BRIDGEWATER STATE UNIVERSITY
INSTITUTIONAL REVIEW BOARD INTERNET RESEARCH GUIDELINES

Internet-based data collection methods, ranging from the use of existing data and observations to interventions and interview procedures that involve data collection methods such as email, listservs, electronic bulletin boards and web surveys, require IRB review. These guidelines are intended for researchers conducting recruitment, informed consent, and/or data collection procedures over the internet.

Research utilizing data that are both existing and public is typically ruled exempt. Data only accessible through special permission or registration/login (with username and password) are generally not considered public. Some publically accessible data may be considered private if it includes identifiers or information about individuals who did not authorize the release of data.

Investigators must be sensitive to the definition of public behavior. Those navigating a public space may have an expectation of privacy, and investigators need to be sensitive to that expectation. Discussion boards are public, but group participants may include personal experiences regarding their struggles and may believe that discussions and potentially identifiable information will remain confidential. Researchers must make sure that all participants are aware of researcher's presence and intentions, that "observation" is taking place, that any information exchanged may be used for research purposes, and have consented to participate. If a researcher creates a chatroom for research purposes a greeting should inform them about the study and ask them for their informed consent.

Internet-based procedures for advertising and recruiting potential participants must follow IRB guidelines. Examples of internet-based recruitment methods include emails, online advertising, and chatroom postings. For non-exempt research these materials must be submitted for review and approval before use in the field. Research that excludes minor participants should describe the procedures to be employed to authenticate that the participants are adults.

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 consent. In general, investigators conducting internet-based research with minors must obtain both child assent and parent permission. Researchers may request a waiver of parent permission provided the study fits the appropriate criteria.

It is generally acceptable to use "I agree" or "I do not agree" buttons (or other electronic methods for indicating affirmative consent) on online pages in lieu of

signatures. For surveys sent to and returned by participants through email, investigators should include a consent document and inform participants that submitting the completed survey indicates their consent. This would constitute implied consent and requires the investigator to request a waiver of documented consent on the IRB application.

Online consent may not be suitable for high risk studies where the research involves data that:

- places participants at risk of criminal or civil liability, or
- could damage their financial standing, employability, insurability, reputation, or
- could be stigmatizing

Researchers conducting web-based research should not to make guarantees of confidentiality or anonymity, as the security of online transmissions may not be guaranteed. Investigators using an online survey tool should review confidentiality measures and data security policies and make sure that they are described in the protocol. Research participants also need to be informed of data security measures.

Researchers should format online survey instruments in a way that will allow participants to skip questions if they wish to or provide a response like "I decline to answer." Similarly, participants must always be given the option to withdraw from a study, even while in the middle of a survey. At the end of an online survey, participants should be able to either discard the data or to choose to submit it for inclusion in the study. When appropriate, online surveys must include mechanisms for identifying the responses of a participant for the purposes of discarding those responses.

Names of internet personas (characters or avatars) or real names may be used in reports and publications only with consent from the participant. If research participants give consent to be identified, data must still be secured properly to avoid any misuse by a third party.

Even when it is not the intention of the researcher to collect identifiable information, internet protocol (IP) addresses can easily be used to identify respondents. Proper confidentiality measures need to be in place in order to protect the subjects' identity. 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 investigator's responsibility to research possible restrictions and revise data security measures accordingly.

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.

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

- "Although every reasonable effort has been taken, confidentiality during actual Internet communication procedures cannot be guaranteed."
- "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." (Penn State)
- "Data may exist on backups or server logs beyond the timeframe of this research project."