Standard Operating Policy & Procedure No. 10

USE OF INTERNET/SOCIAL MEDIA FOR HUMAN SUBJECT RESEARCH

INTRODUCTION

As the use of social media sites, including but not limited to Facebook, Instagram, Twitter, YouTube, and LinkedIn, continue to evolve and popularize, its uses in human subject research do as well. Internet/social media-based research projects are reviewed by the Institutional Review Board (IRB) just as any other research project, except that there are additional considerations related to the establishment and protection of human research subjects' identity, as well as research data security concerns that the investigator must address.

Investigators should be aware of any research-related restrictions on the use of the internet/social media site through which they intend to conduct their research activities. The IRB cannot take responsibility for ensuring that the terms and conditions for conducting research on internet/social media sites have been met. Failure to acquire appropriate permissions could result in consequences that may include loss of the data collected, reputational harm to the investigator and Saint Joseph's University (SJU), and possible legal action by the site owner, research subjects, or grant agencies against the Principal Investigator and/or the University.

The information presented in this Standard Operating Policy and Procedure (SOPP) sets forth requirements for research conducted at SJU that makes use of Internet/social media sites and/or applications. Special consideration should be given to each aspect of human subject research projects when internet/social media is involved. It is important to note that all recruitment, interaction with subjects, and data collection via social media for the purposes of human subject research should be conducted in accordance with the standard SOPPs as non-internet-based research.

POLICY STATEMENTS

1. Passive Data Collection

   Passive data collection for internet/social media sources may not constitute human subject research if the research project does not involve any interaction or intervention with the individual about whom data is being collected (i.e., Twitter feeds, Facebook profiles or wall postings, Instagram postings, and information from open chat rooms).

   Typical examples of internet/social media-based research projects that are not human subject research include:

   1.1 The individual user or internet/social media site has not placed any restrictions on access to information about himself/herself (e.g., information available on a public website, blog, feed, chat room) OR

   1.2 The data is officially and publicly archived and are not protected by password or login, AND the site policy does not prohibit the direct quotation of material from the site.

The Principal Investigator should ensure that all the information on any human subject is de- identified and that research results are presented in aggregate. The IRB recommends that subjects not be individually identified or that the information on the human subjects be combined in such a manner that the identity of the group or individual subject can be readily ascertained. In cases where the research requires that individual subjects be identified, researchers should explain the reason in an IRB application.

The Principal Investigator should send a project description to the Research Compliance Coordinator and seek a formal confirmation of non-human subject research status for the study.

2. Active Data Collection

   2.1. Active data collection is considered human subject research that requires IRB approval when an individual has restricted access to the internet/social media data in any way (i.e., the investigator has to request or seek access from the individual or from the group that the individual belongs to; or if the investigator has to belong to, be invited to, or invite others to a particular "interest" or "friend" group), or if the internet/social media site has restrictive provision in its terms of service, an expectation of privacy has been established.

   2.2. If research is being done on a site or chat platform that requires consenting to an End User License Agreement (EULA), Terms of Service (TOS), or other site or platform rules, users must follow the internet provider guidelines.

   2.3. Individuals must be made aware that they are participating in a research project that involves any experimental manipulation of the media environment, such as stimulus intended to assess reactions or responses, game or role playing, etc.

   2.4. Research projects including deception research projects can be conducted using internet/social media-based research projects; however, individuals must consent to participate as described in SOPP 2.

3. Special Types of Research Subjects

   3.1. Online Identities: Personas or avatars and their corresponding character names established in online communities should be treated just like human persons. These personas and their reputations can usually be tracked back to real individuals who are the human controller. If an investigator wishes to use names of personas or real subjects' names in publications, it is normally sufficient to consent the human controller or to recognize consent from the personas as a proxy for the controller, although in some cases consenting both the virtual persona and the human controller may be more appropriate.

   3.2. Collateral Research Subjects: During data collections, investigators may gather information not only about and from the individual specifically recruited for the project, but also about individuals connected to the recruited subject's social network of "friends" by accessing the information that those individuals have made available to the recruited subject. Information made available by "friends" on the "wall" or another public space on the social network may be considered to belong to the subject and can be included

without the explicit consent of the "friend". Investigators must exercise caution to protect the identity of the "friend".

3.3. Individuals Who Decline to Participate: Investigators may not collect any information from any individual who declines to participate in the project.

4. Recruitment

Investigators should be aware that in internet/social media-based research settings, the potential subject population may not be entirely under the investigator's control. For example, the recruitment information can be forwarded or otherwise accessible to other individuals who may not be part of the intended subject pool. Investigators should exercise caution to appropriately identify the target subject population in the protocol and in recruitment messages. Investigators must ensure safeguards are in place for screening children, prisoners, and other vulnerable populations, unless these populations are the intended subjects of the project.

5. Compensation of Internet/Social Media-Based Research Subjects

The use of compensated research panels as a recruitment method for human subject studies continues to grow. Panels such as Amazon Mechanical Turk (mTurk) advertise for panel subjects as a "marketplace for work," and individuals who take part in the activities (called "HITS") on this site are referred to as "workers." The consent document should explicitly state that the research project is "research." For compensation guidelines please see SOPP 9.

6. Consent

6.1. The IRB does not allow passive consent for human subject research. The process of requesting consent should not disrupt the normal activity of an internet/social media- based research site that is not expressly set up for research purposes and for which the investigator is not the site administrator.

6.2. In real-time environments (including chat rooms, virtual worlds, multiplayer gaming "MMOG", etc.) the process of requesting consent publicly is often perceived as disruptive. In such cases, the investigator should consider announcing publicly that they are conducting research. Investigators may then request that people contact them via private messaging or email for more information about the research project.

6.3. When a waiver of consent is requested, the information sheet used for consent must appear as the first page on the online survey website and an Accept or Decline checkbox is usually acceptable. Online consent forms should include a link to download the consent document, or the investigator should provide instructions on how to obtain and print a copy of the consent document.

Depending on the level of risk, a single checkbox to Accept/Decline may not be acceptable. Instead of a single checkbox at the end of a consent statement, investigators may use a checkbox for each item in the consent form, taking subjects through each step of the informed consent process. The IRB may require signed consent forms for research projects that are greater than minimal risk.

6.4. Investigators are prohibited from collecting personal information from a child under 13 years of age without posting notices about how the information will be used and without getting verifiable parental permission. See Section 9.11 below. The IRB may require parental consent forms for research projects that are greater than minimal risk and include human subjects who are 13 years of age and older.

7. Mobile Devices and Emerging Technology

   Additional considerations apply to research involving data collection via social media applications that are networked with mobile devices or installing applications on a person's mobile device to collect data. Investigators must not collect location information or other data that is not explicitly approved by the research subject in the consent document.

   If the research involves installing an application (app) on a person's mobile device for the purposes of data collection, the investigator must describe how the app will be deactivated at the conclusion of the research project. This should be done either by making the deactivation part of the research project's exit procedures, or by providing instructions to subjects on how to deactivate the app.

8. Data Security

   Collecting data over the internet can increase potential risks to confidentiality because of third- party sites, the risk of third-party interception when transmitting data across a network and the impossibility of ensuring that data is completely destroyed once the work is complete. Subjects should be informed of these potential risks in the consent document.

9. Applicable Regulations and Guidelines

   9.1. Federal Regulations

      9.1.1. Children's Online Privacy Protection Rule (COPPA) 16 CFR Part 312

   9.2. Referenced IRB SOPPs

      9.2.1. SOPP 6: Informed Consent

      9.2.2. SOPP 9: Recruitment and Payment of Human Subjects