GUIDELINES FOR RESEARCH INVOLVING SOCIAL MEDIA

Table of Contents

1. Purpose

The purpose of this guideline is to provide researchers with information related to research involving social media platforms. *[i]

2. Background

Conducting research-related activities involving social media has become increasingly common among researchers. Social media platforms (such as Facebook, Twitter, Instagram, Snapchat, etc.) provide researchers with powerful tools to recruit participants, collect and analyze data, and disseminate findings.

3. Social Media Competency

Researchers who wish to conduct research-related activities using social media platforms should demonstrate to the Toronto Metropolitan University Research Ethics Board (REB) that they are aware of how the particular social media outlet they intend to use works. Privacy restrictions, user settings, and legal requirements change and evolve, and researchers should be aware of how these policies affect the rights of potential research participants.

4. Recruiting Participants Using Social Media

Recruiting research participants using social media platforms 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.

Just as other recruitment documents (e.g., emails, posters, in-person scripts, etc.) require REB review and approval, so too do social media recruitment documents. This includes but is not limited to: (i) tweets, (ii) Instagram posters/pictures, and (iii) Facebook advertisements, posts, videos, and messages. Where possible, the same ethical requirements that apply to recruitment documents, generally speaking, also apply to social media recruitment documents. In addition to these requirements – see the "Guidelines for Recruitment of Research Participants" for more information – special attention and care should be given to protecting and respecting the privacy and confidentiality of research participants and researchers.

Respecting the Privacy and Confidentiality of Research Participants

Respecting the privacy and confidentiality of participants typically entails that potential research participants are able to find out more information about a given study, and are able to participate in a particular study, without having such information made known to individuals outside of the research team. To this end, social media platforms that cannot adequately

protect the privacy and confidentiality of individuals who decide to participate in a study should not be used for recruitment purposes.

For example, researchers should not recruit research participants – where participants have a right to their participation remaining confidential – using the "Create Public Event," or "Create Private Event" features on Facebook. The former allows for anyone with a Facebook account to be able to see who is interested in participating in a project, and the latter enables those individuals invited to participate in the project to see who is planning on participating in the project. Given Facebook's current privacy features, participation in a Facebook Event does not allow research participants to participate in a study privately, and in a way that respects the confidentiality of research participants. Researchers should thus discourage participants from reading a Facebook Recruitment post and responding publicly to it. To protect confidentiality researchers should invite participants to reach out to researchers privately.

Protecting the Privacy and Confidentiality of Researchers

In addition to researchers being responsible for ensuring that their social media recruitment tool protects the privacy and confidentiality of research participants, they should also be cognizant of the risks associated with sharing their own social media accounts with potential research participants. The REB typically discourages researchers from using a personal social media account (e.g., Facebook, Twitter, Instagram, etc.) to conduct online recruitment.

The use of personal social media accounts for conducting online recruitment is problematic for two reasons. First, personal social media accounts tend to reveal private details about individuals (such as addresses, places of work, political affiliations/ideologies, etc.) that may put researchers at risk, especially if, for example, an adverse event occurs that negatively affects research participants. Second, using a personal social media account for recruitment purposes can be problematic because such accounts typically not only share personal information about the researcher, but also share details about the researcher's friends, family, and colleagues, who may not want such details revealed to potential research participants. Thus, out of respect for those individuals who may indirectly feature in the researcher's social media account, personal social media accounts are discouraged from being used in research-related activities. Researchers are instead encouraged to develop a research-specific Facebook or other social media profile.

In some cases, however, it is possible that researchers may have compelling reasons to use personal social media accounts to conduct research-related activities. In these cases, the onus is on researchers to demonstrate to the REB that (i) their social media recruitment tool adequately protects the privacy and confidentiality of research participants, and that (ii) the recruitment method is professional in nature and does not pose any increased risks to the researcher, research team, or other individuals.

5. Collecting and Analyzing Social Media Data

One of the biggest misconceptions many researchers have when conducting social media research is that just because social media data (e.g., Instagram posts, Facebook pictures, tweets, etc.) exists on a seemingly "public" social media platform, that researchers are free to use such data as they wish, for their own research purposes. This is incorrect. There are two things that researchers should do when conducting and analyzing social media data: (i) respect the privacy restrictions, user settings, and legal requirements of the particular social media platform they intend to use; and (ii) take seriously the potential risks associated with collecting and analyzing social media data.

Respecting Privacy Restrictions, User Settings, and Legal Requirements

Researchers collecting and analyzing social media data must familiarize themselves and abide by the privacy restrictions, user settings, and legal requirements of the social media platforms they intend to use. These policies vary across different social media platforms and evolve over time. Let us look at one example.

Presently, according to Facebook's Terms and Services, individuals own the rights to the information that they themselves have produced and posted on Facebook. This includes pictures, comments, notes, videos, and so on. In cases where researchers wish to collect and analyze social media data that does not belong to them – regardless of how easily available the data may be – they must obtain consent from the owner before using the data for research-related activities. Individuals who share data on Facebook have an intellectual property right over their data, and respecting the rights of research participants necessarily entails receiving their consent before using their data for research-related purposes.

For example, if a researcher is seeking to conduct a photovoice project using someone else's photos that appear on Facebook, even if such pictures are shared widely, they must nonetheless obtain consent from the owner of the photos in order to use them in their project. The important thing to note is that just because social media data may be widely accessible does not mean that consent is not required in order to use such data for research-related purposes.

Potential Risks Related to Research Involving Social Media Data

Individuals conducting research-related activities involving social media data must be cognizant of the potential risks associated with such activities. Even in cases where social media data is widely shared, there may be significant risks to research participants. For example, it is not uncommon for individuals to upload and share information on a social media platform that (i) does not belong to them, (ii) that they have no right to share, and that (iii) may cause significant harm.

For instance, individuals may create and operate a fake social media account that in no way represents the actual user or create and operate a social media account with the intent of bullying, harassing, or exploiting others. Unfortunately, such social media accounts exist, and it is important for researchers to be aware of the precarious nature of social media data, and to think carefully about how using social media data may affect the rights of research participants.

Respecting the rights of research participants entails that (i) researchers take reasonable steps to authenticate the social media data they intend to use, and (ii) to abstain from using social media data that has been produced or shared in an illegal or unethical way.

---

[i] *For research involving other internet-based platforms, see "Guidelines for Internet-Based Research" on the REB website.