SOP 502L: INTERNET/SOCIAL MEDIA-BASED RESEARCH

1. POLICY

Internet/social media-based research projects are reviewed by the IRB just as any other research projects, except that there are additional considerations related to the establishment and protection of human research participants' identity and research data security concerns that must be addressed by the investigator.

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 the University and, in the worst case, legal action by the site manager or research participants against the Investigator and/or the University.

When conducting internet and social media research, the investigator is responsible for knowing the University Information Technology, Information Security, and HIPAA policies concerning (but not limited to) Privacy, Terms of Use of University Equipment, Data Security, and Disposal of Electronic Media and Hardware.

Because the nature of research involving these technologies continues to evolve, it is not possible to identify every circumstance or type of research activity. If there are circumstances that are unique to a research project, the IRB will review the research project on a case-by-case basis.

Specific Policies

1.1 Passive Data Collection

Passive data collection from internet/social media sources may not constitute human subjects research if the research project does not involve any interaction or intervention with the individual about whom data is being collected (examples: Twitter feeds; Facebook profiles or wall postings; information from open chat rooms, whether the data is collected through silent observation or from archives).

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

1.1.1 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, Twitter feed, chat room,) OR

1.1.2 The data are officially and publicly archived and are not protected by a password or login, AND

1.1.3 The site policy does not prohibit the direct quotation of material from the site (or prohibit research more generally).

For passive data collection on internet or via social media archives, the investigator shall ensure that all the information on an individual is de-identified and that research results are presented in aggregate.

1.2 Active Data Collection

1.2.1 If an individual has restricted access to the internet/social media data in any way (for example: 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 provisions in its terms of service, an expectation of privacy has been established and the research will be considered Human Subjects Research that requires IRB approval.

1.2.2 Additionally, if research is being done on a site or chat platform that requires consenting to a EULA (End User License Agreement), TOS (Terms of Service), or other site or platform rules, users must follow the internet provider guidelines. If this includes requiring permission from the host site's administrator(s), investigators must first obtain consent from the administrator(s).

1.2.3 Individuals must be made aware that they are participating in a research project that involves an experimental manipulation. Deception research projects can be conducted using internet/social media-based research projects; however, individuals must consent to participate (see SOP 502J: Categories of Research Social/Behavioral for further guidance on deception studies).

1.3 Special Types of Research Participants

1.3.1 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 who are the human controller. If a investigator wishes to use names of personas or real participant 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.

1.3.2 Collateral research participants: During data collection, investigators may gather information not only about and from the individual specifically recruited for the research project, but also about individuals connected to the recruited participant’s social network (e.g., his/her “friends” on Facebook) by accessing the information that those individuals have made available to the recruited participant.

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”. Investigators must exercise caution to protect the identity of such “friend” participants and report results in aggregate as much as possible.

1.3.3 Individuals Who Decline to Participate: Investigators may not collect any information from any individual who declines to participate in the research

project. **Exception:** if the process for making an accept/decline decision is the subject of the research project; the investigator must acknowledge the deception in a subsequent debriefing process and, when possible, allow the individual the opportunity to withdraw her/his response. (see SOP 502J: Categories of Research Social/Behavioral).

1.3.4 Individuals Who May Be Deductively Re-identified: Research projects may include 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.

1.3.5 Individuals Whose Identity is Accidentally Revealed During Passive Data Collection: [data mining, scraping and mashing in glossary] Passive and active data collection practices may make it possible for the information to be combined in such a manner that the identity of the group or individuals can be readily ascertained. Research projects that include the risk of accidental identification need to be approved by the IRB as human subjects research.

1.4 Recruitment

Investigators should be aware that in internet/social media-based research settings, the potential participant 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 participant pool. Investigators should, therefore, exercise caution to appropriately identify the target participant population in the research protocol and in recruitment messages. Investigators must ensure safeguards are in place for screening children, prisoners, and other special populations, unless these populations are the intended participants of the research project.

The research protocol should include procedures to authenticate potential participants, if appropriate. For example, investigators can provide each participant (in person or by regular postal mail or email) with a Personal Identification Number (PIN) to be used for authentication in subsequent internet/social media-based research data collection. The PIN used must not be one that could be used by others to identify the individual (*e.g.* Social Security number, etc.).

1.5 Compensation of Internet/Social Media-Based Research Participants

The use of compensated research panels, such as Amazon Mechanical Turk (mTurk), as a recruitment method for human participant studies continues to grow. Panels such as mTurk often advertise for panel participants 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 mention that the research project is "research" and not a "job." The compensation for the tasks accomplished is typically very small, usually less than $1.00.

Depending on the nature of the research, the IRB may request that methods of incentives and/or compensation allow participants to receive remuneration either without revealing their identities or without connecting their identities to survey responses. *For example:* Using gift certificates from online retailers and displaying the

unique certificate redemption number to respondents at the completion of an online survey. This allows participants to receive an incentive without revealing their identity.

1.6 Consent

1.6.1 The IRB does not allow passive consent for human subjects research participation (See SOP 701 Consent Process and Documentation for details about alternative consent processes). 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.

1.6.2 In real-time environments (including chatrooms, virtual worlds, multiplayer gaming “MMOG”, etc.) the process of requesting consent publicly is often perceived as disruptive. In such cases, investigators should consider announcing publicly that they are conducting research. Investigators may then request that people contact them via PM (private messaging using the site or platform in question), IM (instant messaging on another platform), email, website, etc. for more information about the research project and the process to become a participant.

1.6.3 When a waiver of consent documentation is requested, the information sheet used for consent must appear as the first page of 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 the participant with instructions for how to print or obtain a copy of the consent document when they are completing the online survey.

1.6.4 Depending on the level of risk, a single checkbox to Accept/Decline may not be acceptable. Since internet culture is such that people often check such boxes without reading the content, the investigator cannot assume that participant consent is legally effective. Instead of a single checkbox at the end of a consent form, investigators may use a checkbox for each item in the consent form, taking subjects through each step of the informed consent process. It is also possible that investigators will be required to obtain signed print copies of consent in some circumstances.

1.6.5 For surveys sent to and returned by participants through email, investigators should include an information sheet with consent information and inform participants that submitting the completed survey implies their consent. If PHI is included as part of content, the email must comply with HIPAA Privacy and Security regulations and University HIPAA policy.

1.6.6 For greater than minimal risk research, if the IRB does not approve a waiver of documentation of consent, the consent form can be mailed or emailed to the participant who can then sign the form and return it via fax, postal mail, or as an email attachment. If PHI is included as part of content, the email must comply with HIPAA Privacy and Security regulations and University HIPAA policy.

1.6.7 Some survey vendors and/or software packages provide a means to record whether a respondent has consented to participate before beginning the survey (e.g., a date/time stamp feature). Investigators should consider the use of this functionality.

1.6.8 Investigators subject to the Children's Online Privacy Protection Act (16 CFR Part 312) 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. For research that excludes minor participants, the IRB may ask the investigator to describe the procedures to be employed to authenticate that the participants are adults.

1.7 Consent Document: Confidentiality Section Addition

For internet/social media-based research, additional language must be added as part of the confidentiality statement in the consent document provided to the participant.

A disclosure included in the informed consent information provided to the participant stating, "*Please note that the survey(s) [is/are] being conducted with the help of [company name], a company not affiliated with the University and with its own privacy and security policies that you can find at its website."*

AND/OR: "This is an academic not-for-profit research project. 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 or privacy.

AND/OR: "Although every reasonable effort has been taken, confidentiality during actual Internet or email communication procedures cannot be guaranteed."

AND/OR: "Your confidentiality will be kept to the degree provided by the technology being used. No guarantees can be made regarding the interception of data sent via email or the Internet by any third parties."

AND/OR: "Data may exist on backups or server logs beyond the timeframe of this research project."

1.8 Consent Document: Voluntary Nature Section Addition

Survey question responses must be voluntary unless the consent document clearly indicates that answering a question is a requirement and reminds prospective participants that they may choose not to participate or stop participation in the research at any time.

If the participant completes an anonymous survey and then submits it to the investigator, the investigator may not be able to extract/remove/delete their specific data from the database should the participant wish it withdrawn. The consent document should inform prospective participants of this limitation.

1.9 Consent Document: Opt-in for Permission to Quote or Paraphrase Participants

1.9.1 If the research is not greater than minimal risk, the consent form may include an opt-in allowing quotation. Investigators are encouraged to omit or modify participant provided information that would be harmful if revealed so that the individual's identity cannot be linked to other publicly available data or re-identified.

1.9.2 For greater than minimal risk research, quotes from participants should be paraphrased so that they are not searchable. Searchable data may be traced back to individuals, thereby putting them at risk.

1.9.3 In some social media environments, the participants may have a persona with a pseudonym or may request that a pseudonym be used to protect the participant's identify. Pseudonyms and real names may be used with permission of individual participants.

1.9.4 Since individuals using social media may use pseudonyms to conceal their identities, investigators 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.

1.9.5 For greater than minimal risk research, pseudonyms and other identifying information (place, organizational affiliation, institutional names, etc.) should be changed. Additionally, false details may be deliberately introduced by the investigator to further protect research subjects.

1.10 Mobile Devices and Emerging Technologies

Additional considerations apply to research that involves the collection of data via social media applications that are networked with mobile devices or that involves 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 participant 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 participants on how to deactivate the app. Additionally, investigators should describe plans to ensure they do not continue to collect data once the research project is complete, in case a participant does not effectively deactivate the app.

If the research project involves the use of a mobile device provided by the investigator, the investigator 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 research project.

1.11 Technology-Assisted Survey Administration

Investigators can use a variety of software programs to conduct internet/social media-based research. These options fall within one of the following three broad categories:

1.11.1 Commercial or third-party survey creation and data collection hosting services. In these cases, the investigators often enter into a contract through the University with the vendor to provide some or all of the services related to the creation and management of the internet surveys. Investigators are advised to therefore collect data using third-party survey software, with known policies for data security and anonymity.

1.11.2 Surveys developed either internally or by using survey development software and hosted on web servers managed by investigators or by University IT services.

1.11.3 Surveys that are conducted via email, because the nature of the transmission to and from respondents may carry additional risks to confidentiality.

1.12 Data Security

1.12.1 Collecting data over the internet can increase potential risks to confidentiality because of third-party internet sites, the risk of interception by non-authorized persons when transmitting data across a network, and the impossibility of ensuring that data are completely destroyed once the research project is complete.

When conducting internet /social media-based research, if the investigator is not using a third-party internet site that has been previously approved by the University IT for use, then the investigator must demonstrate that the following minimum standards are met:

1. A standard encryption technology such as SSL is used.
2. The server is administered by a professionally-trained person with expertise in computer and Internet security.
3. Access to the data hosted on the server is limited to key project personnel and configured to minimize the possibility of external access to the server data.
4. How the security of the web server is being ensuredto prevent unauthorized access.
5. The server is subject to periodic vulnerability assessments to determine that the server is configured and patched according to industry best practices.

1.12.2 For certain studies that present greater than minimal risk to the participation, the IRB may elect to require additional protections, such as certified digital signatures for informed consent, technical separation of identifiers and data, or a higher level of encryption.

1.13 Data Management, Storage, and Destruction

Investigators are encouraged to keep the research participant's personal identifying information separate from the research data and to de-identify the research data set promptly after data collection. Both sets of data should be stored in encrypted format on an encrypted device or server.

Data backups must be stored in accordance with University IT data security and cloud storage security standards and other applicable Information Technology security policies. Encryption of backup data is also recommended. The investigator should consult with the Information Technology representative who is assigned to their academic department for assistance.

Competent data destruction services should be used to ensure that no data can be recovered from obsolete electronic media. Investigators should contact the University Information Technology office for services related to destruction of media content. It is advisable that the investigator receive assurance of the procedures used for the destruction of the materials and instruction on how to monitor the service.

2. SCOPE

This SOP applies to all human participant research conducted by investigators who conduct research under the auspices of the University.

3. RESPONSIBILITY

The investigator is responsible for verifying that any third-party internet sites that are to be used for research participant recruitment, consent, data collection, or data storage, or from which data will be transmitted to the investigator are approved by University IT Security.

If the investigator wishes to use a third-party internet site for research participant recruitment, consent, data collection, or data storage, or from which data will be transmitted to the investigator that has not already received University approval, the IRB administrator is responsible for providing a checklist to be completed by a representative of the third-party internet site. After satisfactory review of the third-party internet site provider by the IRB in consultation with Information Technology and Legal Counsel, as appropriate, the investigator and a representative from the third-party internet site are responsible for signing the Non-OU Employee Collaborator Assurance document provided by the IRB. The investigator is responsible for uploading the executed agreement into the IRB's electronic information system prior to approval of the research project.

The HRPP Director is responsible for reviewing the third-party internet site response to the checklist with other OU offices, as appropriate, in order to determine if the investigator will be allowed to use the proposed third-party internet site. The determination will be communicated to the IRB administrator.

The IRB administrator is responsible for providing the Non-OU Employee Collaborator Assurance document to the investigator.

4. APPLICABLE REGULATIONS AND GUIDELINES

University's Information Technology Office for Information Security policies and in particular, the Media Sanitization Policy and the Technology Hardware Disposal Service.

HIPAA Security policies

HIPAA Privacy policies

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

5. REFERENCES TO OTHER APPLICABLE SOPS

SOP 502J: Social Behavioral Research

SOP 701: Consent Process and Documentation

6. ATTACHMENTS

Third-party Internet Site Checklist

Non-OU Employee Collaborator Assurance

7. PROCESS OVERVIEW

7.1 Research submission processing will follow normal procedures in the applicable SOPs referenced in Section 5 of this SOP.

7.2 Based on the information provided by the investigator in the submission, the IRB Administrator will determine if the research involves internet or social media.

For studies involving internet/social media-based research, the reviewer will inform the investigator that an additional statement regarding internet/social media-based research must be included in the Confidentiality section of the informed consent document.

7.3 Based on the information provided by the investigator in the submission, the IRB Administrator will determine if the research involves a third-party internet site.

For studies involving human research activities hosted on a third-party internet site, the IRB administrator will confirm that the third-party internet site is on the University approved list. If not, the IRB administrator will provide the investigator with the checklist to be completed by a representative from the third-party internet site and returned to the IRB by the investigator using the IRB's electronic information system.

7.4 The HRPP Director reviews the third-party internet site response to the checklist with other OU offices as appropriate in order to determine if the investigator will be allowed to use the proposed third-party internet site. The HRPP Director will communicate the determination to the IRB administrator.

7.5 Once the IRB Administrator has determined that the third-party internet site is on the University approved list, they provide the investigator with the Non-OU Employee Collaborator Assurance document.

7.6 The research project can be approved when the signed Assurance document has been uploaded into the IRB's electronic information system.

APPROVED BY: _____ DATE: 09/09/2016

NEXT ESTABLISHED REVIEW DATE: AUGUST 2018