Architecting Global Ethics Awareness in Transnational Research Programs

John Murray, SRI International, Silicon Valley CA

jxm@sri.com

November 2015

Summary: Traditionally, the ethical principles that guide scientific studies involving people are primarily intended to cover direct *human-centered* research. However, in the modern online world, cyber-centric research is inherently *data-centered* in nature, and researchers frequently operate with limited awareness of the potential human risks and effects of their activities. Indeed, the nature of their work is such that any organizational oversight of their research may be absent. Recently, a series of updates to the U.S. policies and regulations governing Institutional Review Boards have been proposed, which are likely to have a significant impact on the online research community. However, since online studies inherently cross the boundaries of multiple jurisdictions, there is now an even greater need for harmonizing ethics observance regulations and guidelines in a global context.

Recent developments in the field of cybersecurity studies have focused attention upon the ethics involved in undertaking such academic research. In particular, such discussions often center upon the challenges of publishing articles that discuss cybersecurity explorations and exploits, which may reveal potential or real system exposures or vulnerabilities.

While the moral dilemmas of revealing system vulnerabilities in academic publications are indeed important, they generally come towards the end of a (potentially lengthy) research effort, well after other damage may already have be done. In reality, the actual ethical challenges should have been considered much earlier in the process, when the research team were designing their initial investigations and data collection activities.

The policies and standards based on the 1979 Belmont Report [1], which are used to guide scientific ethics reviews across the U.S. and beyond, have limited practical relevance to modern human data collection and analysis activities that involve highly-networked information and communications technology (ICT) systems.

Consider for example the case of Batea (https://batea.docgraph.com/study/), which is a web browser extension that research volunteers can download and install, in order to track their use of Wikipedia's health related materials. The tool watches what they do within the site, and one step away from it when they link out. The idea is to gain insight into the way that people use the health resources on Wikipedia, in order to help develop the software, policies, and social infrastructure necessary to support such usage of Wikipedia in the most natural fashion.

The problem is that collecting such data could be invasive or the resulting logs could be misused. The tool could also potentially form a slippery slope into less ethically designed research by others, or it could introduce a hacking vulnerability within the

browser system. However, because of the distributed and voluntary nature of the Wikipedia community, it's not clear how domain-knowledgeable ethics reviewers should be involved, to provide diligent oversight of the research activities.

In the broader field of online studies in general, these 'locus-of-overview' impracticalities are exacerbated by the pervasive need to undertake comprehensive, transnational experimental projects, where much of the human data collection and analysis is undertaken remotely across varied, and often incompatible, legal regimes and social norms. Yet such is the case for numerous researchers nowadays, who are studying ubiquitous social networks and global crowd-sourcing applications, as well as online educational and gaming environments, cybersecurity tools, surveillance systems, etc.

In consideration of these challenges, the Menlo Report[2] was specifically developed to address issues of online security, privacy, anonymity, and other personal identifiable information (PII) concerns. The report's authors recognized that the broad cyber-research community needs a more rational and coordinated strategy for managing ethics observance, which particularly considers the scope and needs of ICT research. Such a tailored approach should emphasize studies of human behavior and community activity online, and apply across multiple jurisdictions in interactive professional and social environments.

This transition of some of these concerns into formal policies and regulations recently progressed with the publication of a Notice of Proposed Rulemaking (NPRM) in the U.S. Federal Register[3]. This serves to promote conversation and comment from parties affected by the proposed changes. The latest period for public comments on the NPRM is open until January 2016. As they currently stand, some of the proposed changes may have significant implications for trans-national cyber-research. One key concern is the extent that they might exacerbate the differences between human subjects research requirements in the U.S. and elsewhere, while at the same time relaxing some of the more stringent requirements that currently apply to the U.S. research community.

Traditional ethics reviewers try to ensure equitable distributions of burdens and benefits among the human subjects actually involved in the study. However, online research activity can also adversely affect innocent bystanders and neutral non-participants. Given the risks associated with real-time data-intensive experiments, such studies might better be reviewed in terms of *human-harming* research, rather than *human subjects* research.

For example, solid contingency and response plans are needed for mitigation of realized harms, especially for low-probability/high-impact events. These types of safety monitoring procedures are standard in traditional biomedical studies, but are rarely considered in ICT research. Furthermore, when research involves surveillance, profiling, or monitoring, additional vulnerability protections are needed to prevent the misuse of findings and results. This is particularly the case when novel mergers of partial data from several public sources may produce PII that is not individually available from just one of them. Other concerns arise from

the potential for abuse of data for social discrimination, especially by non-investigators.

Provisions are required to ensure conformance with international regulations on transborder data flow that include personal information. In this regard, the current oversight policies and data handling processes for multi-jurisdictional ethics approvals are primarily centered upon the requirements of pharmaceutical drug trials, medical device tests, etc., rather than on the research needs in global-scale social science, human-machine systems, and ICT.

To address this gap, an international ethics observance organization is needed, which would coordinate/oversee regulations and guidelines for research in online systems and other cyber-environments across multiple jurisdictions. This could be a consortium of non-profit organizations in several domains, which would ensure smooth transnational processing of approvals. It seems appropriate that such a consortium would need to have the backing of a recognized international entity such as UNESCO.

The first steps toward such harmonization could be merely a matter of coordinating and making available the critical features of each local research context, or it could extend to negotiating safe harbors for compliance with local research context. Thus, if a study complies with certain key components, then it is deemed to satisfy local research context requirements for specific countries. Another, further step might be to aim for legislative harmonization on the topic of research protection.

The bottom line is that almost any form of standardized ethical framework would help cyberspace researchers worldwide become more aware of the challenges and know when they have addressed some required basic considerations. This must be better than the current haphazard obstacle course, which generally leaves everyone guessing as to what they still need to do, to work through this ethical minefield.

References:

[1]: *www.hhs.gov/ohrp/humansubjects/guidance/belmont.html*

[2]: *www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCOMPANION-20120103-r731_0.pdf*

[3]: *www.federalregister.gov/articles/2015/09/08/2015-21756/federal-policy-for-the-protection-of-human-subjects*

Dr. John Murray is a Program Director in the Computer Science Laboratory at SRI International. His research interests encompass interactive collaborative systems, software engineering, cognitive ergonomics, and human-machine systems. He has led many innovative interdisciplinary systems research and development projects both in academia and in industry, and has held technical leadership and executive management positions at several international corporations. His technical experience includes diagnostic modeling in complex networked systems, human behavior modeling in computer gaming studies, smart product design, and mobile wearable computer systems. Dr. Murray has received advanced degrees from Dublin Institute of Technology in Ireland, Stanford University, and the U. of Michigan, where he was also an adjunct faculty member. He is also a Visiting Scientist in the College of Science at San Jose State University.