DISCLAIMER: This document has not been updated to reflect regulatory changes effective January 21, 2019.

Use of Social Networking Sites or Mobile Devices for Human Participant Research

Guidelines for IRB application and review

1. Subject

As new media and technologies for social networking – such as Facebook, Twitter, YouTube, Foursquare and World of Warcraft – continue to transform communication and informational practices, and the social networking technologies continue to evolve in scope, relevance and applications, the ethical considerations in the study of interactions that are now enabled or transformed by these technologies also continue to evolve.

Research involving the collection of data about people through social media and networking sites involves many of the same considerations as any other research with human participants: determining an appropriate and effective informed consent process; assuring that participation is voluntary; protecting privacy and confidentiality of individuals and the data collected; minimizing risks and maximizing benefits; and assuring equitable selection of participants. However, with the dynamic and evolving nature of norms and technologies in social media use, translating these principles into real practices can be challenging.

This policy describes general guidance to investigators in planning their research with human participants using social media technologies. As the nature of research involving these technologies continues to evolve, it is not possible to identify every circumstance or type of research activity that may involve the use of social media. If there are circumstances that are unique to a study, the IRB will need to adopt a case by case approach to the review and approval of the study. The IRB policy on the use of Internet surveys in human participant research also addresses a number of related issues. We encourage you to refer to both these policies as you design your research study, and to contact the IRB office if you have specific questions not addressed in them.

2. Definitions

- **Human subject:** a living individual about whom an investigator (whether professional or student) conducting research obtains (1) Data through intervention or interaction with the individual, or (2) Identifiable private information.
- **Private information:** Information about behavior that occurs in a context in which an individual can reasonably expect that observation or recording is not taking place, or information which an individual has provided for specific purposes and which the individual can reasonably expect will not be made public. This information may be clearly private (a medical record or personal diary), but may also include a person's Facebook profile that is set so only friends can see messages or photographs. In order for obtaining the information to constitute research involving human subjects, 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).
- **Interaction:** Any communication or interpersonal contact between investigator and subject with any medium.
- **Intervention:** (1) Physical procedures by which data are gathered (for example, surveys, focus groups, experiments, venipuncture etc.) and (2) manipulations of the subject or the subject's environment performed for research purposes.
- **Social media/network services:** Web and mobile device-based services that provide a collection of ways for users to interact, such as social networking sites, blogs, discussion groups, or other information sharing or communication services that support messaging, email, video, posting comments, etc.

3. Type of research with human participants in the social media realm

a. Data mining or passive information gathering:

This type of research involves no interaction or intervention with the individual about whom data is being collected (examples: public twitter feeds; public Facebook profiles or wall postings; information from public/open chat rooms, whether the data is collected through silent observation or from archives; etc.).

If the individual or social media/network site has not placed any restrictions on access to information about himself/herself (e.g., information available on a public website, blog, twitter feed, chat room, etc.), the following best practices should be followed:

- The researcher should send a project description to the IRB office and seek a formal confirmation of non-human participant research status for the study. We

believe that in most cases, this will not be considered human participant research, but caution is recommended before a researcher makes his/her own determination, because of the emerging ethical sensitivities in this area.

- The researcher should ensure that all the information on an individual is de-identified and that research results are presented in aggregate. As a courtesy, we recommend that individuals not be individually identified or that the information on the individuals be combined in such a manner that the identity of the group or individuals can be readily ascertained. In cases where the research requires that individuals be identified, researchers should explain the reasons in the IRB application for the IRB to make a decision on the impact to the risk/benefit of the study procedures to participants.
- Note that the individuals on many of the public "blogs" use pseudonyms to conceal their identities. In general researchers should avoid eliciting information from other sources to establish the real identity of these individuals and must exercise caution to ensure that accidental revelation of their identity does not occur.
- For research that involves collection of data that individuals may not realize is accessible (e.g., data left on directories that are accessible via use of a web crawler), investigators should regard data as private unless they can demonstrate that data is sufficiently de-identified. Otherwise, investigators should plan to submit an application to the IRB office and provide sufficient justification to access the data, describe whether use of it will pose any risks to individuals, and/or explain how privacy/confidentiality will be protected.

If an individual has restricted access to the data in any way or the social media/network site has restrictive provisions in its terms of service, an expectation of privacy has been established and the investigator must seek IRB approval before conducting the research. Examples of such restrictions include:

- If the researcher has to request or seek access from the individual or from the group that the individual belongs to,
- If the researcher has to belong to, be invited to, or invite others to a particular "interest" or "friend" group, or
- If the researcher seeks access when "role playing" or recruits individuals who have the restricted access.

In the IRB application, the researcher must include a description of consent procedures and how the consent will be documented. In general, passive consent

(i.e., where a potential research subject is asked to opt out of being included in the research) is not acceptable when access to information has been restricted.

b. "Experiment" type research

Examples of this type of research include manipulating the media environment as a stimulus intended to assess reactions or responses, game or role playing. This type of research involves interaction or intervention of the individuals' environment; therefore, it is considered research with human participants. The researcher must submit an application to the IRB office before conducting any research activities .

c. Deception research

This type of research involves interaction with or intervention in the individuals' environment; therefore, it is considered research with human participants. The researcher must submit an application to the IRB office before conducting any research activities . Special considerations include the following:

- Individuals must be made aware that they are the subjects of an experiment. Totally blind deception experiments are not acceptable.
- In most cases, individuals must agree to participate. It may be acceptable to not reveal the true purpose of the experiment at the outset. However, prompt and thorough debriefing is expected. To ensure that the research is not compromised, it may be necessary in some cases for the investigator to conduct debriefing after the entire data collection is completed rather than immediately after a subject finishes his/her direct participation. The researcher should clearly state this in the application and provide a justification. Since the participants' consent for participating in the specific study was based on a deception, it is generally recommended that participants be given the opportunity to withdraw their data from the study. If this is not possible, the researcher should clearly articulate the reasons to the IRB in her/his application, the reasons.
- Unless the study is aimed at children, researchers must ensure that they have implemented safeguards to prevent children from participating in deception studies. In most cases the IRB will ask for these safeguards to be put into place.

d. Social media as recruitment venue

This type of research involves interaction with or intervention in the individuals' environment; therefore, it is considered research with human participants. The researcher must submit an application to the IRB office before conducting any research activities . Special considerations include the following:

- Consent for enrollment into the study should always be a process that is independent from the recruitment (e.g., before or as part of the survey process).

It is generally not acceptable to consent the individual only as part of the recruitment message.

- Researchers must clarify that the data are collected only when the participant accesses the survey site. In other words, no opportunistic data can be collected. For example: If an investigator sends a link to individuals to access a survey or an application, s/he **may not** collect information about the person if they click on the link to access the consent/survey or application. If data is collected in this manner, it would qualify as deception research and require debriefing and the ability of the unsuspecting participant to withdraw their data.
- Researchers may not collect any information from any individual who declines to participate in the study. **Exception:** if the process for making an accept/decline decision is the subject of the study, the investigator must acknowledge the deception in a subsequent debriefing process and, when possible, allow the individual the opportunity to withdraw her/his response.
- Researchers should ensure that recruitment of individuals using the social networking site meets the criteria for equitable selection of participants and that sample selection is justified. Researchers should also be aware that in a social media or other Internet based research settings, the respondent population may not be entirely under the researcher's control, as the recruitment information can be forwarded or otherwise accessible to other individuals who may not be part of the intended participant pool. Researchers should, therefore, exercise caution to appropriately identify the target participant population as part of the survey process.
- Researchers must ensure safeguards are in place for screening children, prisoners and other vulnerable populations, unless these populations are the intended participants of their study.
- Researchers may seek to get information not only about and from the individual specifically recruited for the study, but also about individuals connected to the recruited participant's social network (e.g., his/her "friends") by accessing the information that those individuals have made available to the recruited participant. In this circumstance the participant population now includes the "friends" who may need to be consented before data about them can be included in the study. Information made available by "friends" on the "wall" or another public place on the recruited participant's social network may be considered to belong to the participant and can be included without the explicit consent of the "friend," if the study itself is considered to be no more than

minimal risk. Researchers must exercise caution to protect the identity of such participants and report results in aggregate as much as possible.

- An opt-out type of consent may be possible. Participant informs friends that data posted on her/his site between certain dates will be available for research. Those not wanting their data included should inform her/him or refrain from posting. This waiver of consent should be OK for no more than minimal risk studies.

e. Use of mobile devices and other emerging technology

This type of research may involve the use of existing data and/or interaction with or intervention in the person's environment. In either case, the guidance in the preceding descriptions will apply as appropriate to the research design. However, additional considerations apply to research that involves the collection of data via social media applications that are networked with mobile devices, or by installing applications on a person's mobile device to collect data:

- Researchers must not collect location information or other data that is not explicitly stated to the study participant in the consent form.
- If the research involves installing a mobile application (app) on a person's smartphone or other device for the purposes of data collection, the researcher must describe how the app will be deactivated at the conclusion of the study. This should be done either by making the deactivation part of the study's exit procedures, or by providing instructions to study participants on how to deactivate the app. Additionally, researchers should describe plans to ensure they do not continue to collect data once the study is complete, in case a participant does not effectively deactivate the app.
- If the study involves the use of a mobile device provided by the researcher, the researcher should explain the confidentiality safeguards that are in place (e.g., how s/he will ensure the data is under the research team's control and that third parties do not have access to it), as appropriate to the study.

f. Use of Amazon Mechanical Turk as recruitment venue for surveys and other studies

The use of Amazon Mechanical Turk as a recruitment method for human participant studies continues to grow. Mechanical Turk is advertised as a "marketplace for work," and individuals who take part in the activities called "HITS" on this site are referred to as "workers." The compensation for the tasks accomplished is typically very small, usually less than $1. The considerations for using this site for recruitment of participants are the same as with any human participant research. Additionally, the IRB suggests that investigators consider the following:

- Explicitly mention that the study is "research" and not a "job."
- Address whether or not the compensation is contingent upon certain conditions. Ensure that the complexity of the task and the amount of time expected for completion is reasonable and communicated clearly in the consent process.

Sample statement to include in the consent information: "This is an academic not-for-profit research study. This form is designed to give you information about this study. We will describe this study to you and answer any of your questions."

Note: Data collected using the Amazon Mechanical Turk data collection tool resides on the Amazon servers and no assurance can be made as to its use for purposes other than the research. Researchers are advised to therefore collect data using a third party survey software, such as Qualtrics, with known policies for data security and anonymity.

4. Terms and conditions of use of the social networking site or software

Researchers should be aware of any research related restrictions on the use of the social media/networking site through which they intend to conduct their research activities. Neither Cornell University nor the IRB can take responsibility for ensuring that the terms and conditions for conducting research on such sites have been met. Failure to ascertain and acquire appropriate permissions could result in consequences that may include sequestration or loss of the data collected, reputational harm to the researcher and the institution and in the worst case, legal action by the site manager or participants.

5. Virtual identities, personas

Online identities (personas or avatars) and their corresponding character names established in online communities should be treated just like real persons. These personas and their reputations can usually be traced back to real individuals. If a researcher wishes to use names of internet personas or real names in publications, it is normally sufficient to consent the human controller or to recognize consent from the avatar as a proxy for the controller, although in some cases consenting both the virtual persona and the human controller may be more appropriate.

6. Security of data and confidentiality

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. Participants should be informed of these potential risks in the informed consent document. For example:

- "Although every reasonable effort has been taken, confidentiality during actual Internet communication procedures cannot be guaranteed."
- "Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties." (Penn State)
- "Data may exist on backups or server logs beyond the timeframe of this research project."

7. References

- Berkeley CPHS Policy on Internet Based Research; April 2012 (http://cphs.berkeley.edu/internet_research.pdf)
- Internet Research Ethics and IRBs, Elizabth Buchanan, OHRP Research Forum, Chicago May 2012 (http://www.slideshare.net/InResEth/internet-research-ethics-and-irbs-4159809)
- IRB Review of the Use of Social Media in Research; The Quorum Review, December 2012
- Considerations and Recommendations Concerning Internet Research and Human Subjects Research Regulations, with Revisions SACHRP meeting March 12-13, 2013 (http://www.hhs.gov/ohrp/sachrp/mtgings/2013%20March%20Mtg/internet_research.pdf)

Approved: 5/3/2013