of Policy & Procedure

Computer- and Internet-based methods of collecting, storing, utilizing, and transmitting data in research involving human participants are developing at a rapid rate. As these new methods become more widespread in research, they present new ways of enhancing the management of surveys to human research participants while also presenting new compliance challenges to the protection of those participants.

This policy sets forth requirements and recommendations by which researchers can plan, develop, and implement computer- and Internet-based survey research protocols that provide equivalent levels of protection of human participants to those found in more traditional research methodologies such as paper based surveys.

All studies, including those using computer and Internet technologies, must:

1. Ensure that the procedures fulfill the principles of voluntary participation and informed consent,
2. Have appropriate safeguards to protect the privacy or confidentiality of information obtained from or about human participants
3. Adequately address possible risks to participants, including psychosocial stress and related risks

In determining the adequacy of certain survey programs, data collection and storage methods, and informed consent procedures for the protection of human participants, Cornell University's Institutional Review Board for Human Participants (IRB) will assess whether proposed survey research is minimal risk or greater than minimal risk. In making this determination, the IRB will consider whether the resulting data could be stigmatizing, result in criminal or civil liability, damage financial standing, employability, insurability, or reputation, result in stolen identity, or pose a threat to an individual's confidentiality.

2. Scope

This Policy & Procedure applies to all human participant research projects conducted by Cornell faculty, staff, or students or by anyone conducting research in which the participation of Cornell University meets the definition of "engagement" as defined by the Office of Human Research Protections (OHRP).
(http://www.hhs.gov/ohrp/humansubjects/guidance/engage08.html)

3. Terms and Definitions

- **Personal Identifying Information** (as defined in the Office of Management &Budget memorandum M-07-16 at http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf): "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
- IRB Glossary at http://www.irb.cornell.edu/glossary/.

4. Online Surveys

Researchers may need to use a variety of software programs and options to distribute and collect survey data over the Internet. These options fall within one of the following three broad categories:

- Commercial or third party survey creation and hosting services. In these cases, the researchers often enter into a contract with the vendor to provide some or all of the services related to the creation and management of the internet surveys.
- Surveys developed either internally or using a survey development software, and hosted on web servers managed by researchers or by Cornell University IT services.
- Surveys that are conducted via email, because the nature of the transmission to and from respondents may carry additional risks to confidentiality.

Cornell University's IRB has partnered with the Cornell Information Technology's Information Security group, to develop a checklist for the assessment of such survey services. This assessment checklist is provided in Appendix A of this policy. The IRB has reached out to several service providers currently used by Cornell researchers and based on the information provided in writing by these companies, created a list of approved vendors. This list is available on www.irb.cornell.edu/internetsurveys.

Please note that the IRB does not, in any way, promote the use of these service providers. An approval by the IRB simply means that the written statements and policies around security, privacy and confidentiality of data provided to the IRB by these companies allow their use for Internet surveys for human participant research. The IRB welcomes suggested companies to consider adding to this approved list. ORIA will periodically evaluate the written statements, policies and terms of use of the vendors included in the list and update it accordingly.

If the researcher proposes to use a service provider that is not IRB approved, s/he must submit to the IRB, as part of the Initial Approval Request, a completed assessment of the security, privacy and confidentiality practices of the service provider. This assessment is provided as Appendix A of this policy. The IRB will, in consultation with the appropriate experts in IT security, review the information provided to assess whether or not the service

provider can be used for conduct of the survey. In addition, the IRB may decide to add the vendor to the approved list of vendors.

Researchers who would like help mapping the technical requirements indicated in this policy to an option they are considering should contact the Cornell Information Technology's Security office at security-services@cornell.edu.

5. Server Administration

The server used for online surveys of greater than minimal risk must meet the following criteria:

- The server must be administered in accord with current best practices by a professionally trained person with expertise in computer and Internet security.
- Access to the server must be limited to key project personnel and configured to minimize the possibility of external access to the server data.
- The server must be subject to periodic vulnerability assessments to determine that the server is configured and patched according to industry best practices.

6. Data Storage/Disposal

- Personal identifying information must be kept separate from the research data, and both sets of data should be stored in encrypted format.
- It is recommended that data backups be stored in a safe location, such as a secure data room that is environmentally controlled and has limited access. Encryption of backup data is also recommended.
- Competent data destruction services should be used to ensure that no data can be recovered from obsolete electronic media. Investigators should consult data destruction best practices outlined by CIT at http://www.cit.cornell.edu/security/depth/practices/media_destruct.cfm. A link to the tape/disk degausser at Cornell Recycling is as follows: http://www.cit.cornell.edu/services/degausser/. Investigators can also contact professional shredding services for destruction of media content. It is advisable that the service be monitored to ensure the destruction of the materials.

7. Allowable Survey Software based on Study Risk

- The IRB will review each application and designate it as either minimal risk or greater than minimal risk. Researchers should refer to IRB SOP #3: "Initial and Continuing review by the IRB" for guidance on the criteria used by the IRB in making such determinations. For online surveys, the sensitivity of the data being collected will be an additional factor in determining the risk level of the study. While all studies must be approved by the IRB before any research activities can be commenced, the requirements

for these two designations of surveys differ in the types of survey management options allowed by the IRB.

- For studies that are no greater than **minimal risk** and do not involve the collection of sensitive data, the IRB requires these minimum standards:

    - **If an IRB-approved vendor (*one on the IRB approved list or one that is approved for use by the IRB upon an assessment of the responses to the questions in Appendix A*)** is used to conduct the survey, the researcher must, as part of completing the application to the IRB, include the following statement in the informed consent information given to the participant: "*We anticipate that your participation in this survey presents no greater risk than everyday use of the Internet."*

    - **For all other online survey methods,** the researcher must demonstrate, in their application to the IRB, that the following minimum standards are met:

        1. Use of a standard encryption technology such as SSL.

        2. How the security of the web server is being ensured, to prevent unauthorized access. The server must be administered by a professionally trained person with expertise in computer and Internet security.

        3. A disclosure included in the informed consent information provided to the participant stating, "*Please note that the survey(s) [is/are] being conducted with the help of [company name], a company not affiliated with Cornell and with its own privacy and security policies that you can find at its website. We anticipate that your participation in this survey presents no greater risk than everyday use of the Internet."*

- For studies that present **greater than minimal risk**, the IRB requires the following:

    1. That surveys are conducted using an IRB-approved service provider. As stated above, the options currently available to Cornell researchers are available on the IRB website at www.irb.cornell.edu/internetsurveys. If another service provider is proposed, the researcher must complete and submit Appendix A, as outlined in Section 3 above.
    2. For all surveys, the following statement must be added as part of the confidentiality statement in the informed consent information provided to the participant: "We anticipate that your participation in this survey presents no greater risk than everyday use of the Internet."

- **Depending on the risk level and the specific circumstances of the study**, the IRB may elect to require researchers to provide an alternative means of filling out the survey—for example, allowing the participant to complete it and send it via postal mail to the researcher. In addition, the IRB may elect to require additional protections, such as

certified digital signatures for informed consent, technical separation of identifiers and data, or a higher level of encryption.

8. Recruiting Participants

- Computer- and Internet-based procedures for advertising and recruiting potential study subjects (*e.g.*, Internet advertising, email solicitation, banner ads) should follow the IRB guidelines for recruitment that apply to any traditional media, such as letters, telephone scripts, newspapers and bulletin boards.

- The text of the recruitment script, the context in which the recruitment takes place (*e.g.*, posting a message on a newsgroup, mass emailings, and websites created for recruitment of participants) must be reviewed and approved by the IRB.

- If researchers wish to recruit participants for which special protection is required by the Cornell IRB (such as children, prisoners, Cornell students or employees, etc.), they should refer to the IRB SOPs on those topics in designing the study.

- The IRB may advise researchers to take steps to authenticate respondents, if appropriate to the study design. For example, investigators can provide each study participant (in person or by regular postal mail) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer- and Internet-based data collection. The PIN used must not be one that could be used by others to identify the individual (*e.g*. social security number, etc.)

- Depending on the nature of the research, the IRB may request that methods of incentives and/or compensation allow participants to receive remuneration either without revealing their identities or without connecting their identities to survey responses. *For example:* Using gift certificates from online retailers and displaying the unique certificate redemption number to respondents at the completion of a questionnaire. This allows participants to receive an incentive without revealing their identity.

9. Informed Consent

Special Requirements

- For Internet-based surveys, researchers should provide options for prospective participants to indicate their active consent to participate.

- Researchers are required to include a confidentiality disclaimer in the consent document as described in section above.

- When conventional written informed consent will not be obtained, an Internet consent document should be written like a cover letter and should include all the elements of the

regular signed consent document. The consent line should state, "By completing the survey you are agreeing to participate in the research." For web-based surveys, a click-through button should be added.

- If the IRB determines that documented consent is required (*e.g.*, participants' anonymity is not maintained and/or the study is greater than minimal risk) the consent form can be mailed or emailed to the participant who can then sign the form and return it via fax or postal mail.

- Some survey vendors and/or software packages provide a means to record whether a respondent has consented to participate before beginning the survey(s) (e.g., a date/time stamp feature). Researchers should consider the use of this functionality.

- For surveys sent to and returned by participants through email, researchers should include an information sheet with consent information and inform participants that submitting the completed survey implies their consent.

Participation by minors

- Researchers subject to the Children's Online Privacy Protection Act are prohibited from collecting personal information from a child without posting notices about how the information will be used and without getting verifiable (likely written) parental permission. For minimal risk research, written permission may be obtained via postal mail or fax. If the research is more than minimal risk, parental permission should be obtained in a face-to-face meeting.

- For research that excludes minor participants, the IRB may ask the researcher to describe the procedures to be employed to authenticate that the participants are adults. Some options are using Internet Monitoring software or using Adult Check systems can screen out minors.

10. Skipping Portions of/Withdrawing from the Survey

- Unless completion of an entire survey is a requirement of participation, Internet-based survey instruments should be formatted in a way that will allow participants to skip questions if they wish or provide a response such as "I choose not to answer."

- If completion of an entire survey is a requirement of participation, the consent document should clearly indicate this requirement and remind prospective participants that they may choose not to participate, or stop participation in the research at any time.

- If the participant completes an anonymous survey and then submits it to the researcher, the researcher may not be able to extract/remove/delete their specific data from the

database should the participant wish it withdrawn. The consent document should inform prospective participants of this limitation.

11. See Also

Affected researchers and employees should also consult:

- "Ethical and Legal Aspects of Human Subjects Research on the Internet": a report from the American Association for the Advancement of Science, Program of Scientific Freedom, Responsibility and Law, in collaboration with NIH/Office of Protection from Research Risks, at http://www.aaas.org/spp/sfrl/projects/intres/report.pdf.
- Guide to protecting the Confidentiality of Personally identifiable information (PII): Recommendations of the National Institute of Standards and Technology (NIST) http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

12. Regulations Applicable to Computer- and Internet-Based Research

- Children's Online Privacy Protection Act of 1998, at http://www.ftc.gov/ogc/coppa1.htm

APPENDIX A

Cornell University Survey Software Checklist
(and minimum requirements for approval)

1. **Secure transmission**
   Information sent to and from websites can either be transmitted in clear text that could be read if the information was intercepted by a third party (http protocol) or encrypted so that a third party could not read the intercepted information (https protocol).
   1. Does the survey use https encryption? *(Answer should be Yes)* If so, please provide details.
   2. Are there controls in place to prevent a respondent from accidentally entering survey data via the http protocol instead of the https protocol (i.e. does the server display an error message or automatically re-route the respondent to an https page)? *(Answer should be Yes)* Please explain.

2. **Database security**
   1. Do researchers have access to their data in the database via a username and password? *(Answer should be Yes)*
   2. How do you ensure that survey data contained in your databases cannot be improperly accessed or information cannot be disclosed to parties other than authorized researchers? Do your employees have access to this data? How do you monitor access to the data to prevent and detect unauthorized access?

3. **Server security**
   1. Are the servers that contain the research data located in a data center, with physical security controls and environmental controls? *(Answer should be Yes)* Please outline the steps taken towards establishing physical and environmental controls.

4. **Back ups**
   1. Is the data backed up regularly? How often? *(Answer should be nightly at a minimum)*
   2. Is there a finite time period in which a deleted dataset can still be retrieved? What is that time period?

5. **Confidentiality of respondent**
   1. Is the respondent's IP address masked from the researcher? *(Answer should be Yes)* If collected, please explain what is done with the information? Do other third parties have access to IP addresses?
   2. Are cookies installed on machines during the course of taking the survey? Are the cookies specific to the activity on the survey site itself, or are they browsing cookies that can track other online browsing behavior? Are the cookies automatically deleted? If so, when are the cookies deleted?

3. Do the cookies being used also embed, carry or otherwise contain the identity of the respondent? Can the researcher optionally ensure that the survey responses are not tied to the identity of the respondent?
4. Does the software provide (or have the capability to provide) to the researcher a record that captures that a respondent has consented to the survey before the survey? What other information is retained as part of the record (timestamp, respondent ID of some sort that ties the respondent as being the one that agreed to taking the survey)

6. Panel based surveys:

1. What are your policies regarding release of respondent identifiers to researchers who are collecting survey data from the respondent panels that you have recruited?
2. Please provide the written consent document that is provided to the participants at the time of enrollment into the panel and at the time of enrollment into particular surveys. If not specific language, please provide the key elements of the consent that would help the IRB establish that the principles of voluntary participation, confidentiality and privacy required by Federal regulations, are met in these types of surveys.
3. Are there any circumstances where you would release the respondent identifiers and their survey responses to third parties? *(Answer should be No)*