Electronic Data Policy Statement

Texas Tech University Institutional Review Board Electronic Data Policy Statement October 2007

Many research projects involve the use of surveys. Over the past few years, the use of online survey software has become increasingly popular. Unlike paper-based surveys, wherein the PI maintains control of collected data, both the survey and the data may be collected and stored elsewhere. Thus, online surveys require the PI to consider several factors regarding the host computer. By this we mean the computer that stores questions and responses to those questions. The following guidelines should assist PIs in their choice of a host server.

There are three possible places the questions can be hosted:

1. a TTU IT-hosted server, that is a server hosted by the TTU IT department
2. a TTU non-IT hosted server, such as a personal or departmental server
3. a private survey hosting provider such as SurveyMonkey, InstantSurvey, or Zoomerang

In all cases, security is important, but in particular, when a PI is collecting data over the Internet from a private provider (SurveyMonkey, Google, Yahoo, etc.), he or she is out-sourcing the dissemination, collection and storage of participant responses to a non-TTU entity. Therefore, the PI must take steps to ensure participant responses are treated in a professional and ethical manner. Moreover, the PI must demonstrate to the IRB reviewer that the responses to the survey will be handled by all in a responsible and secure manner. People included in this proviso are the administrator of the server, and all the other people who may have access to the server (e.g., other administrators and other users of the server that routes your messages.)

Here are specific steps that the IRB recommends.

1. Review the data you are collecting. Are participant responses of a sensitive nature? Sensitive information includes, but is not limited to, social security numbers, religious affiliation, sexual preference, information about criminal behavior, political affiliation, and any socially deviant behavior. It may also include information that allows others to gain access to details of participant responses. Some examples of the later include data, such as name, address, mother's maiden name, passwords, telephone numbers, email addresses, which could provide other individuals with the necessary information to contact participants without their prior consent. Note that the IRB will not require strict security measures for non-sensitive data.
2. If the data are sensitive, then you need to offer evidence to the IRB that:
    a. Data are encrypted when transferred across the Internet (e.g. SSL)
    b. Data are stored on the survey host equipment in an encrypted form
    c. People who have access to the decryption algorithm will not use the data to harass (e.g., marketing), steal from, embarrass or contact participants in any way. In other words, you need to prove that the host has strong security measures and guidelines for all employees that can access data

d. Any server hosting sensitive TTU data must comply with the following:
    i. Data storage, transfer, and collection must be in compliance with Texas Tech University (TTU) IT Security Policies (copies available upon request), FERPA standards, and other privacy laws pertaining to higher education
    ii. Electronic access to all services must be restricted to authorized users, as outlined in the TTU IT Security Policies. Authentication of users must be accomplished through Texas Tech University's official authentication protocol
    iii. Web based interfaces used in the delivery of services must comply with all applicable federal laws and state statutes, to include, but not limited to:
        1. Texas Administrative Code Title 1, Part 10
        2. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) for accessibility by disable persons

If you use a TTU IT-hosted server, the systems and policies are already fully compliant with the required criteria. To host a survey or data on a TTU IT-hosted server, you can contact Technology Operations and System Management (TOSM) at (806) 742-2900 or the TTU Office of the CIO at (806) 742-5156. Thus, all that is required is that you name the server being used and certify that it is TTU IT hosted.

For those TTU non-IT hosted servers, college administrators will be aware of these requirements and can provide documentation that satisfies these criteria. If you use a non-TTU server, then the burden of proof and liability is on the investigator.

If you elect to use a TTU-hosted server, you have the following resources to create Internet-based surveys:

- Your college or division technologists
- You can create your own survey (Technology Support offers training, the Teaching, Learning, and Technology Center offers consulting, the TTU IT Division has a site license for products you can use to create the survey, such as FrontPage and Dreamweaver)
- For larger scope projects, Institutional Research and Information Management (IRIM) may be of assistance.

Finally, please keep in mind that if you provide an email list of people to send the survey to, you are automatically collecting sensitive information. Moreover, many servers send a unique URL via e-mail to insure that the same person does not fill out the survey twice. This means you can link the records to particular respondents, and hence are not maintaining anonymity.