CUNY HRPP Guidance: Internet or Mobile Technology Based Human Subject Research

1. Purpose

The purpose of this document is to provide guidance to CUNY's research community concerning responsibilities and considerations related to Internet or mobile technology based human subject research.

2. Applicability

These guidelines are applicable to the use of the Internet or mobile technology as a tool for subject recruitment; as a tool for data collection, whereby researchers use existing information without engaging source participants; and to the use of the Internet or mobile technology as a tool for data collection, where researchers engage with the source participants.

Examples of Internet or mobile technology sources include: public email archives, blogs, data repositories, cloud data services, Facebook, Twitter, RSS feed, Amazon Mechanical Turk and mobile applications/GPS technology.

3. Privacy and Confidentiality Considerations

Researchers and IRBs must ensure that adequate provisions are in place to maintain confidentiality of research data and privacy of research subjects. When evaluating subject privacy, researchers and IRBs must take the following into consideration:

- Depending on the nature of subject data being collected, it may be possible to combine de-identified data with other available datasets to identify the individual subjects. The researchers and the IRBs should consider a) the implications of one's ability to re-identify subjects; and b) provisions for accurately informing subjects of mechanisms in place for ensuring confidentiality of research data as opposed to ensuring anonymity.

- Potential subjects may not have a complete understanding of the privacy policies associated with their use of the Internet or mobile technology. Therefore, the principal investigators are responsible for a) becoming familiar with the terms of service and privacy policy for each Internet venue or mobile technology to be used in their respective research prior to the implementation of human subject research activities; b) providing the IRB with their assessment of how best to safeguard subject privacy and confidentiality based on the tools being used; c) ensuring that all research team members are trained in adequately safeguarding human subjects of research given the nature of the tools being used; and d) informing subjects of the risks of invasion of privacy and breach of confidentiality associated with the specific use of the Internet venue or mobile technology, and the safeguards the researchers will use to protect the subjects from such invasion or breach.

- Researchers should ensure that research data is kept confidential, both physically and electronically. In doing so, CUNY researchers are required to comply with section 12 of CUNY Policy on Acceptable Use of Computer Resources. The HRPP/IRB may require additional safeguards, as appropriate.

- Some Internet venues, such as Amazon Mechanical Turk, store identifying information about their users. When using such a venue for subject recruitment, researchers are strongly encouraged to use a different venue, such as Survey Monkey and Qualtrics, for data collection purposes. This type of strategy allows for separation of subject identifiers from other subject data, and adds another layer of protection from breach of subject confidentiality.

- CUNY researchers are required to use their CUNY email address for communications related to research in which CUNY is engaged; and when registering with online services, databases, cloud services, etc. for CUNY research-related purposes.

4. Informed Consent Considerations

The researchers and the IRB must consider the following when evaluating the informed consent process and document associated with non-exempt Internet based human subject research:

- When appropriate, CUNY UI-IRBs may grant a waiver of informed consent or a waiver of documented informed consent in accordance with CUNY HRPP Policy: Informed Consent Process and Documentation. For research that meets the criteria for a waiver of documented informed consent, informed consent may be obtained via a research information site. The information site should provide potential subjects with information about the research, and a button to click to agree to participate. The contents of the information site must receive CUNY UI-IRB review and approval prior to implementation.

    - Other mechanisms for obtaining Internet or mobile technology based informed consent may also be used as appropriate for the venue and when approved by the IRB.

5. Cloud Computing

When using cloud services or applications, where it is typical that virtualization obscures the underlying infrastructure and data protections of the cloud service provider, particular care must be taken. Researchers must nevertheless ensure that:

- Research data remains in possession and control of the researcher;

- Export restrictions are observed;

- Unauthorized individuals do not have access to sensitive and/or confidential research data;

- Unauthorized individuals are not able to store personal copies of the research dataset; and

- The data access and storage mechanisms allow for compliance with CUNY's Intellectual Property Policy.

6. **Age Verification**

   Researchers must incorporate mechanisms to ensure that the subjects enrolled in the research meet the study's inclusion/exclusion criteria, including age limitations. Thus, researchers are encouraged to use multiple confirmation points for age verification, i.e. asking for a subject's age in different formats (age, date of birth, etc.) at different points during research participation.

References

1. Code of Federal Regulations, Title 45 – Public Welfare DHHS, Part 46 – Protection of Human Subjects

2. Paolacci, G., J. Chandler, and P.G. Ipeirotis. "*Running Experiments on Amazon Mechanical Turk*," Judgment and Decision Making, Vol. 5, No. 5, August 2010, pp 411-419.

3. Buchanan, Elizabeth A. and Zimmer, Michael, "Internet Research Ethics", *The Stanford Encyclopedia of Philosophy* (Fall 2013 Edition), Edward N. Zalta (ed.), forthcoming URL = http://plato.stanford.edu/archives/fall2013/entries/ethics-internet-research/