WHITWORTH
UNIVERSITY

Guidelines for Research Using Online Tools and Mobile Devices

The use of the online tools for research is increasingly prevalent. Email, surveys, social media sites, and mobile devices provide a quick way to gain access to a large number of potential subjects and information without expending too many resources. While this is good news for investigators, this raises many unresolved questions concerning recruitment, privacy, confidentiality, and informed consent. The current regulations do not address many of the unique issues associated with transmission of data over the Internet. This guidance is intended to review on a variety of issues surrounding research involving web-based tools and mobile devices and to help investigators design studies that are in line with the currently regulatory and ethical landscape.

Research using the Internet includes both use of the web as a tool for research and use of the web as a locale or venue of research. For example, research employing survey instruments, search engines, databases, or databanks would constitute using the web as a tool for research. Such research may not involve direct interaction with human subjects, but identifiers or personally identifiable information may be generated, collected, and/or analyzed. In contrast, using the web as a medium or locale of research entails qualitative or quantitative studies of various web-based spaces, such as chat rooms, virtual environments, or social media sites. Some of the most common uses of the web for research include:

- Research studying information that is already available online without direct interaction with human subjects (harvesting, mining, profiling, scraping – observation or recording of otherwise-existing data sets, chat room interactions, blogs, social media postings, etc.).
- Research that uses the web as a vehicle for recruiting or interacting, directly or indirectly with subjects (self-tests, survey tools, crowdsourcing sites, etc.).
- Research about the web itself (use patterns or effects of social media, search engines, email; evolution of privacy issues; information contagion; etc.).
- Research about web users – what they do online, and how that affects them and their behaviors.
- Research that utilizes the web as an interventional tool (e.g., interventions that influence subjects' behavior).
- Others (emerging and cross-platform types of research and methods, including mobile research).
- Recruitment in or through web locales or tools (e.g., websites, screening applications, social media, push technologies).

Definitions

- **Chatroom:** An online location where individuals can come together to have text-based discussions that occur in real time.
- **Data Mining:** The process of analyzing collected data from different perspectives and summarizing it into useful information.
- **Identifiable Private Information:** Information is identifiable if the identity of the subject is or may readily be ascertained by the investigator or associated with the information.
- **Private Information:** Information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public.

Confidentiality or Anonymity

Researchers conducting online research should be careful not to make guarantees of confidentiality or anonymity, as the security of transmissions over the Internet differs depending on the specific protections used. Investigators need to address how they intend to assure confidentiality of the data collected, keeping in mind that the degree of concern and protection is directly related to the sensitivity of the data.

- **Anonymity** means that either the project does not collect identifying information from individual subjects (name, address, email address, etc.) or the project cannot link individual responses with subjects' identities.
- **Confidentiality** means that only the investigator(s) or individuals collecting/analyzing data can identify the responses of individual subjects. However, the researchers must make every effort to prevent anyone outside of the project from connecting individual subjects with their responses.
- Data transmitted via email cannot be anonymous without employing additional steps. When using Qualtircs, select anonymize responses and prevent indexing. For other methods, make sure the settings prevent the entity from identifying the subject.
- Data transmitted over the Internet can be anonymous only if software is used to store the information directly in a database without identifiers; otherwise, identifiers are attached to the data. Web servers automatically already store information about visitors to a website and that information can be accessed by others.

Public versus Private Space

There are no regulations that speak to whether the internet is a public or private space.

A **public space** is one in which most participants have a reasonable expectation that anyone can read, cite, reproduce, link, collect, and share their contributions, statements, and media. Most social media environments fall within this definition. Examples include public profile pages of social media sites and services, public blogs, comment areas on news websites and many other forums. Certain social media services permit users to specify which content is accessible to the public at large and which is restricted. The term "public space" refers to areas of a website where there is an expectation, determined by privacy settings and or Terms of Use, that data will be publicly accessible.

- Normal public conventions should apply in the absence of information that indicates otherwise.
- When quoting comments from a public space, it may be appropriate to mask or hide the identity of the individual when negative consequences to the subject could reasonably arise from disclosure. Key considerations for hiding the identity of a subject include:

    - Sensitivity of the topic.
    - Inclusion of abusive or offensive language.
    - Discussion of anything unlawful, embarrassing, or likely to negatively
    - affect career opportunities.
    - Inclusion of personally identifiable information about the subject or
    - others (except when it is about a well-known person in the public
    - domain and it is not libelous).

A **private space** is available only to registered members in a location where users would expect their comments to be private. Although the process for gaining access may be nearly instantaneous, these spaces can be accessed and viewed only after the user has created a login and/or password designed to restrict all forms of access. Examples include many private forums, communities, and chatrooms, instant messaging systems, and forums/groups where an administrator or moderator controls admission and where content cannot be accessed or viewed by the general public.

- Because private spaces can be legitimately accessed only with a username and password granted and/or controlled by an administrator or moderator, researchers should obtain affirmative opt-in from subjects before using their content to conduct research.
- Researchers should also include reference to their role in interactions with members of the private space, so that existing and new members are never in doubt about the identity/role of the persons to whom they are talking.
- Researchers should observe great sensitivity when interacting with people in private spaces. As a general rule, they should not copy or collect content within private spaces, even if they have permission of the site owner, unless subjects are fully informed and have opted in to the process.
- If a researcher wishes to collect content in these environments, there should be total transparency, and the researcher should provide members with a process by which they may be excluded from such data collection.
- In a private space, researchers should seek explicit permission from subjects to quote their comments.

Data Collection

Web-based data collection methods can range from the use of existing data and observations to interventions and survey/interview procedures. Each is discussed below.

Existing Data: Research utilizing data that are both existing and public is not considered human subjects research and does not require IRB review. Data accessible only through special permission are generally not considered public. However, if steps are required to access data (e.g., registration/login, payment, etc.) but access is not restricted beyond these steps (e.g., anyone who creates a username and password can access the data) the data may qualify as publicly available. When determining whether data are public, the investigator must decide if there exists an expectation of privacy. If it is determined that the data were not intended for public use, even if the data are technically available to the public, the data should be considered private. Researchers accessing data that are identifiable or that when combined could readily be identifiable must obtain IRB review and approval.

Observations

When online research procedures are employed, the investigator must be sensitive to the definition of public behavior. Despite navigating in a public space, an individual may have an expectation of privacy, and investigators must be sensitive to that expectation. For example, an investigator wishes to collect data from discussions posted in an online community support group for substance abusers. The online community is technically public, in that anyone can view the discussions and join the group, but some group participants are there to provide personal experiences and support regarding substance abuse and may believe that all discussions and personally identifiable information will remain private.

Chatrooms

It is important that participants in a chatroom are able to let the researcher know if they are not comfortable with the researcher's presence there and that the researcher will respect their privacy. Because access to chatrooms can prove difficult for investigators and chatroom participants are not always eager to have a researcher in their midst, an alternative technique is for investigators to create their own chatrooms just for research purposes. Investigators can greet individuals joining the chatroom with a message informing them about the study and asking them for their informed consent. This is a good way to be sure that all participants are fully aware of the research and have consented to participate.

Surveys: Survey research is one of the most common forms of web-based research. Researchers are advised to format survey instruments in a way that will allow subjects to refuse to answer specific questions. For example, the list of responses can include an option such as "Decline to answer." In addition, subjects must always be given the option to withdraw from a study, even while in the middle of a survey.

Third-party online survey tools: Use of tools such as Qualtrics is permitted for most minimal risk studies employing online survey procedures. Investigators should

review confidentiality measures and data security policies for the given online survey tool and make sure that they are described in the protocol. If security measures are not in line with what the IRB requires, use of the given survey tool may not be approved. Research subjects also need to be informed of data security measures.

- Researchers should have a familiarity with the survey software being used, the types of information being collected (e.g., IP address, email address), the options the survey software offers regarding what information to collect, the ways in which information will be stored, and how any identifying information will be de-linked from survey data.
- Whitworth provides a survey tools that faculty, staff, and students can utilize for conducting online research surveys. Qualtrics is a cloud-based survey tool available for licensing through Whitworth University.

MTurk: Amazon's Mechanical Turk does not support participant anonymity. MTurk worker IDs are linked to Amazon.com public profiles. Amazon.com may disclose worker information. Additionally, worker information may be available to others (who submit a request) for tax reporting purposes. In light of these privacy concerns IRB materials need to inform study participants about how their MTurk worker IDs will be retained and used for study purposes and design the project to reduce privacy risks. The following are considerations for Informed Consent Procedures and/or Study documents

- Add a disclaimer that any work performed on MTurk can be linked to the user's public profile page. Workers may wish to restrict what information they choose to share in their public profile. Consider referencing Amazon.com's warning to workers: Http://www.mturk.com/mturk/contact this warning states that "Your email address will automatically be inserted into the message so the Requester (investigator) can reply to you." Amazon.com insert the workers' name as well. Therefore, it is possible that when a worker makes contact with you that their name and email address will be included.
- Add a statement in the consent explaining the MTurk worker IDs (I.e., the 14 character sequence of letter and numbers used to identify workers) will NOT be shared with anyone.
- If there will be study compensation, add a statement in the consent that MTurk worker IDs will only be collected for the purposes of distributing compensation and will not be associated with survey responses.
- Add in the "privacy and confidentiality" section that MTurk worker IDs will not be shared with anyone outside of the research team, will be removed from the data set, and/or will not be linked to survey/study responses (as applicable).

Survey Monkey: You can use Skip Logic to disqualify respondents who don't consent to being surveyed. It is up to every survey creator to decide to collect responses anonymously or to capture respondents' personal information. You can set the time-frame in which the data remains at Survey Monkey. Survey monkey uses cookies, but does not use targeted advertising cookies on survey pages. Survey Monkey requests that you identify:

- What personal information you are collecting and whether you are collecting the responses anonymously or if you're tracking them by email address, name, ticket number, etc.
- How you plan to use the responses
- Whether the responses will be disclosed to anyone else
- Can the respondents access their responses to correct or request that any personal information collected about them be deleted
- They also ask that you avoid any sensitive information and collect only the minimum amount of personal information.
- Opt out of benchmarking

Interviews: Conducting interviews online allows researchers to gather information from respondents who would have been difficult to contact otherwise, such as those at too great a geographic distance or otherwise unable to participate in person. Interviews may be conducted online using email or chat applications. When conversing with a research subject via online chat in text only, investigators should take into account the inability to read visual and auditory cues, which can lead to possible misinterpretation of both questions and responses. Voice intonation and facial expressions are often used to convey meaning. Thus, investigators may need to ask clarifying questions in order to accurately interpret responses, and may need to provide additional information in order to be sure that subjects understand the questions. If interviews are to be audio- or video-recorded, subjects should be informed prior to agreeing to participate.

Social Media as a Recruitment Tool

Investigators are using social media and other online forums to identify and contact potential subjects for participation in all kinds of research, from surveys to clinical trials. Because subjects self-identify on social media and other websites and choose which sites and forums to join, investigators can target subjects with specific interests, making recruitment efforts more effective and efficient. Online recruitment is conducted via many different forums and methods, including electronic flyers posted on social media sites, messages to social media groups, websites devoted to clinical trials, and even posts on blogs and discussion groups/boards. Regardless of the specific recruitment method, investigators should consider the following guidelines when using online forums for recruitment purposes.

<u>Advertising content</u>

- Recruitment materials available on the online should follow the same guidelines applicable to traditional recruitment methods.
- Recruitment is the first step in the informed consent process; as such, all materials presented to potential subjects must be reviewed and approved by the IRB.
- Recruitment materials should include investigator contact information, information about the purpose of the study, any eligibility criteria, benefits to the subject, and time commitment required for participation in the study.

- Materials should never promise free medical treatment, imply unanticipated benefits, or emphasize payment.
- Websites and recruitment materials for clinical trials and FDA-regulated research may not make claims inconsistent with approved FDA labeling, must indicate when drugs and/or devices are investigational, and may not offer post-approval discounts on drug/device costs in return for participation in the study.

Initial contact of potential subjects

- Despite the public nature of social media and the web, investigators should carefully consider ethical recruitment practices and subjects' privacy when determining how subjects will be contacted.
- Contact methods must be clearly described in IRB documentation
- Unsolicited recruitment ("cold contact") of individual potential subjects via social media is strongly discouraged. The IRBs would generally expect that initial contact with a potential subject be conducted by someone whom the potential subject would recognize, either because the individual has connected with or followed the study team or has otherwise agreed to be contacted, or because the recruiting individual is a part of the potential subject's care team
- Recruitment from the researcher's own social media page or recruitment within a ***public*** group on a social media site is generally acceptable. However, researchers should not join a ***private*** social media group for the purposes of recruiting subjects into a research study.

Sharing of potential subject data

- The recruitment process logistically necessitates the sharing of data between the potential subject and the study team. During initial IRB review, investigators must describe provisions for protecting confidentiality of potential subjects and subjects. Such provisions are especially critical when recruitment is conducted online.
- Investigators should never request that potential subjects provide identifiable information via public forums, including tweeting, private messaging, posting, etc.
- Potential subjects interested in participation should be directed to contact the study team via non-public means.
- Health information should never be shared via email or social media contact methods.

Using Social Media for Subject Contact and Follow-Up

Online forums may be an effective way to stay in contact with subjects after they've agreed to participate in the study. However, subjects should prospectively be informed of and consent to the possibility of electronic contact.

- The informed consent process should clearly describe any anticipated contact via social media or other electronic forum.
- Subjects should provide consent to be contacted via social media.
- If they agree, subjects should provide their Facebook profile names, Twitter handles, etc., to the study team for contact purposes.
- If contact via social media and other electronic means is anticipated, the HIPAA authorization should clearly request authorization for such contact.

- If subjects do not prospectively consent to contact via social media or other online forums, the study team may request permission to do so from the IRB by requesting a waiver of informed consent for this purpose and justifying it appropriately. Such a request should include:
  - A plan for ensuring that the study team identifies the correct individuals.
  - A copy of the planned contact language. Language must not imply or share potential confidential information, including protected health information.

Research with Mobile Devices/Applications

Many research projects utilize mobile applications either as a tool for collecting research data or as the object of the research. This type of research may involve the use of existing data and/or interaction with or intervention in the person's environment. Additional considerations apply to research that involves the collection of data via social media applications that are networked with mobile devices, or through installed applications on a person's mobile device to collect data.

- Researchers must explicitly inform subjects of the data they will be collecting via the mobile device, include GPS location.
  - If the researchers do not plan to collect GPS location information from the subjects, they should explicitly inform subjects of this and provide instructions for deactivating the device's location services.
- 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 subjects 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 subject 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 he/she 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.
- Some mobile apps are regulated by the FDA as medical devices. In general, if a mobile app performs the same function as a medical device (i.e., intended for diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease), it may be subject to FDA regulations and requirements. IRB documentation should clearly describe the purpose of any mobile apps in order to assist HSO staff in determining whether FDA regulations may apply.

Secondary Subjects

Mobile device studies are particularly likely to capture information about persons who are not the intended (and consented) subjects of the research.

- Researchers should prepare themselves for this possibility and take steps to limit the amount of information gathered.
  - Can subjects turn the device off to avoid recording information in inappropriate locations?
  - Can subjects effectively advise other people of their participation?

- Does the study require the subject to download a software app? Was the app created specifically for this study, or was it created by a third party?
  - For third party apps, the researcher needs to be familiar with the terms and conditions and direct subjects to review it. The researcher should also know what information the app sends to the app developer.
- Does the study rely on the subject's data plan to transmit data?
  - The research should advise the subject that participation could lead to increased costs, and if possible provide an estimate for data use.

Consent Issues:

- As with research conducted in offline settings, researchers employing web-based surveys still have a responsibility to inform prospective subjects about the research and any potential risks associated with their participation. For most web-based surveys, it is not practical to obtain *signed* consent from subjects. As such, for non-exempt studies, the researcher should request from the IRB a waiver of documentation of informed consent.
- Generally it is appropriate to simply state in the information provided to potential subjects that by completing and submitting a survey, or completing a research task, consent is implied. Other times, researchers may wish to include an "I agree" button that must be clicked before proceeding to the research procedures.
- Research conducted via a third-party site may result in the retention by the third party of data provided by subjects, and should be noted as appropriate.
  - A written consent form may not be the best way to ensure that subjects are informed about the study. While still needed so that subjects can save or print a form for their own records, the consent process may involve videos, interactive forms, or other online methods that more effectively convey the needed information.

Child Issues:

- Obtaining parental consent for online research with minors will rarely be practical. Even if a researcher attempts to obtain parental consent, it is likely not verifiable.
  - A waiver of parental consent will likely be needed for any online research involving children. However, depending on the nature of the research, the researcher should suggest that their potential child subjects inform their parents of the research and their involvement, as appropriate.
- Contacting adolescents for research purposes is different from contacting younger children. Adolescents are considerably more likely to already have an online presence and have much greater freedom and decision-making capacity than younger children.
  - The minimum age/grade level for inclusion in online/mobile device research without parental consent is thirteen (13), in compliance with COPPA.
- Researchers should consider the possibility that a parent may discover that his/her child is taking part in a research study about which he/she was not previously notified. This could lead to increased risk for child subjects, as their confidentiality could be more at risk and they could be subject to punishment for participating without their parents' knowledge. The researcher and Whitworth could also be put at risk.
  - Researchers should note these risks and take appropriate measures to protect against them.
- **COPPA:** Operators of commercial websites and online services directed toward children under 13 years of age that collect personal information from these children must comply with the federal Children's Online Privacy Protection Act (COPPA). The goal of COPPA is to protect children's privacy and safety online, in recognition of the

easy access that children often have to the web. COPPA requires website operators to post a privacy policy on their website and create a mechanism by which parents can control what information is collected from their children and how such information may be used. For more information, please see: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/childrens.html.

- Research conducted online meant to exclude children should consider including a statement in the study information that the research is intended only for individuals 18 years of age and older. For example: *This research is intended for individuals 18 years of age or older. If you are under age 18, do not complete the survey.*

Transnational Issues:

As with all international research, activities and behavior that are acceptable/legal in the United States may not be in other countries.

- Researchers should carefully target their intended audience.
- Research on topics likely to be problematic (e.g., sexual behavior in Saudi Arabia, attitudes toward government censorship in China) should include information regarding any risks and plans to protect against them.
- Because the Internet reaches across borders, it can be difficult if not impossible to exclude individuals outside the United States from participating in research conducted online. Therefore, researchers should consider the inclusion of a statement in the study information that the research is intended for residents of the United States only. For example: *This research is for residents of the United States. If you are not a U.S. resident, do not complete the survey.* If researchers wish to target and/or include non-U.S. residents, or transnational subjects, they should be familiar with applicable local laws in the country(ies) where those subjects reside.
- If you are considering this type of research, please discuss with Sponsored Programs.

General Issues:

- Many websites used to recruit research subjects or conduct research procedures include terms and conditions to which members and/or visitors of the website are bound. Researchers should familiarize themselves with the terms and conditions of any websites they intend to recruit from or conduct research on to ensure subjects are not asked to violate a service agreement.
- Researchers should consider informing subjects that they should be aware of the terms and conditions of the website to understand what, if any, data may be used/maintained by the website itself. For example: *Before you begin, please note that the data you provide may be collected and used by [survey agency/website] according to its user privacy agreement or terms of service*.
- 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 informed consent and study information. Some examples of statements you may want to share with subjects include:
  - *"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."*

- *"Data may exist on backups or server logs beyond the time frame of this research project."*
- Recruitment via social media or other sites may unintentionally reveal information about the subject to a third party unless ads specifically target individuals with traits already publicly disclosed.

Data Collection and Storage:

- Depending on the level of sensitivity of the data being collected, consideration should be given to where the data will be stored. For example, the use of a third-party survey tool is likely adequate for a de-identified survey collecting innocuous data.
- Data that is not de-identified or anonymous and is more sensitive in nature, such as illegal activities, should utilize a more secure data collection and storage method, such as those IU makes available.
- Researchers should also consider informing subjects where their data will be stored, especially if a breach of the data could cause increased risk of harm to the subjects.
- Whitworth University provides additional resources to assist researchers in the appropriate means of data storage, contact Sponsored Programs.