From: noreply+feedproxy@google.com on behalf of Ampersand <noreply+feedproxy@google.com>
Sent: Wednesday, April 29, 2015 5:45 PM
To:
Subject: Ampersand

Follow Up Flag: Flag for follow up
Flag Status: Flagged

Ampersand

Webinar Follow-Up: Hot Topics in Online Survey Research

Posted: 29 Apr 2015 06:46 AM PDT

On March 12, 2015, PRIM&R hosted a webinar titled **Hot Topics in Online Survey Research: Subject Identification, Consent, and Risk**, which was presented by **Elizabeth Buchanan, PhD, and B.R. Simon Rosser, PhD, MPH, LP**.

Online research methods are increasingly common across scholarly disciplines. Particular scientific and ethical issues arise for online researchers in the areas of recruitment, consent, and risk/benefit analyses. This webinar addressed three "hot topics" in online survey research: subject identification, models of consent, and risk/benefit analyses. Following a vibrant discussion at the conclusion of the webinar, Dr. Buchanan and Dr. Rosser agreed to respond to some of the incoming questions in writing to share with the readers of *Ampersand*.

1. Is the review of the terms of service (TOS) the sole responsibility of the IRB, or an institutional or PI responsibility?
Elizabeth Buchanan (EB): While reviewing TOS or end user license agreements is an extra-regulatory consideration, it is becoming more important to understand what is included and what might be significant for your research.

A consent document may indicate that the research team will destroy all project data in a number of years, and the team stores project data in storage cloud (e.g., Amazon Cloud, Google Drive, or Dropbox). Typically, the TOS for each of those services does not specify how long data will be stored; thus, data may exist beyond the time frame outlined in the consent. Or, the consent document may say **only** the research team will have access to study data, when a cloud service will routinely access the data for maintenance: "We may use, access, and retain your files in order to provide the service to you and enforce the terms of the agreement, and you give us all permissions we need to do so. These permissions include, for example, the rights to copy your files for backup purposes, modify your files to enable access in different formats, use information about your files to organize them on your behalf, and access your files to provide technical support" (Amazon Cloud Drive, 2015).

Also, we want to be sure we aren't conducting research that is in violation of the TOS. For example, many sites restrict automated mining, spidering, or scraping data. A site might disallow what might be considered exempt research from an IRB's perspective. Due to the complexity of these agreements, it is best to consider reviewing TOS a shared responsibility. They are

legal documents, and even though most of us click through without reading them, we want to be aware of the potential implications for our research.

2. Do you have any concerns with minors participating in online research geared for an adult population?

Simon Rosser (SR): Yes and no.

Yes—because each study must be viewed on its own merits, the possibility of harm considered, identified, and where possible reduced and risks versus benefits analyzed. Researchers have to work within the law; in addition those of us who are mandated reporters are compelled—if we have the relevant information—to intervene. And where there is risk of serious harm (e.g., a study where the methods could expose a minor to inappropriate relationships with adults) then the onus is on the researcher (and IRB) to address the risk.

No—because in this webinar we were focused on minimal risk research which, by definition, is unlikely to harm children. It's rather difficult, if not impossible, in online research to expose anyone to serious harm (over and above that which is already found online) since anyone can click out of the study if they wish. A very important caveat, mentioned during the presentation, is that we are not talking about research involving deception or emotional manipulation.

Much of research geared for an adult population is low risk (e.g., participating in an online study on engine maintenance, advanced calculus, or appreciating Beethoven) where there simply isn't harm. Some potentially harmful topics (e.g., studying sexual abuse, suicide, and religious radicalization) may put a minor at no more risk than if they visit a website on the same topic.

As a parent and grandparent, I'd be more worried about my children being on an unregulated website promoting destructive or harmful behavior than in any research study. And there are probably some methods (e.g., using social media groups) where children interact with adults or adults have to access a child's information that introduce the possibility of harm. I also think we confuse what is distasteful from what is harmful (which seems to me to be a higher standard). There are a lot of things I choose not to watch or see online (e.g., graphic images in the news) but that doesn't mean I've been harmed. It means I leave the website. A different way to think about this is as follows: Because the online environment is not regulated, the bar to demonstrate that the research study has risk over and above that of just being online/everyday life seems, to me, to be a high bar.

3. Investigators often wish to use Facebook to recruit participants. We are very concerned that participants liking a page on Facebook then associates them with a study. What are your thoughts?

EB: If the project team creates a study page and potential subjects "like" the page, yes, their friends and followers will see that "like." As an alternative, study teams can use nondescript language, referencing a study on depression as a "mood disorder," or provide alternate forms of contact so that an individual can review the page but not "like""it. For more sensitive topics, Facebook pages might not be the best tool; Twitter and Mturk can be used with more confidentiality. But, ultimately, I agree with the **University of Minnesota's IRB** on the limitations of privacy inherent in using social media.

4. If it's necessary to collect the IP address, do you inform respondents that you will collect the IP address?

SR: Initially we would disclose this using a statement like: "Your information is confidential. We don't secretly collect any information (beyond IP address which is only used to validate the survey)." Typically now I don't even mentionit for three reasons: (1) IP address is analogous to physical address. Many studies use physical addresses to locate a particular target demographic and maintain these addresses as process data. (2) I think of IP address as inherently observable. Whenever a

person completes any task online, any provider or external agent gains access to this information. (3) Since businesses and third parties use IP address all the time, requiring researchers to ask first holds us to a standard no one else is using.

5. Isn't using the IP address an inherently flawed mechanism for subject verification?
SR: Solely using IP address for verification is inherently flawed—and we don't recommend it. Instead, we talk about a "deduplication and cross-validation protocol" tailored to the study where IP address is one element of a larger protocol. In **The Story of Subject Naught: A Cautionary but Optimistic Tale of Internet Survey Research**, a paper by Konstan et al., where we found one person completing the study 66 times, using IP address and time information helped identify all the computers used as in a lab, and the timestamp showed the person finished the survey, which took researchers 25 minutes to complete, in 12 minutes. S/he would take three minutes off, then go through the survey on the next computer, etc. So, using IP address for verification is not perfect, but without it, our research results would have been fatally flawed.

6. Can you comment on the anonymity of Amazon MTurk? Although the researcher does not ask for any identifiable information and the online consent form may state the survey is anonymous, MTurk may collect IP address information.
EB: MTurk is not anonymous: Amazon has clearly said that the Turk platform is not meant to support participant anonymity. We are seeing this tension play out across social media research, where all kinds of identifiers are being tracked and maintained by the host or company. But—often, these data are not available to the researcher, as you may recall from our definition:

> "Private information must be individually identifiable (i.e., the identity of the subject **is or may readily be ascertained by the investigator** or associated with the information) in order for obtaining the information to constitute research involving human subjects."

This is an important consideration and we need to be careful with promising anonymity at this point in time. We are truly moving away from the language of anonymity, toward confidentiality.

Also, the **University of Texas put out good guidance for researchers wishing to use Turk**.

7. How long should identifiers be maintained with data for verification? Should they be maintained as long as the data?
SR: Most studies I see maintain them sufficiently to conduct the verification, and then, I assume, they destroy or de-link the files. Some may keep identifiers as long as the data especially if there is some expectation that they may need to audit or independently repeat this step.

8. Could you provide links to or names of institutions that have come up with template protocols/consent forms for internet survey research?
EB: Sure, we have a compiled a list **here**. If you have guidelines for internet research that we've missed, be sure and let us know in the comments below Also, I like The University of Massachusetts-Amherst's online consent documents, **here** and **here**.

PRIM&R would like to thank Dr. Buchanan and Dr. Rosser for sharing their expertise on this important topic. Do you have an idea for a webinar? Share it with us at **webinars@primr.org**.

*If you were unable to attend this webinar and are interested in purchasing the archive, you may do so **here**.*