Qualitative Transparency Deliberations

hosted by the Social Science Research Institute at Duke University on behalf of the APSA Section for Qualitative and Multi-Method Research
https://www.qualtd.net/

Cybersecurity and work with human subjects

https://www.qualtd.net/viewtopic.php?f=18&t=181

Cybersecurity and work with human subjects

Posted: **Fri Nov 18, 2016 3:21 pm**
by **aepost**
There are scholarly reasons, as others have noted, for sharing the data we collect from human subjects. Others may be able to build on our work, and knowledge thus accumulate more quickly. It may provide disincentives against misrepresenting evidence. In addition, funding bodies are increasingly requiring that data they finance the collection of be shared with the broader community.

One concern that has not yet been raised in this forum, however, is how cybersecurity should factor into our decision-making regarding the costs and benefits of transparency, and particularly graduated or intermediate forms of data sharing. Cyber "insecurity" may affect the circumstances under which data from human subjects may be shared without endangering participants.

It is important to consider the increasing insecurity of digital storage systems. When sharing transcripts or recordings with journals or a repository (even with access restrictions in place, such as limiting access to members of the scholarly community), one is relinquishing control over the materials, and thus is unable to personally ensure that materials are not broadly disseminated by accident. This is abundantly clear as instances of hacking facilitated by sophisticated phishing schemes proliferate. (I would certainly never fault a journal or QDR if they were hacked by the Chinese or wikileaks, given that the U.S. government has fallen prey to attacks.) Perhaps the way forward is to give researchers the leeway to decide what level of sharing is truly unlikely to put subjects further at risk than they are already, based on their knowledge of the context in which they work, the nature of their IRB approval, content of the interview, etc. This will likely mean sharing transcripts or notes from some interviews (perhaps those that can be realistically anonymized, or where the subject matter could in no way be conceived of as objectionable) and keeping others on one's own computer (with names coded, etc., and nothing stored on the cloud.) Usually, references to anonymous interviews are complemented by material from other sources in articles, so it does not seem unreasonable to ask journals to be accommodating on this front.

My concerns about security do not just pertain to interview data. It is also becoming increasingly difficult to anonymize survey data in an age of big data. My colleagues in more technical disciplines maintain that there is sufficient data on most individuals in countries like the US that much survey data collected these days can be traced back to specific individuals. This is particularly the case for geo-referenced data such as that collected through cell phones. As we move towards tablet-based surveys that collect GPS coordinates, etc. it is incumbent upon us to ensure that measures we take to anonymize data are in fact effective, and if not, that

survey responses would not put respondents at risk.

Re: Cybersecurity and work with human subjects

Posted: **Sat Dec 17, 2016 2:46 pm**
by **AnastasiaSh**
Thank you, Pr. Post, for highlighting cyber "insecurity" as a critical issue in the discussion of transparency in the discipline. Do you have suggestions or examples of the more effective measures to anonymize data?

Powered by phpBB® Forum Software © phpBB Limited
https://www.phpbb.com/