Online Data Collection Confidentiality Issues

Online data collection using commercial survey tools has increased in popularity and a large number of such tools are now available. Use of each one presents unique IRB issues. One survey tool – Microsoft Forms – is provided through the Shepherd University Office 365 license and its use for research has been sanctioned by the IRB. Three other survey tools – Sona's Experiment Management System, SurveyMonkey, and Qualtrics – have been reviewed by the IRB and their use is generally approved. The issues and potential resolutions for each tool will be addressed below.

A Note on IP Addresses

While recording of information such as a survey respondent's email address obviously presents confidentiality issues, many survey tools record a respondent's Internet Protocol address which, although less familiar to researchers, can also present potential confidentiality issues. 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.

Microsoft Forms

Microsoft Forms does not collect survey respondents' IP addresses, nor does it place cookies on the respondents' computers. If the researcher does not request any identifiable information, surveys conducted using Forms are anonymous. It should be noted, however, that Forms does not track in any way who has participated in a survey, so there is no way to prevent the same person from participating more than once. Forms does offer the option to limit respondents within the researcher's organization to a single submission. The means by which this is accomplished is unclear, but no identifiers are written into the data file. There is also the option to – within the researcher's organization – record respondents' names. Doing so would present confidentiality concerns.

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 Qualtrics) linked to EMS to enable credit-granting.

Potential Resolutions:

1. The 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. Lindsey Levitan) 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 potentially 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.

Qualtrics

Surveys administered through Qualtrics can be rendered anonymous by recruiting participants using an "Anonymous Link" and enabling the setting to Anonymize Responses. A survey using an anonymous link will not collect a respondent's name or email address, but will collect IP address and location information. Collection of that information is disabled by enabling the Anonymize Responses setting. For more information see https://www.qualtrics.com/support/survey-platform/distributions-module/web-distribution/anonymous-link/ and https://www.qualtrics.com/support/survey-platform/survey-module/survey-options/survey-protection/#AnonymizingResponses. Researchers should note in their IRB applications that they will make these settings and their Informed Consent forms can state that the data collection is anonymous.

Some other means of recruiting participants through Qualtrics do collect identifiable information. For instance, if participants are recruited using an Individual link, their name and email address are included in the data file (see https://www.qualtrics.com/support/survey-platform/distributions-module/email-distribution/emails-overview/). Researchers choosing to collect data using individual links should address in the IRB application how confidentiality of the information will be maintained and those provisions should be included on the Informed Consent form.

Other Survey Tools

Alchemer (formerly Survey Gizmo)

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

Potential Resolutions:

1. Collection of IP address and geo-location information is easily disabled by making the survey anonymous (see https://help.alchemer.com/help/anonymous-surveys). Anonymous surveys, however, are only available with the Professional ($149.00 per month) and Full Access ($249.00 per month) levels of individual 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 and geo-location information 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 Alchemer web site. This commitment should appear on both the IRB application (in the response to item 5 Confidentiality) and on the Informed Consent form.