UNIVERSITY OF GEORGIA

Human Subjects Office

Internet Research

1. PURPOSE

The Internet is widely used in the conduct of human subjects research during the recruitment and consent processes, and in data collection. Research using the Internet must provide the same level of protection as any other types of research involving human participants. However, it presents its own unique set of issues and concerns during the IRB review process. The purpose of this document is to help researchers plan, propose, and implement Internet-based research protocols that provide the same level of human subjects protections as more traditional research methodologies.

2. DEFINITIONS

2.1. ***Internet Protocol (or IP) Address*** is a unique identifier associated with every computer connected to the Internet. On many networks, the IP address of a computer is always the same, i.e., fixed or static. On other networks, a random IP address is assigned each time a computer connects to the network, i.e., dynamic. Knowing a fixed IP address is equivalent to knowing the identity of its users.

2.2. ***Private information*** *includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public.*

2.3. ***Sensitive Information*** is private information which if released could reasonably place subjects at risk of criminal or civil liability or could damage their financial standing, employability, insurability, reputation or could be stigmatizing. This include, but are not limited, to sexual attitudes, preferences or practices, use or treatment for alcohol, drugs or other addictive products, illegal behaviors, certain health information, including psychological or mental health.

3. POLICY

3.1. The UGA IRB must review all research activities involving the use of the Internet consistent with the basic IRB principles applied to all research involving human participants (45 CFR 46.111).

3.2. The UGA IRB will review the use of the Internet for research activities to ensure that:

3.2.1.risks such as violation of privacy, legal risks, and psychological stress are minimized;

3.2.2.participation is voluntary;

3.2.3.informed consent requirements are met; and,

3.2.4.measures to maintain the confidentiality of information from or about human participants are appropriate.

4. PROCEDURES: Researchers

4.1. Subject Recruitment

4.1.1.Internet-based procedures for advertising and recruiting potential study participants (e.g., posting to a blog, chat room, Facebook or Twitter; e-mail solicitation, web pages created for recruitment) must follow the IRB guidelines for recruitment that apply to any traditional media, such as flyers and letters (see “315-UGA Worksheet – Advertisements” available in the IRB Library in Click IRB).

4.1.2. For advertisements posted on any website, listserv or social media sites (e.g., Facebook, Twitter) not belonging to the researcher, obtain permission from the site gatekeeper (site administrator or owner), and be aware of the site’s privacy notices and group policies/rules.

4.1.3. A posting to a UGA listserv must follow all the UGA policies regarding SPAM (see http://eits.uga.edu/access_and_security/infosec/pols_regs/policies/aup 4.18 and 4.19).

4.1.4. The IRB may advise researchers to take steps to authenticate participants when such steps are necessary. 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 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).

4.1.5. If study will exclude children, verification of age can take place through fact-checking embedded in the research questions (e.g., cross-validating multiple age and birth date questions; adding a checkbox for the respondent to confirm that he/she is 18 years old or older). If the study involves collection of sensitive information, consider utilizing age verification software products like SafeSurf and RSACi ratings or using Adult Check systems. Researchers may advertise only on sites that are age-limited to begin with.

4.2. Data Collection and Security

4.2.1. Internet data collection is rarely private, anonymous, or even confidential because the Internet is an insecure medium as data in transit is vulnerable. The ease with which information can be accessed, shared, hacked, and/or replicated is unique to Internet research, and for this reason, investigator responsibilities for good data stewardship, and heightened awareness of subjects' privacy, confidentiality, and identities, are critical. This risk is accentuated if the research involves sensitive data that places subjects at risk of criminal or civil liability or could damage their financial standing, employability, insurability, reputation or could be stigmatizing. The potential source of risk is harm resulting from a breach of confidentiality.

4.2.2. When information are sensitive or a breach of confidentiality may involve risk to the participant, the instrument should be formatted in a way that will allow participants to skip questions if they wish to, or provide a response like, "I choose not to answer." At the end of the survey, there should be one button to submit the data and another button to discard the data for inclusion in the study. The purpose of these buttons is to ensure that a subject may withdraw at any time, and to help them understand that if they withdraw even after completing the survey, their data can be discarded prior to transmission to the researcher.

4.2.3. The level of security should be appropriate to the risk. For most research, standard security measures like encryption and secure socket layer (SSL) will suffice. This helps ensure that any data intercepted during transmission cannot be decoded and that individual responses cannot be traced back to an individual respondent. However, more than minimal risk studies involving the transmission of sensitive information may warrant multiple-factor authentication, such as passwords delivered by mail or telephone, or via an identity verification software or vendor. For such studies, it is recommended that the highest level of data encryption be used, within the limits of availability and feasibility. This may require that the study participants be encouraged or required to use a specific type or version of browser software.

4.2.4. Depending on the risk level (e.g., collection of sensitive information) and the specific circumstances of the study, it may be appropriate to provide an alternative means of filling out the survey. For example, allowing the participant to complete a hard copy of the survey and send it postal mail to the researcher.

4.2.5. Researchers are cautioned that encryption standards vary from country to country and that there are legal restrictions regarding the export of certain encryption software outside US boundaries.

4.2.6. If data are collected via the Internet and the subject will participate using a personal home, school, or work computer with an assigned address, participation should not be considered anonymous. Rather, there are indirect identifiers (e.g., IP address, Domain Name System, computer name) that may be traceable to the individual location and person. Such participation may be considered confidential if the researchers utilize available data security protections and describe the plan for handling indirect identifiers that may be included with the data.

4.2.7. To post a survey on a website not belonging to the researcher, obtain permission from the site gatekeeper (site administrator or owner), and be aware of the site's privacy notices and group policies/rules.

4.2.8. For surveys posted on any website not belonging to the researcher, obtain permission from the account/page administrator or owner, and be aware of the site's privacy notices and group policies/rules.

4.2.9. When observing a chat room that is not open to the public, obtain authorization from the chat room manager and inform participants that an "observation" is taking place, and that any information exchanged may be used for research purposes.

4.2.10. If the research involves collection of publicly available data (e.g., Twitter or some Facebook accounts that are public access like business pages), the project may not meet the definition of human subject research. Contact the Human Subjects Office for additional information.

4.3. Server Administration

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

4.3.1.1. The server must be administered in accord with current best practices by a professionally trained person with expertise in computer and Internet security.

4.3.1.2. Access to the server must be limited to key project personnel and configured to minimize the possibility of external access to the server data.

4.3.1.3. The server must be subject to periodic vulnerability assessments to determine that the server is configured and patched according to industry best practices.

4.4. Informed Consent Process

4.4.1. Research on information that is already available on or via the Internet without direct interaction with human subjects (e.g., harvesting, data mining or scraping data from user profiles, observation or recording of otherwise-existing data sets, chat room interactions, blogs, social media postings, etc.) is becoming common. Access to this information is not a justification for collecting data without consent from the subjects because not all Internet content is "public information." For non-Exempt research, a consent document must be submitted for the study or a waiver of informed consent must be requested.

4.4.2. An Internet consent document is written like a cover letter and should include all the elements of the consent that are appropriate for the study. As the security of online transmissions may not be guaranteed, the following statement which described the limits to confidentiality is typically required: "Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties." OR "This research involves the transmission of data over the Internet. Every reasonable effort has been taken to ensure the effective use of available technology; however, confidentiality during online communication cannot be guaranteed."

4.4.3. The description of the consent process must indicate how informed consent will be obtained and, if this does not include obtaining physical signatures on paper documents, appropriate waivers must be requested for non-Exempt research (i.e., waiver of the requirement to document informed consent).

4.4.4. For no risk or less than minimal risk research, it may be appropriate to provide participants with informed consent information, and inform participants that submitting the completed survey implies their consent. Or, it could include "I agree" or "I do not agree" buttons with which participants would indicate their active choice of whether or not they consent to participate.

4.4.5. Consent for a greater than minimal risk study may involve a combination of online and in-person interactions (e.g., including a Skype® discussion or use of comprehension quizzes).

4.4.6. If the IRB determines that a documented consent is required, 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.

4.4.7. However the consent process is conducted, individuals should be provided with an opportunity to have their questions and concerns addressed on an individual basis.

4.4.8. For more information on the Consent Process, please see UGA IRB Policies and Procedures on Informed Consent Process.

4.5. Data Storage and Disposal

4.5.1. For sensitive information, if a server is used for data storage, personally identifying information should be kept separate from the data, and 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. Stripping identifiers from data, storing identifiers and data in separate files, auditing the security of data directories should be routine procedures.

4.5.2. It is recommended that competent data destruction services be used to ensure that no data can be recovered from obsolete electronic media.

4.6. Research with Children

4.6.1. Researchers working with children online are also subject to the Children's Online Privacy Protection Act (COPPA). COPPA prohibits researchers from collecting personal information from a child without posting notices about how the information will be used and without getting verifiable parental permission (for example, collecting the parent's e-mail address or phone number along with parental permission).

4.7. Incentives

4.7.1. Depending on the nature of the research, a procedure for granting incentives and/or compensation without revealing their identities or without connecting their identities to their information may have to be implemented. 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.

4.8. Deception and Incomplete Disclosure

4.8.1. Deception and incomplete disclosure in Internet research may be ethically complex. The need for appropriate debriefing following participation must be given special consideration, but difficulties abound. For example, subjects may choose to leave a venue or locale without reading (or even seeing) the debriefing material; may change email addresses; or may fail to respond to electronic communications. Investigators should address these potential challenges when considering if a debriefing procedure is appropriate.

4.8.2. For additional information, see UGA IRB Policy on Deception and Incomplete Disclosure.

5. PROCEDURES: Institutional Review Board

5.1. The IRB will review all research activities involving the use of the Internet with the same considerations and standards for approval of research (45 CFR 46.111). During the review:

5.1.1. The IRB will evaluate the appropriateness of the recruitment and informed consent processes.

5.1.2. The IRB will take into consideration data collection and security vis-à-vis the type of information that will be collected.

5.1.3. The IRB will consider all additional requirements for the approval of research that involves a vulnerable or special population as all other traditional studies recruiting those populations.

5.2. As there is no standard for identifying distressed participants online, the IRB will take into consideration potential participant experiences (the sensitive nature of the research) that may be distressing when evaluating the risk/benefit ratio.

5.3. The definition of minimal risk references both the probability and the magnitude of harm, and RBs will consider both dimensions. A risk of significant harm (e.g., identity theft, breach of confidential medical or personal information) that is technically possible, but of small likelihood, may be judged to be minimal if the IRB is satisfied that the investigator's data security procedures are appropriate.

6. MATERIALS

6.1. None

7. REFERENCES

7.1. Federal Regulations for Human Subjects Protections (45 CFR 46).

7.2. Considerations and Recommendations Concerning Internet Research and Human Subjects Research Regulations, with Revisions (Final document approved by SACHRP March 2013).

7.3. COPPA: Children’s Online Privacy Protection Act http://www.ftc.gov/os/fedreg/2013/01/130117coppa.pdf