Toronto Metropolitan University

GUIDELINES FOR INTERNET-BASED RESEARCH

Development Date: May 2015
Revised Date: November 2017

Table of Contents

1. Purpose

The purpose of this guideline is to provide researchers with information related to internet-based research.*[i]

2. Background

Internet-based research refers to research projects where there is a central web-based component. This includes research where recruitment, consent, data collection, or data storage is being conducted online.

3. Online Recruitment

Online recruitment must be conducted in accordance with the core principles laid out in the Tri-Council Policy Statement (TCPS 2): concern for welfare, respect for persons, and concern for justice. Examples of internet-based recruitment methods include:

- Email
- Online advertising (e.g., online newspapers, Kijiji, Craigslist, Amazon Mechanical Turk, etc.)
- *Online ch*atrooms and online discussion boards
- Websites and webpages
- Online participant pools (e.g., Sona Systems)
- Blogs (e.g., WordPress)
- Video blogs (e.g., YouTube Channels)

Just as non-online recruitment documents (e.g., posters, in-person scripts, phone scripts, etc.) require Research Ethics Board (REB) review and approval, so too do online recruitment documents. Where possible, the same requirements that apply to non-online recruitment documents also apply to online recruitment documents. In addition, there are two unique challenges with respect to online recruitment that researchers should be aware of: (I) managing the dissemination of recruitment notices; and (II) ensuring that research participants meet the inclusion criteria necessary for participation in research projects.

I. Managing the Dissemination of the Recruitment Notice

When recruitment is conducted online, researchers tend to lose some of their ability to control and manage the dissemination of their recruitment documents. This is because once a researcher posts a recruitment notice or poster online it can be picked up and shared widely with others without the researcher's knowledge or permission. In some cases, this can have unintended consequences and raise additional ethical concerns.

For example, suppose a researcher is seeking to interview five female undergraduate students to explore how young women feel about being underrepresented in Canadian politics. Further suppose that the researcher decides to send an email to a few friends to recruit participants for the study. Now, imagine that one of the friends decides to forward the recruitment email to her contact list of over 500 women. As a result, the researcher now has much more interest from potential participants than initially anticipated and is unsure how to determine in a fair and equitable manner who gets to participate in the study and who does not get to participate in the research project.

As a result of the ease with which people can share online recruitment notices, researchers should have a plan in place in the event that interested potential participants outnumber the spots available to partake in the study.

II. Ensuring Participants Meet the Inclusion Criteria

A second challenge for researchers conducting online recruitment is verifying the identity of research participants. Without face-to-face or voice-to-voice interaction, it may be challenging for researchers to know whether potential research participants are misrepresenting themselves or whether they actually are who they say they are and meet the inclusion criteria.

For example, suppose a researcher is seeking to recruit individuals between 20 and 25 years of age to participate in an online anonymous survey. In such a case, it is possible that those who do not meet the inclusion criteria may attempt to participate in the project, especially if there are incentives involved. To help ensure that participants meet the inclusion criteria, it is important for researchers to implement measures to minimize the likelihood of individuals participating in a study that they do not qualify for.

Determining the number and types of recruitment safeguards or measures for a particular project will depend on the nature of the project. Below are a few examples:

- After initial online recruitment, researchers may wish to conduct an in-person information session to ensure that potential research participants meet the inclusion criteria.
- Researchers may wish to ask for certain kinds of verification (student number, employee number, etc.) in order to verify an individual's identity.

- Researchers could provide each participant (in person or by mail) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer and internet-based data collection.
- Age requirements could be verified by checking for internet monitoring software such as SafeSurf and RSACi rating or using Adult Check systems.

For guidance on what types of safeguards may be appropriate for your particular project, and how best to implement them, we encourage you to contact the REB for assistance.

4. Online Consent

In Section 7 of the "Guidelines on Obtaining Consent and Assent," (available on the REB website), a special template has been created to guide researchers who wish to conduct online consent. For research projects that are minimal risk – i.e., where the probability and magnitude of possible harms implied by participation is no greater than those encountered by participants in those aspects of everyday life that relate to the research – the REB accepts the use of "I agree" or "I do not agree" buttons or other electronic methods for indicating consent.

In some cases, the REB may require that consent forms be mailed or emailed to participants, and that participants either scan, fax, mail or personally deliver a signed copy of the consent form to the researcher to keep on file.

It is important to note that researchers collecting identifiable information online – including names of internet personas, characters or avatars (i.e., a graphical image that represents a person) – must obtain consent from the research participant before any research-related activities can begin.

5. Data Collection, Storage, and Transfer

Two of the most common ways of collecting data online are by (1) conducting online surveys or questionnaires, and (2) by conducting online video interviews.

Online Surveys and Questionnaires

Respecting the autonomy of research participants requires that surveys and questionnaires be designed in such a way that participants are able to (I) voluntarily bypass questions that they do not wish to answer, and (II) withdraw from the study during their participation. Regarding the former, responses to questionnaires or surveys should include something like "Skip this question" or "Decline to answer" as a possible response to questions, in order to prevent any undue influence participants might feel toward answering a specific question in order to complete the survey or questionnaire. Participants should also be given the option to withdraw from the study up until they submit their answers. For example, a phrase at the start of the survey, such as “if you wish to withdraw from the study at any point while completing the survey, simply close your web browser, and your data will not be collected” will suffice for ensuring that participants are given a meaningful way to withdraw from the study during their participation.

Online Video Interviews

Conducting interviews online – as opposed to in-person – has become an increasingly popular method for collecting data from research participants. Many researchers now regularly conduct interviews with participants over Skype, Facebook Video-Chat, Google Hangout Video calls, and other online video platforms. Researchers interviewing participants online must (I) be professional at all times during the interview, and (II) treat participants with the same level of respect and consideration had the interview taken place in-person. For example, researchers should not interview participants while, say, lying in bed, or while multi-tasking.

Respecting participants requires that researchers conduct online interviews in (I) a quiet place (preferably at a desk or table) with a strong internet connection, (II) in an area that has aural and visual privacy, and (III) with a sufficiently powerful and reliable technological device.

Data Storage and Transfer

When storing or transferring participants’ data online, it is imperative that researchers take the appropriate steps to protect their participants’ data from being accessed by non-authorized parties and from being intercepted online. To this end, all data stored online (e.g., Google Drive, Microsoft Cloud, Dropbox, etc.) should be at the very least password protected. In addition, most types of data stored and transferred over the internet must also be encrypted. Based on the nature of the information being stored, (its sensitivity, the likelihood of such data being able to bring about harm, the types of information involved, the vulnerability of the participants, etc.) researchers may be required to take a number of further steps to protect the data, including:

- Anonymizing the information, i.e., irrevocably stripping any direct identifiers from the data so that the risk of re-identification of individuals from remaining indirect identifiers is very low;
- Installing the latest anti-virus software on all computers that will be accessing the data;
- Housing data on a professionally managed server; and/or
- Requiring Two Factor Authentication for accessing the data.

In some cases – e.g., where participants’ data is sensitive or personal in nature, or where the likelihood of such data being able to bring about harm is great – researchers may be required to store and transfer electronic data using physical devices, such as hard drives, or USBs. Typically, participants’ data is more secure when stored and transferred using a physical device – e.g., in a file that is encrypted, and password protected on a USB that is kept in a locked safe with limited access – than when stored and shared online.

N.B. Encryption standards vary from country to country and there are legal restrictions regarding the export of certain encryption software outside Canadian boundaries. It is the investigator's responsibility to research possible restrictions and revise data security measures accordingly.

6. Privacy and Security

When conducting internet-based research, researchers need to treat online personas, identities, or avatars with the same level of respect as they would treat in-person research participants. This entails that researchers protect the privacy of data received by online personas and avatars. It is important to keep in mind that behind every online persona or avatar, there exists an individual whose welfare needs to be taken into account, whose personhood needs to be respected, and who ought to be treated fairly, and equitably.

Researchers collecting data using third-party platforms – such as SurveyMonkey.com, Psychsurveys.org, Amazon Mechanical Turk, and so on – are responsible for understanding these platforms' confidentiality measures, security policies, and Terms of Service (TOS) Agreements. Researchers are also responsible for communicating any salient information regarding these policies and agreements to participants as they relate to the rights of research participants. For instance, if a third-party data collection tool stores data on backup servers or backup logs beyond the timeframe of the research project, this must be clearly communicated to research participants. For example, a researcher could include a line on the consent form stating, "that while I will destroy all data within one year, de-identifiable data may exist on backups or server logs beyond the timeframe of this research project."

Where third-party privacy policies and/or TOS Agreements are under review or unclear, researchers should bring their participants' attention to the uncertainty surrounding how their information may be handled by the third party.

N.B. Internet protocol (IP) addresses can easily be used to identify respondents. Researchers should keep this in mind when designing their research projects, and when communicating to participants regarding privacy and confidentiality issues.

7. Online Chatrooms: Public, Private, and Research-Focused Chatrooms

Researchers seeking to conduct research-related activities in online chatrooms need to be mindful of whether the chatroom is private or public. This determination will affect the way in which the researcher should proceed with respect to research-related activities.

Private Chatrooms

Researchers wishing to conduct research-related activities in private chatrooms – i.e., those chatrooms that require special permissions to be granted in order to enter – should seek permission from the relevant body (e.g., the creator, or manager of the chatroom) before conducting any research-related activities.

Public Chatrooms

Researchers seeking to conduct research-related activities in public chatrooms – i.e., those chatrooms where there are no barriers or special permissions to entry, and where there is no reasonable expectation of privacy – must be respectful of already existing participants in the online chatroom. This entails that (I) the researcher provides existing participants in the chatroom with an opportunity to disclose any discomfort or objection to the researcher's presence, and (II) that all research-related activities be as minimally disruptive as possible. In the event that participants in a chatroom disclose discomfort or object to the researcher's presence, the researcher must not conduct any research-related activities in that chatroom. Researchers must ensure that any research-related activity (e.g., recruitment, observation, seeking consent) does not hinder normal group activity. Researchers need to be particularly sensitive of the fact that conducting research-related activities in online chatrooms may be viewed in a negative light.

Research-Focused Chatrooms

Researchers who are unable to either receive the appropriate permissions to conduct research-related activities in chatrooms, or who are unable to conduct research-related activities in a non-obstructive way may wish to create their own research-focused chatrooms just for research purposes. Creating a research-focused chatroom typically provides researchers with the ability to (I) more closely manage the nature of the discussion, (II) obtain the required data, and (III) ensure that participants are aware of their rights as research participants.

N.B. In some cases, where seeking consent will harm the validity of a study or make the research impracticable, it may be possible to obtain a waiver of consent by the REB. When requesting a waiver of informed consent, issues regarding deception or incomplete disclosure may need to be addressed in the researcher's online ethics application.

8. Online Observational Studies

Research involving the observation of people in online public places is exempt from REB review only in cases where the research involves (a) no direct interaction with individuals, (b) no identifying information, and (c) where the individuals observed have no reasonable expectation of privacy.

[i] *For research conducted using instant messaging, Facebook, Twitter, and other types of social media, see “Guidelines for Research Involving Social Media” on the REB website.