IRB GUIDANCE FOR CONDUCTING HUMAN SUBJECTS RESEARCH STUDIES ONLINE

Protecting Participants

Collecting data over the Internet can increase potential risks to confidentiality because of the frequent involvement of third party sites and the risk of third party interception when transmitting data across a network. For example, when using a third party website to administer surveys, the website might store collected data on backups or server logs beyond the timeframe of the research project. In addition, third party sites may have their own security measures that do not match those of the researchers'.

Participants should be informed of these potential risks in the informed consent document. For example:

i. "Although every reasonable effort has been taken, confidentiality during actual Internet communication procedures cannot be guaranteed."

ii. "Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties."

iii. "Data may exist on backups or server logs beyond the timeframe of this research project."

iv. "Given that surveys can be completed from any computer (e.g., personal, work, school), we are unable to guarantee the security of the computer on which you choose to enter your responses. As a participant in our study, we want you to be aware that certain 'key logging' software programs exist that can be used to track or capture data that you enter and/or websites that you visit."

Data Collection

1. Surveys: Survey research is one of the most common forms of Internet-based research. Researchers are advised to format survey instruments in a way that will allow participants to refuse to answer specific questions. For example, the list of responses can include an option such as, "Decline to answer." In addition, participants must always be given the option to withdraw from a study, even while in the middle of a survey.

   Use of Qualtrics, Mechanical Turk, and other online survey tools is generally permitted for most minimal risk studies employing online survey procedures. The UND IRB strongly recommends that researchers use UND Qualtrics to collect survey data. If researchers utilize a different online survey platform, researchers should review confidentiality measures and data security policies for the given online survey tool and make sure that they are similar to protections provided by UND Qualtrics.

   For online surveys, special attention must be paid to how participants data will be secured. This entails having a familiarity with: the survey software being used, the types of information being collected (IP address, email address), the options the survey software provides regarding what information to collect, the ways in which information will be stored, and how any identifying information will be de-linked from survey data, etc. It is important to note that third party survey software companies (i.e. Survey Monkey, Zoomerang, etc.) differ from UND Qualtrics so the researcher will need to be aware of these differences and the affect this will have on how and where survey data is stored and maintained.

2. Interviews: Conducting interviews online allows researchers to gather information from respondents who would be difficult to contact otherwise, such as a very geographically dispersed population. Interviews may be conducted over the Internet using cross-platform communication technology such as Google Chat, WhatsApp, Skype, Zoom, etc. When conversing with a research participant via chat, researchers should consider the inability to read visual and auditory cues, which can lead to possible misinterpretation of both questions and responses. Voice intonation and facial expressions are often used to convey meaning. Thus, researchers may need to ask clarifying questions in order to accurately interpret responses, and provide additional information in order to be sure that participants understand the questions. The UND IRB strongly recommends that researchers use UND Zoom or Skype for Business to conduct interview research online. If researchers utilize a different online communication technology, researchers should review confidentiality measures and data security policies for the given online survey tool and make sure that they are similar to protections provided by UND Zoom or Skype for Business.

3. COPPA: Operators of commercial websites and online services directed towards children under 13 years of age that collect personal information from these children must comply with the Children's Online Privacy Protection Act (COPPA). The goal of COPPA is to protect children's privacy and safety online, in recognition of the easy access that children often have to the web. COPPA requires website operators to post a privacy policy on their website and create a mechanism by which parents can control what information is collected from their children and how such information may be used. It is the responsibility of the researcher to ensure full compliance with the COPPA regulation.

   For more information about COPPA, visit:
   http://www.ftc.gov/privacy/privacyinitiatives/childrens.html

4. Additional Considerations:
   a. When recording material that would otherwise be temporarily posted online, consideration should be given to whether the act of recording this information potentially creates risks for subjects. For example, information is, at times, posted on the Internet by a third party without the consent of the involved individuals. If a study is likely to record illegal or socially undesirable activity, the researcher should judge whether recording this information would create risk for the subjects and, if so, reconsider using or retaining the data.

   b. Researchers should make sure to review any applicable Terms of Service (TOS). TOS outlines the rules a person or organization must observe in order to use a service. Internet service providers (ISPs) and all websites that store personal data for a user have TOS, in particular, social networking sites, online auctions and financial transaction sites.

Data Security

Researchers must consider additional data-security issues when conducting Internet-based research.

1. Even when it is not the intention of the researcher to collect identifiable information, Internet protocol (IP) addresses are potentially identifiable; thus, if IP addresses will be collected, proper confidentiality measures must be in place in order to protect the subject's identity. These measures include password protection and encryption. The UND IRB strongly encourages researchers to turn off IP address collection on any online data collection platform being used, unless there is a valid reason to collect this information.

2. All identifiable or coded data transmitted over the Internet must be encrypted. This helps ensure that any data intercepted during transmission cannot be decoded and that individual responses cannot be traced back to an individual respondent. It is important to note that encryption standards vary from country to country, and there are legal restrictions regarding the export of certain encryption software outside US boundaries. It is the researcher's responsibility to understand possible restrictions and plan data security measures accordingly.

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. However, research involving particularly sensitive topics may require additional protections, such as housing data on a professionally managed server.

References

UConn Guidance for Data Security and Internet-Based Research Involving Human Participants. Retrieved from https://ovpr.uconn.edu/computer-and-internet-based-research-involving-human-particpants/

UC-Berkeley Guidance on Internet-Based Research. Retrieved from https://cphs.berkeley.edu/internet_research.pdf

UMass-Amherst Online Survey/Survey Research Guidance. Retrieved from https://www.umass.edu/research/guidance/survey-guidelines