Online Data Collection Confidentiality Issues

Thus far, online data collection at Shepherd has involved 3 online survey sites. Use of each one presents unique IRB issues. The issues and potential resolutions will be addressed below for each site.

A Note on IP Addresses

An Internet Protocol address (or IP address) is similar to a street address or telephone number in that it uniquely identifies a particular device connected to the Internet. Access to an IP address provides only a limited possibility for identifying a particular survey respondent for most researchers (my home IP address, for instance, is identified on most easily accessible Internet IP lookup sites as belonging to Comcast with a physical location in Shepherdstown). Should a researcher's data fall into the hands of a third party (law enforcement, for instance) it is possible that the IP address could be used to identify a particular individual.

Experiment Management System (EMS)

The Experiment Management System by Sona Systems (often referred to as the Sona System) is the software used by the Psychology Department to manage its research participant pool. Its major function is to allow students in the pool to confidentially sign up for and participate in research and then receive the appropriate class credit for their participation. In addition, the software allows for the administration of simple online surveys. By default, EMS allows researchers to see the study participants' names. This applies to both surveys administered within EMS and for studies administered through external sites (such as Survey Monkey or Survey Gizmo) linked to EMS to enable credit-granting.

Potential Resolutions:

1. This display of participants' names can be easily disabled by selecting "Identify participants only by a unique, random identifier" during study setup. Once that setting is made it cannot be undone and, from the researcher's standpoint, the survey is then anonymous. Signing up, participation, and the awarding of credit are all handled by EMS and participants are identified to the researcher using only the system-generated ID number. Researchers do not know who participated in their study and course instructors do not know which studies their students participated in. It should be noted, however, that the local system administrator (a Psychology faculty member, currently Dr. Christopher Lovelace) can still see the names of the participants and their ID numbers. This allows resolution of situations in which a student participant claims to have taken part in a study, but did not receive credit. Researchers should state in their IRB application (in the response to item 5 Confidentiality) that they will use the option to display only ID numbers. On the Informed Consent form, researchers should indicate that they will not be able to link participant names with the data, but that – at least for a period of time – the SONA administrator will be able to do so.

2. There may be situations in which a researcher chooses not to disable the display of participant names. In such situations, the researcher cannot say on either the IRB application or on the Informed Consent form that data collection will be anonymous. At least for a period of time it will be possible to link the name of a participant with that participant's data. It should be noted, however, that the link only occurs within EMS. The participants' names are not written into the

data file. The Informed Consent form should tell the participant that the researcher will have identifiable information and should also outline the steps to be taken to keep it confidential.

Survey Monkey

By default, Survey Monkey records a survey respondent's IP address which could – as noted above – render the data identifiable.

1. IP address collection is easily disabled at all levels of Survey Monkey membership. Researchers should set "Anonymous Responses" to on when setting up a collector. See http://help.surveymonkey.com/articles/en_US/kb/How-do-I-make-surveys-anonymous for instructions on how to do so. Researchers should note in their IRB applications that they will disable IP address collection and their Informed Consent forms can state that the data collection is anonymous.

2. Should a researcher choose not to disable IP address collection, neither the IRB application nor the Informed Consent form can state that data collection will be anonymous. At least for a period of time the researcher will have potentially identifiable data. The Informed Consent form should tell the participant that the researcher will have that information and outline the steps to be taken to keep it confidential. The researcher should also commit to rendering the data anonymous at a particular point in time (say at the end of data collection). At that point the researcher should delete the IP address information from all locally-held copies of the data file. Further, the data should also be deleted from the Survey Monkey web site. This commitment should appear on both the IRB application (in the response to item 5 Confidentiality) and on the Informed Consent form.

Survey Gizmo

By default, Survey Gizmo records the respondent's IP address and some geo-location information.

Potential Resolutions:

1. IP address collection is easily disabled by making the survey anonymous (see http://help.surveygizmo.com/help/article/link/anonymous-surveys). Anonymous surveys, however, are only available with the Professional ($65.00 per month), Premier ($95.00 per month), and Enterprise (starts at $3000 per year) levels of membership. This may not be practical for student researchers or for most faculty researchers, but it should be noted that student or educator discounts may be available. If the survey is set to be anonymous, the researcher can state that the data collection is anonymous in the IRB application and on the Informed Consent form.

2. Should a researcher choose not to disable IP address collection, neither the IRB application nor the Informed Consent form can state that data collection will be anonymous. At least for a period of time the researcher will have potentially identifiable data. The Informed Consent form should tell the participant that the researcher will have that information and outline the steps to be taken to keep it confidential. The researcher should also commit to rendering the data anonymous at a particular point in time (say at the end of data collection). At that point the researcher should

delete the IP address and geo-location information from all locally-held copies of the data file. Further, the data should also be deleted from the Survey Gizmo web site. This commitment should appear on both the IRB application (in the response to item 5 Confidentiality) and on the Informed Consent form.