Guidance for Internet-Based Human Subjects Research

Computer- and internet-based methods of collecting, storing, utilizing, and transmitting research data involving human participants are developing at a rapid rate. Today, researchers e-mail surveys, use publicly available postings, social media, and utilize recruitment tools employing artificial intelligence. Nevertheless, computer- and internet-based research protocols must address the same risks (e.g., violation of privacy, legal risks, psychosocial stress) and provide the same level of protection as other types of research involving human participants.

All studies, including those using computer and internet technologies, must (a) ensure that the procedures fulfill the principles of voluntary participation and informed consent, (b) maintain the confidentiality of information obtained from or about human participants, and (c) adequately address possible risks to participants. The purpose of this guideline is to help researchers plan, propose, and implement computer and internet-based research protocols that protect the human subjects involved. The guideline addresses common steps in the research cycle from instrumentation selection and data management to recruitment and informed consent.

RECRUITMENT

Chat rooms/discussion boards

Recruitment of subjects online--whether by email, chat room, discussion board, or other means--must be guided by the level of privacy expected by participants. Online privacy expectations are very subjective and depend on the person/group and the nature of the information being obtained online. Some sites are “fully public” whereas others require user login or invitation by a site administrator. For instance, discussion boards (e.g., Reddit) have multiple “administrators” who have more privileges than people who post. These administrators may be cautious about responding to requests for permission to analyze their discussion board posts. Researchers must ensure they obtain appropriate permission from a website or discussion board administrator and include a copy of that approval in their IRB submission.

Electronic mail

E-mails are not “public information” simply because they are posted on a website. The websites of many professional societies often have guidelines for contacting (or not contacting) its members to participate in research, even if the members’ names/emails appear on that organization’s website.

INSTRUMENTATION

Instrument Integrity

Research instruments such as surveys, questionnaires, tests, or rating scales, can be administered online or in-person using a traditional paper format. Regardless of the format, the researcher should assess the integrity of the instrument. The instrument must be able to measure what the researcher needs or else it will affect the integrity of the research. Use the following guiding questions to assess the validity and reliability of tests and instruments:

1. Do they really measure what they claim to measure?
2. Do they measure consistently over time, with different research subjects and ethnic groups, and after repeated use?

Since many scientific journals want to see data on instrument reliability and validity, research articles featuring the instrument will often include this data. Making use of previously validated data collection instruments can save time and increase the study's credibility. However, researchers should use caution and try to ensure that the research instrumentation and any information obtained via the instrument are used for the purposes of research.

Copyright of Materials

Research instruments are often copyrighted. When obtaining a copy of the instrument(s) to be used in research, researchers should also ensure they obtain permission to use the instrument. If someone posts a published test or instrument without the permission of the copyright holder, he or she is violating copyright and could be legally liable. Contact the copyright holder in writing to obtain permission to use a research instrument. The person should be able to state in writing that they are indeed the copyright holder and that they grant you permission to use the instrument.

INFORMED CONSENT

Obtaining Consent

Informed consent is a key element of protecting the rights and welfare of human subjects. Whenever possible, informed consent must be obtained and documented. The language of the consent must target the age as well as reading and comprehension level of the target audience.

Documenting Consent

Often consent is documented by the subject signing a form. Other mechanisms include audio- or videotaping the subject’s agreement to participate. However, this is often difficult or impossible in internet-based/online research. Under certain circumstances, the requirement to document (get signatures or record the consent process) informed consent for online research activities can be altered or waived. We suggest researchers use “Form 100 Exempt and Minimal Risk or Waiver of Documentation of Consent” as their consent document when conducting online research.

Excluding Minors Who Cannot Consent

People under the age of 18 cannot legally consent to participate in a research study. However, researchers recruiting from the internet cannot know the exact age of respondents. For this reason, it is best to limit online research studies to minimal risk research that would typically qualify for waiver of parental consent under federal regulations unless you are able to authenticate the identity of your respondents through a reliable means.

Deception & Debriefing

The internet provides unique opportunities for conducting observation research in “private” settings. For example, a researcher can join a closed group (e.g. a “members only” chat room devoted to a mutual topic of interest) with relative ease to observe interactions among the members while concealing his/her identity. Such research can only be approved if the IRB determines that the deception is justified. Any research involving deception should have a plan for debriefing subjects, so they may learn about the research that occurred and have the opportunity to withdraw use of their data if they choose.

Ensuring Understanding

When anyone who has access to the Internet is a potential research subject, it may be difficult to ensure that he/she understands the consent information. One method of enhancing comprehension includes incorporating short questionnaires within the consent process to assess understanding of the information presented, and then direct the subjects to additional material. Another method is to design and implement an interactive consent process tailored to the potential subjects' characteristics or primary language.

Right to Withdraw

The principle of respect for persons requires that subjects be allowed to withdraw from a research study without negative consequences. Online survey instruments must explain at the outset what options are available, if any, for retrieving and discarding responses, and for some studies it may be appropriate to provide a "no response" option for questions subjects may consider to be sensitive or intrusive.

DATA COLLECTION

Authentication

Authentication (e.g., proper qualification and/or identification of respondents) is a major challenge in computer and internet-based research as it can potentially affect the integrity of research data and the validity of research results. Whenever possible, researchers should take steps to authenticate online research participants. Measures to verify the identity and characteristics of respondents will vary depending on the nature of the study. For example, in a complex longitudinal study with specific inclusion criteria, investigators can provide each study with a Personal Identification Number (PIN) to use for authentication in subsequent internet-based data collection.

Encryption

It is strongly recommended that any data collected from human participants over computer networks be transmitted in an "encrypted" or coded format. Website URLs should begin with the https:// identifier to insure that information is being transmitted using a Secure Socket Layer (SSL). This minimizes the risk that any data intercepted during transmission could be decoded and traced back to an individual respondent.

Ideally, the highest level of data encryption should be used if it is available and feasible. This may require that the study participants use a specific type/version of browser software. For example, an older version of Internet Explorer, Chrome, Firefox, or Safari may have less security features than newer, updated versions of the same web browser. Please note that encryption standards vary from country to country and that there are legal restrictions regarding the export of certain encryption software outside U.S. boundaries.

DATA STORAGE/DISPOSAL

Password Protection

If computers are used to record human subjects research data, the computer(s) and corresponding files should be password-protected. At FAU, protection of individual faculty/staff computers is managed by Information Resource Management (IRM); password-protection of individual files is usually offered by the manufacturer of the software you are using (for example, Microsoft Word 365 has a Protect Document feature with multiple levels of document access).

Data Storage

If you use a server to store research data, you should limit as much as possible the amount of personal identifying information maintained *(*for example, record the age rather than the birthdate). Personal identifying information should be kept separate from the research data, and data should be stored in an encrypted format. It is recommended that a professionally administered survey server be used for online data collection (e.g., Survey Monkey, Qualtrics). However, if researchers choose to run a separate server for data collection and/or storage, the IRB recommends **a)** the server is administered by a professionally trained person with expertise in computer and internet security; **b)** access to the server is limited to key project personnel; **c)** there are frequent, regularly scheduled security audits of the server; and **d)** the server is subject to periodic security scans.

Data Back-up

Ideally, data backups should be stored in a safe location, such as a secure data room that is environmentally controlled and has limited access.

Data Destruction

Competent data destruction services should be used to ensure that no data can be recovered from old electronic media.