UNIVERSITY OF CALIFORNIA PRESS
JOURNALS + DIGITAL PUBLISHING

Computer Science Security Research and Human Subjects: Emerging Considerations for Research Ethics Boards

Author(s): Elizabeth Buchanan, John Aycock, Scott Dexter, David Dittrich, Erin Hvizdak

Reviewed work(s):
Source: *Journal of Empirical Research on Human Research Ethics: An International Journal*, Vol. 6, No. 2 (June 2011), pp. 71-83
Published by: University of California Press
Stable URL: http://www.jstor.org/stable/10.1525/jer.2011.6.2.71
Accessed: 29/02/2012 07:52

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

University of California Press is collaborating with JSTOR to digitize, preserve and extend access to *Journal of Empirical Research on Human Research Ethics: An International Journal.*

http://www.jstor.org

Computer Science Security Research and Human Subjects: Emerging Considerations for Research Ethics Boards

Elizabeth Buchanan
University of Wisconsin–Stout

John Aycock
University of Calgary

Scott Dexter
Brooklyn College, City University of New York

David Dittrich
University of Washington

Erin Hvizdak
Loyola University Chicago

ABSTRACT: this paper explores the growing concerns with computer science research, and in particular, computer security research and its relationship with the committees that review human subjects research. It offers cases that review boards are likely to confront, and provides a context for appropriate consideration of such research, as issues of bots, clouds, and worms enter the discourse of human subjects review.

KEY WORDS: computer science research, computer ethics, computer security, data security, human subjects review, Internet research, research ethics, research regulation, IRB, research ethics boards

Received: December 19, 2010; revised: April 13, 2011

Computer Science (CS) is largely focused on the care and feeding of the electronic devices our societies have come to rely upon, ranging from personal computers to mobile devices and embedded identification chips. Throughout this paper, we follow the CS definition given in Denning et al. (1989): "Computer science [...] is the systematic study of algorithmic processes—their theory, analysis, design, efficiency, implementation, and application—that describe and transform information" (p. 16). The range of possibilities for research on these tools, given this definition, is vast and increasingly complex from a human subjects perspective. CS research might be empirical, theoretical, or some combination of the two, and encompasses a broad range of research areas, ranging from studies on systems and/or data security to the construction of virtual reality and artificial intelligence (ACM, 1998).

In the brief history of the discipline, relatively little CS research has directly involved *human subjects* as defined by the United States federal research regulations (45 CFR 46 [102]), which define a human subject as "a living individual about whom an investigator (whether professional or student) conducting research obtains (1) Data through intervention or interaction with the individual, or (2) Identifiable private information."

There are two important implications of this. First, CS research does not readily fit into extant research ethics guidelines or review models that were developed primarily for the medical/biomedical and social sciences. Second, CS researchers themselves may not fully understand or believe that their projects align with the same ethical concerns that pertain to human subjects, such as the minimization of risk or harm to individuals, confidentiality, privacy, and just recruitment methods. CS research, broadly conceived, is concerned with systems and processes, and the connection to individuals may not be directly evident. The connection between a disparate piece of data and a human subject may, indeed, be a stretch. But, as the line between human and data continues to blur, especially in the realms of CS research, it is important that we consider the relationship between current ethics guidelines and regulations in light of CS research, so that we ensure that such research is conducted with a strong understanding of broadly accepted ethical standards. Those standards are grounded in medical and biomedical perspectives, and have grown out of the U.S. regulatory context which, in turn, grew out of the research atrocities of Nuremberg and Tuskegee. From the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research and the Belmont Report, three foundational principles of research ethics emerged: respect for persons, beneficence, and justice.

As empirical research on human subjects grows in the computer sciences (Moløkken-Østvold, 2005 and Hall &

Journal of Empirical Research on Human Research Ethics, pp. 71–83. print issn 1556-2646, online issn 1556-2654. © 2011 by joan sieber. all rights reserved. please direct all requests for permissions to photocopy or reproduce article content through the university of california press's rights and permissions website, http://www.ucpressjournals.com/reprintinfo.asp.
DOI: 10.1525/jer.2011.6.2.71

Flynn, 2001), these three principles must be examined in the context of the CS discipline and its research practices. The subdiscipline of HCI (Human-Computer Interaction) is obviously an area where researchers have considered human subjects concerns, and have adapted to the review framework of research ethics boards (REBs) in their presentation of the risk-benefit, consent, and recruitment aspects of their research. But, increasingly, data aggregation, transaction log analyses, and data mining processes implicate human subjects, and these forms of research do not fit readily into the typical regulatory framework. As such research expands, forms of data become more representative of, and more fitting to, human subjects, sometimes unwittingly and unintentionally.

For example, a current research project at Carnegie Mellon includes building hallway robots that capture data about passersby (Sweeney, 2003); research that examines and captures human movements in the forms of geocoding or geolocation-based stamping (Krieger et al., 2005); research on implantable medical devices (Dittrich, Bailey, & Dietrich, 2009); and research that uses such tools as Google Earth images as forms of qualitative data. Researchers across disciplines are grappling with the myriad human subjects–related implications for such emergent computer technologies. For instance, Myers (2010) has accurately noted that, "Along with the concern about dehumanization of research subjects is the simple fact that the people captured by Google's satellites have no say in the recording of their persons and properties and no say in their online representations" (p. 10). Researchers across disciplines, including CS, are experiencing novel forms of "personhood" in the guise of avatars, bots, and artificial agents,[1] many of which are actively involved in the research enterprise itself: Avatars research other avatars, bots scrape data from websites, artificial agents can act morally or immorally, or can engage in ethical or unethical research (Floridi, 2004, 2010). Albrecht (2009) has provided a strong philosophical argument supporting the notion that avatars do meet standards for human subjects based on a Kantian analysis. She argues that an avatar is rational, behaves humanly, interacts with other rational individuals of the same kind, and as an individual, ought to be treated as an end in himself or herself and not as a means to some other end; that is, as a human.

These brief examples indicate that CS research is diverse, evolving, and directly challenging notions of *human subjects* research. CS is, moreover, interdisciplinary and international or transborder in scope and reach, and thus CS research is a varied and diverse field in which legal, ethical, and policy concerns can and most certainly do arise at multiple junctures or moments. While disciplinarily distinct, CS may share more commonalities with Internet research at the current time in terms of its alignment with REBs.

In the past ten years, REBs across the United States and abroad have been focusing on Internet research, as more research is conducted through the Internet. For example, REBs have been evaluating studies involving online information collection via online surveys, studies of how people use the Internet, online ethnography, online interviewing, and uses of online datasets, databases, databanks, and repositories. However, in a study of 700 U.S.-based REBs, Buchanan and Ess (2009) found that few boards were reviewing research from CS departments. The majority of online or Internet-related protocols were received from social sciences and medicine, with the fewest coming from the arts and humanities and engineering/applied sciences. The types of ethical challenges reported most frequently by respondents concerned issues around data storage, access and retention in cloud space, encryption of data, privacy, and concerns of data security. In many cases, Buchanan and Ess found that REBs did not know exactly what issues to consider as problematic or potentially harmful. IP addresses, clouds, worms, and bots are not part of the standard vocabulary of human subjects research protections.[2] For example, one respondent commented that "most REB members don't have degrees in CS," while another respondent noted, "I would suggest that all of the REB concerns should be discussed with IT professionals and have a set of standards developed for REB members/professionals to follow. We must remember the turnover rate of REB is high so this standard would help PIs and the REB stay consistent." To this end, Buchanan and Hvizdak (2009) have suggested that boards retain such an expert member from an IT unit or from the CSs. In subsequent research, Buchanan and Ess found that a small number of REBs were bringing in an IT expert or, in one case, a computer scientist with an expertise in security, to their membership. In this particular case, the university was located in an area of large-scale tech companies with robust CS research efforts. The board felt it necessary to have a specific member of the board well versed in online research, and specifically CS research to "[teach] the board a new vocabulary and [explain] the hard-core tech research to the rest of us so we know what to look for."

While Internet research poses ethical quandaries concerning anonymity, pseudonymity, identification, consent, and virtual harms (see, for example, Buchanan, 2010; Buchanan & Ess, 2009), CS research presents similar ethical concerns, but the direct impacts on human subjects may be less evident and harder for an REB to

see immediately (as will be illustrated subsequently). Harm, or risk, may be further "downstream" in CS research than in other disciplinary forms of Internet social-behavioral research, such as studies coming out of communication, mass communications, or anthropology, where *an* individual or *a* community is the direct focus of a study. In those contexts, there is a subject who is being interviewed or observed or surveyed; or an individual or a community's postings are a data source. Risk is presented in traditional forms, such as discomfort with answering questions, inconvenience with the time involved in research activities, risk to reputation, and similar potential harms. Certainly Internet-based social-behavioral research runs along a continuum, where sensitive information may be collected from a higher risk population, such as online ethnographies from pro-anorexic (Dias, 2003) or cutting/self-mutilation websites. Risks go beyond data and privacy, and also include availability, integrity of data, and information systems (Aycock et al., 2011). However, much Internet research reviewed by REBs falls under exempt or minimal risk (Buchanan & Ess, 2009).

Confusing REBs even further, as they review protocols from both the novel realms of Internet research and CS research, is the subdiscipline of *computer security*. *Computer security* is defined less precisely than the larger realm of CS, and intersects a variety of disciplines, such as applied security, cryptography, number theory, psychology, and law. It is a subdiscipline that grew out of larger CS interests in privacy, encryption, fault-tolerance, and access control in the late 1960s (Bell & LaPadula, 1973). The emergence of networked computers and shared resources among computers has contributed to an active computer security field.

Simson Garfinkel (2008) directed attention to the complex relationship between computer security and the role of the REB: "As more security researchers turn their attention to usability and other human factors issues, many are surprised to discover that they must comply with regulations governing the use of human beings as experimental subjects" (p. 1); the "Common Rule, as written, clearly applies to much work in the field of usability, psychology and security" (p. 5). While no seminal definition of computer security research has yet been agreed upon, the realm of security research has been identified, and includes research that evaluates, detects, and prevents malicious software, and studies denial of service attacks, phishing, and botnet attacks[3] (Dittrich, Bailey, & Dietrich, 2009, 2011; Kenneally, Bailey, & Maughan, 2010).

Although ethical issues have long lingered in the background of CS in general, and computer security in particular, bringing them to the forefront is crucial as empirical research is on the rise, and as human subjects become more clearly identifiable in these forms of research. In response to Garfinkel's 2008 assertion, there has been active response from the security field itself. Recent workshops (e.g., The Workshop on Ethics in Computer Security Research [WECSR], 2010, 2011) have demonstrated that human subjects ethical standards are not universally accepted within the security community at the present time.

The remainder of this paper has two goals: (1) to draw attention to the potential human subjects research ethics principles that might be underapplied or misapplied in computer security research, and (2) to explore how rapidly changing technologies might necessitate reconceptualizing human subjects research ethics review. We question the appropriateness of extant REB models to emerging forms of computer security research. There have been few empirical studies of REB review practices with CS research that could illuminate these issues. Thus, this paper is offered as a preliminary theoretical analysis, with suggestions and recommendations for best practices based on anecdotal and professional evidence collected and experienced by the authors, all of whom have expertise in the CS and REB environments. We briefly explore relevant literature before presenting three examples of computer security research that include human subjects ethics issues, and we seek to respond to the following research questions:

1. Do current guidelines and regulations adequately address the unique issues in these computer security examples?
2. What best practices can be adopted by REBs in order to respond to these novel cases?

Research Framework: CS, Ethics, and REBs

Codes of professional ethics and practice have long guided the CS discipline, including those of the Association of Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). Discussion and analysis of these codes is well documented in the literature and is not our focus (see Tavani, 2011; Gotterbarn, Miller, & Rogerson, 1999; Johnson, 2009). Those codes are appropriate and adequate in their treatment of largely nonhuman subjects research ethics issues, such as professional duties, copyright, plagiarism, falsification/fabrication of data, peer review, publishing practices, and conflict of interest, among other core issues of research integrity. However,

as more CS in general and security research in particular *explicitly* involves human subjects, it is important to acknowledge the larger framework of research ethics grounded in human subjects models. Regulations specific to human subject protections were not written with an eye to technology-specific research, nor should they be. They are meant to apply across disciplines, grounded in the basic tenets of justice, beneficence, and respect for persons. But as REBs begin to apply these regulations to unique forms of computer security research, challenges arise quickly. There are disciplinary, jurisdictional, and temporal constraints that impede an easy alignment between CS and computer security research, broadly conceived, and human subjects ethics models.

Hall and Flynn (2001) conducted a survey of CS departments in the United Kingdom regarding human subjects research ethics in software engineering (SE) research with a response rate of 47% (44 department heads). A low number (36%) of respondents indicated that they found the monitoring of ethics in empirical research important, and 59% responded that their university does not require any software engineering research to gain ethical approval. Even with ethical approval processes in place, very few indicated that they were confident that all projects that needed approval were being submitted. Some responded that it is up to the individual to monitor his or her own research for ethics. With few formal approval processes in place and a low expectation that researchers monitor their own projects, it is questionable if and how this research is being monitored at all. Wright (2006) most aptly divides this monitoring into three possibilities: (1) strict guidelines, (2) self-regulation, and (3) informed self-regulation.

In contrast, many Canadian university CS researchers are funded by the Natural Sciences and Engineering Research Council of Canada (NSERC), a national funding body, and NSERC, along with related funding organizations, makes ethical research guidelines very clear (CIHR, 1998, 2010). Even then, however, some security research falls through ethical cracks.

Problems with obtaining REB approval for phishing research in particular have been discussed by Finn and Jakobsson (2007) and Jakobsson, Finn, and Johnson (2008). Phishing is the theft of sensitive information, such as account names, passwords, and banking information, often collected using deceptive e-mail messages (APWG, 2010). Finn and Jakobsson sought to research how individuals respond to phishing attempts, which is an urgently important question as more individuals are exposed to phishing attempts and as more identifiable information is stolen in online venues. The researchers asked: "Does a phishing experiment that deceives a subject and exposes the subject to a fake phishing attack adversely affect the subject's rights or welfare?" (2007, p. 7). Their experiments and subsequent dialogue with their REB focused on the major issues of risk, harm, waiver of consent, and debriefing procedures. The practice of phishing often crosses jurisdictional boundaries, and correspondingly, research on it may too. This brings into play international research ethics, and REBs must be prepared to look at these jurisdictional issues as they do in other forms of research in international settings.

Given the urgency surrounding such security risks and attacks that impact society, much security research may align more readily with emergency or disaster research protocol review. While Finn and Jakobsson did not make this analogy explicit, they note that "A very important issue in this research is the timeliness of the study in regard to the current types of actual phishing attacks, in terms of the REB review process, and in terms of arriving at an approach that adequately addresses the legal issues" (p. 19). Hall and Flynn (2001) also found that the time to approval was problematic and provides a significant dis-incentive for researchers not only to carry out empirical research but also to submit it for approval (p. 313), a sentiment echoed by Singer and Vinson (2001). While approval might not be necessary, or the researcher may not want to go through the approval process, it might also be a case of the researcher not recognizing that the project is human subjects research; while some may argue that their studies are in fact only carried out for development and not for "research" purposes, the line between the two is not always clear (Lethbridge, 2001).

In addition to these temporal considerations, Lung et al. (2008) indicate that replication studies prove problematic if the original study did not obtain or need REB approval; if approval is needed from the university in which the replication study is being performed, some aspects of the original study might not make it past the REB and it would no longer be a true replication. For example, if an original study paid participants, but a research board does not permit this for a replication study, it may become too difficult to recruit subjects.

A final point to keep in mind when judging the relevance of an REB to CS research is that modern computer technology is very egalitarian. Unlike other disciplines such as medicine, a great deal of CS research is conducted by people outside a university or research laboratory environment; for example, there are numerous self-styled researchers in the field of computer security, some unaffiliated completely, others working for industry. While we do not mean to imply that these nontraditional researchers are not concerned with ethical behavior, or that they are not acting ethically, it is fair to

say that they are not required to submit to an REB. They may, however, be subject to other laws and regulations related to data privacy and/or data security laws; their contractual constraints may be more binding than the regulatory stamp of an REB. The relevance of emergent frameworks such as those presented by Ross et al. (2009) on community-based participatory research hold promise for alternative models for researchers who are not institutionally based.

Three Case Examples

Each of the following examples of computer security research has potential human subjects issues embedded. These cases typify the disciplinary, temporal, and jurisdictional ethical challenges noted above. The authors recognize the complexity in these cases, and to some end, that is intentional. While every effort was made to present them in a straightforward way for non-computer security readers, the intricacies and difficulties in identifying the *subject* versus the *data*, and the *research* versus the *process* of security work, speak to the need to bridge the gap between security researchers and REBs. While a reader may not completely understand the intricacies of each case, the subsequent discussion will elucidate the human subjects ethics concerns.

CASE 1

Some researchers within computer security engage in proactive threat research, examining potential computer security threats along with their defenses *before* the threats are seen "in the wild" on people's computers. The ethics of conducting such research is a substantial topic in itself and has been preliminarily explored by Aycock and Maurushat (2007); Aycock and Sullins (2010); Kenneally, Bailey, and Maughan (2010); and Dittrich, Bailey, and Dietrich, 2009.

As part of her proactive security research, Alice, a North American researcher, has devised a new type of computer worm, which is a form of malicious software that propagates itself from one computer to another via the Internet. Her graduate student, Bob, has implemented this new worm so that he and Alice can study its properties in the controlled environment of their own lab; that is, the worm will not be intentionally released to the open Internet. Alice and Bob do not have to get REB approval for their research, because they are not experimenting with, nor gathering data from, humans. However, an accidental release of the worm would affect humans' computers, perhaps even making computer networks unusable. Furthermore, the worm release could trivially infect computers across cultural and legal boundaries. Dissemination of the work, even assuming no accidents occur, may benefit the "bad guys" as well as regular computer users.

CASE 2

Alice and Bob are hard at work on another research project.[4] Here, a malicious worm is spreading on the Internet. Every time the worm infects a new computer, it automatically contacts a website in Europe, requesting a file from its web server. This website, which does not appear to be affiliated with the worm's creator(s), keeps records of all such requests, logging the date and time of the request; the name of the requested file; and, most significantly, the Internet Protocol (IP) address of the requesting computer. This address identifies the computer (which may have only a single user who is therefore also identified); even a portion of the address might provide details about the location of a user (e.g., coming from a specific organization or particular location, such as a work computer).

The website, realizing it is involved with a worm infection, makes these logs public to help security researchers (including Alice and Bob) thwart the worm. This is a legitimate action. However, the data were generated by a worm infecting computers without the legal right to do so. The traceable IP addresses of computers may be considered personally identifiable information. Even if a specific person is not identifiable, the ability to identify an organization might be sensitive; an antivirus company or bank may suffer reputational damage from such a disclosure.

Alice and Bob most likely do not need REB approval to work with these data. The data are publicly available, and, assuming the worm propagated itself from computer to computer without human involvement, the data were arguably not collected from humans. However, as in Case 1, indirect effects of Alice and Bob's research may impact people and organizations.

CASE 3

Alice is also interested in the methods "bad guys" use to attack and take control of computers across a network. In one of her research projects, she has set up a computer on her university's network which is designed to be attractive to attackers. Studying the logs of this computer's network activity may shed light on attackers' methods.

The best results require the collection and analysis of full IP addresses, which raises the privacy concerns noted in Case 2. Furthermore, Alice anticipates intensive data processing that exceeds her lab's capacity, so she will be performing much of her analysis using a cloud computing cluster, which allows her to access powerful

computers through the Internet. But cloud computing resources are, by design, shared resources. As the National Institute of Standards and Technology (2010, np) defines it, cloud computing is a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released." Thus, performing analysis of potentially sensitive data in a cloud computing environment raises further concerns about privacy and confidentiality.

Alice is well aware of the issues with both IP addresses and cloud computing, but also wants the best research results. She submits an REB application that outlines the potential risks involved with privacy, anonymity, risk, and harm in her protocol. She is diligent and makes her best effort to conduct the research in an ethical fashion. She selects a domestic cloud-computing provider to avoid data crossing legal jurisdictions. The cloud computation is performed on a version of the data that are anonymized to avoid identifying individuals in the event the data are acquired by outside parties. The IP addresses she collects are reported only in aggregate form to avoid identifying individuals or organizations.

Discussion

An REB would first ask: *Is this research?* In each case, the researchers are producing generalizable knowledge for the benefit of society, and thus, the answer is yes. We would then ask: *Does this research involve human subjects?* Not surprisingly, each case raises the level to which an REB might be involved in a protocol review, as each blurs the line a bit more between human subjects and nonhuman subjects research. We are not asserting an overly conservative view of these forms of security research, nor are we contributing to what has been commonly called REB "mission creep." However, we do want to advocate for an ethical evaluation based on the potential for harm to humans from research actions, not whether humans are directly involved or not. Under the U.S. regulatory framework, we believe that most likely these cases would be categorized as minimal risk. Researchers and boards must balance presenting risks related to the specific research with risks related to the technologies in use.

We contend that Case 1 would clearly not be considered human subjects research, as no identifiable information is being collected, nor is there any intervention with a human subject; although there is potential for harm to society at large if the worm were to be released. But, we must ask:Who may be harmed by this research and how is that potential harm addressed? Does anyone need to consent or be informed if an experiment goes awry? Due diligence and professional and disciplinary ethics are key in this case, and those standards have been established in the realms of the ACM and the IEEE; while the security field, as noted, may be less solidified in its ethical frameworks, there are professional standards to uphold.

As we move into Cases 2 and 3, the distance between the researcher and human subjects decreases, and accordingly, a review board's involvement becomes more likely. Markham and Buchanan (forthcoming) have referred to this concept as the *distance principle*, which is relevant to addressing the question "Is this human subjects research?" in novel computer-mediated research. Markham and Buchanan assert that

> as the conceptual or experiential distance between the researcher and author/participant decreases, we are more likely to naturally define the research scenario as one that involves humans. For example, an email or virtual worlds interview produces data that are experientially near the participant. As the conceptual or experiential distance between the object of research and the person who produced it increases, there may be a tendency to define the research scenario as one that does not involve "human." For example, an aggregation of surfing behaviors collected from a bot or a data set containing thousands of tweets is conceptually distant from the participant.

In Case 2, the researchers' distance from the human subject is considerable. As in Case 1, we can ask, "Who are the subjects?" Is the availability of the personally identifiable information recorded by the worm's activities available for use by the researchers? Of import, the researchers are not themselves collecting data; this example aligns more closely with publicly available data sets. However, Case 2 does raise the hot-button issue of IP addresses. The Office for Human Research Protections has not issued a formal statement on whether IP addresses are considered to be personally identifiable information for purposes of the HHS protection of human subjects regulations at 45 CFR Part 46. However, for purposes of the HIPAA Privacy Rule, the HHS Office for Civil Rights has opined that an IP address is considered to be a direct identifier of an individual. Other European data regulations consider IPs as identifiers, and as such fall under the realm of the EU Data Directives (1995, 2006). This presents a challenge for international research and should be considered carefully by researchers and boards[5] (Buchanan, Gallant, Odwazny, & Miller, 2011; Buchanan, 2012).

As we move into Case 3, the researcher is collecting IP data; the issue of consent arises. Who would be consenting? Similar to phishing research, the subject population may be dispersed and obtaining consent impracticable. This would qualify as a minimal risk with waiver of consent. However, if the researcher were to obtain consent from subjects, the language of traditional consent documents and protocols would not fit. Risks and harms should be presented in appropriate language, such as "There are potential risks of data loss, data manipulation, or unauthorized access by outside parties in this form of research. All appropriate precautions will be taken to ensure the security and integrity of the data." Statements informing subjects where data will be housed, for how long, and accessible by whom is significantly different in computer security research—though any disciplinary research using computer-enabled and especially networked forms of collection, analysis, or dissemination technologies will continue to share in these concerns. For this reason, while this paper focuses on the specific area of computer security, many of its concerns are generalizable in this age of networked and dispersed research activity.

As depicted in Case 3, the use of cloud services poses confidentiality concerns for REBs, and of course not only in the area of computer security research but across disciplines. As Pearson (2009) has pointed out, "[C]loud services … typically result in data being present in unencrypted form on a machine owned and operated by a different organization from the data owner"; consequently, researchers will need to take significant precautions with anonymization techniques and data security strategies. Because most researchers, and indeed, many REB members are not computer security experts, universities will need to prepare themselves in a shared responsibility model. We recommend the data security model developed by Harvard (2010).

Case 3 shows the potential where a security breach plus lack of encryption can put the privacy of potentially sensitive material at high risk. While it is up to the researcher to control data privacy, this might not always be possible when data are stored offsite or in the hands of another. The researcher in our case took appropriate precautions, but third-party sites do change their policies and terms of use regularly, and as such, a diligent researcher must actively anonymize data, aggregate data, and remain aware of the cloud service's policies. Furthermore, access to data changes in the cloud environment, as Jaeger, Lin, and Grimes (2008) state: "Cloud providers have legitimate reasons for monitoring use of the resource, which is necessary to perform routine maintenance" (p. 276). Further, if the research is overseen by an institution/REB, in the U.S. context, the federal government has the right to see the data. A related issue is ownership of the data, and a researcher may not have the certainty to claim ownership and to assure his or her subjects that the data belong to the researcher. Chow et al. (2009) further bring into question the level of access or control a researcher might have over his or her data when they are stored in a cloud. While the researcher might hold his or her data privacy to certain standards, the same might not be said for the companies: "The commercial providers of various cloud computing innovations say little about the confidentiality or privacy of the information placed under their control, and the legal rights and regulatory authority for the protection of the privacy of cloud computing users are not well defined" (Aldrige, Medina, & Ralphs, 2009, p. 8). For these reasons, Case 3 presents the most challenge for REB review; issues of privacy, ownership, access, control, retention and destruction of data become mediated issues, not solely under the auspices of the researcher—or even the REB.

Best Practices

The most basic question we must ask is one that challenges an implicit assumption we have made throughout: Is an REB (still) relevant to CS research?

We assert that ethics oversight is highly significant and meaningful for CS research, to maintain the public trust and safeguard the public interest. Reviewing research for potential harm is a good thing, regardless of discipline. We therefore reject the extreme notion that no ethics oversight is needed in CS research, such as raised in our cases. What we have not addressed, however, is whether such oversight should come from an REB, or, what form that REB may take. As noted, Ross et al. (2010) have provided an alternative to the traditional REB in the framework of community-based participatory research in translational medicine. Their model readjusts the notions of risk and benefit, and accordingly, changes the ways in which the REB operates.

For an REB to provide meaningful, relevant oversight, it must be in a position to understand technological issues and provide appropriate guidance. As suggested by Buchanan and Hvizdak (2009) and by Aycock et al. (2011), one way to achieve that goal is to involve computer scientists in the REB, either on the committee directly or in an expert advisory capacity when needed. We suggest that the former is preferable to the latter, as most research does involve computers at some point. At the U.S. regulatory level, supplementing the board with outside expert consultancy is advised and certainly

within the rights and responsibilities of the REB (see 45 CFR 46.107[a]).

Another approach to ethics oversight is to transform the REB in a more fundamental way to make it relevant to CS research. U.S. Federal Regulation 45 CFR 46(f) suggests that a technical expert can advise on a board but in a non-voting capacity. Alternatively, we may focus on 45 CFR 46.107(a) and constitute a board that includes computer scientists, not only biomedical and social scientists. Instead of adding CS expertise to the board in an advisory capacity, we suggest a shift towards a CS-focused review board. This model would work best at larger institutions, and would follow the model used by various types of review boards existing across an institution (for example, a board for clinical research, a social science board, a board which deals only with exempt research, a Conflict of Interest Committee, and so on). None but the largest universities could staff such a board, hence we propose an *extra*-review board, or E-RB, an ethics review board unaffiliated with any one university that would be comprised of computer scientists and security specialists from many different institutions. We could conceive of the E-RB in both the traditional sense, that is, it could exist with institutional powers of authority, or it could be developed to exist as an advisory board.

While the advisory model challenges extant notions of regulation, it holds potential for novel ways of assisting or enhancing existing review boards. If a university's review board receives a protocol based on Case 3, and is unsure of the implications for subjects, the board could consult with the E-RB; they could provide expert guidance and call attention to the unique ethical issues within a specific research realm. An added benefit to extricating ethics review from individual institutions is that nontraditional researchers outside academia could conceivably have their research reviewed, as could researchers from smaller institutions or from developing countries where the resources for a full REB may be lacking. Establishing and operating E-RBs would seem to fall within the mandate of professional computing organizations like the ACM, in conjunction with national research bureaus. This model requires that the CS experts within these E-RBs have human subjects regulatory expertise. It assumes that ethics will be considered relevant and that human subjects ethics is understood and applied where appropriate within a discipline, CS, and a subdiscipline, computer security, that does not have a long-standing relationship with REBs and extant research ethics frameworks. Another conceptualization may be a board that evaluates "human non-subjects research" (Brothers & Clayton, 2010) such as data, or even biological specimens. This model, of course, has implications for other disciplines, as well. What would prevent another discipline from arguing its specificity such that it needs its own unique review board?

We hope that the issues presented herein have shown that computer security indeed presents significant challenges, and that currently, REBs are often unprepared to review such protocols. At this time, this model of an E-RB could be beneficial to both researchers and review boards. As REBs evolve, and as more research becomes fundamentally mediated by computers, which is occurring, this model may be unnecessary.

CS-related organizations (e.g., ACM, IEEE, USENIX) can assume a leading role in cultural change by requiring conference and journal papers to be submitted along with a certificate of E-RB/REB approval or a statement explaining why one was not required. This is similar in spirit to requirements for medical journal submissions, for example, the *Journal of the American Medical Association* (*JAMA*), and many other journals. Aycock et al. (2011) have advocated for this model in computer security research, and such "certification" was endorsed at the recent Workshop on Ethics in Computer Security Research (2011).

No amount of REB restructuring or cultural change makes any difference if CS research is not vetted through ethical review processes, as in Cases 1 and 2. We see many implications to this.

First, explicit ethics policies can be developed to cover specific situations. For example, École Polytechnique in Montréal, Canada (EPM), has ethics guidelines enacted to cover research involving computer security risks; this is the only such policy that we are aware of. The major drawback to this method, of course, is that it is piecemeal and invariably will miss some research that should receive ethics approval. In fact, the underlying problem is deeper and derives from the nature of computers themselves. Simply stated, computers (particularly networked ones) allow indirect, second-order effects to occur with a speed and reach rarely matched in the physical world. In Case 1, a worm program thought to be safely contained could quickly spread around the world and indirectly affect people worldwide. In Case 2, a worm running autonomously on computers worldwide generates data that can identify people indirectly. Even something pedestrian by CS standards, such as releasing research software publicly, can have indirect consequences if that software is then used by programmers to develop an application for end users.

Second, computer security research review can follow more closely the protocol review standards of other "nontraditional" forms of research review, e.g., disaster or emergency research (noting the recent release of the

March 2011 FDA: Guidance—"Exception from Informed Consent Requirements for Emergency Research"). We must consider the full physical and virtual environmental impact of CS research as part of ethics review. Given the recently recognized demands of community-engaged research and translational medicine, the task of assessing the environmental impact of research on the larger society is not a new role for REBs. Awareness of these potential adverse effects is of course ultimately tied with consent. Standard practices of waiving elements of informed consent in minimal risk research will and should apply to CS research. In our cases, and in many examples of CS research, obtaining consent is impracticable. Regarding informed consent processes, we recommend that researchers work with their REBs to best establish practices for "knowledge checks" throughout the research process to ensure understanding of risks and benefits, especially in complex CS research settings.

If obtaining consent is impracticable, as with any research, if the scientific value overrides the need for consent, the researcher should clearly justify these conditions (see FDA, 2011). Relatedly, when an adverse event occurs in CS research, the researcher must be very clear about reporting such events. However, in a large-scale computing environment, this may be impracticable as well.

Ultimately, for ethics guidelines to fully apply to CS research, a fundamental change in the concept of a "human subject" may be in order. At the current time, federal regulations covering federally funded research in the U.S. define a human subjects specifically as a "living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable personal information" (45 CFR 46.102[f]). Much CS research will fall under an exemption. We hold that while research may not conform exactly to the extant regulatory definitions, there is still a need for ethical review. At the most fundamental level, if a researcher is collecting data about or from a bot that is person-based, i.e., representative of a living person, it will be considered human subjects research. As online environments become more sophisticated, and as researchers engage in more bot-enabled research, the threshold of *human subjects* will change. But, in order to make sound decisions around bot or avatar subjects research, the level of interaction or intervention is significant to consider. We advocate using the *distance principle* as a supplementary starting point, in addition to the regulatory flowchart's questions. A researcher may be engaging only in observation of behavior and not direct intervention. If observation is occurring, we would then ask if the bot or avatar is in a public space, with any expectation of privacy. These lines are indeed very fuzzy in online environments. A baseline consideration for review boards should be the "entry requirements" for the researcher into a specific site or environment where such bots or avatars exist. If there are strong entry requirements in the forms of cost or restrictive policies, such venues should be considered private and thus the observation exemption will not apply. But, computer security research brings the added complexity of criminal behavior, so REBs may need to elevate a seemingly minimal risk protocol to risk, if criminal behavior in the forms of phishing or direct denial of service attacks are the issue under observation. Then, of course, an exemption would not apply.

Educational Implications

The implications of this discussion for education are twofold, as they apply to two distinct groups: already-active researchers and up-and-coming students. CS researchers who are already active could, quite rationally, see changes to ethics requirements as imposing an obstacle to their research progress. While educational outreach to established CS researchers would be helpful, we suggest that any changes here must be enforced by pressure from publishing venues for demonstrably clean ethical "bills of health" as mentioned earlier, as well as imperatives from national granting agencies. The other group, students, are in the best position to learn about new perspectives on ethics in CS research because they are still in training. Furthermore, students are ultimately where long-term educational initiatives will pay off, as already-active researchers leave the system.

Acculturating students in a framework of research ethics that is at once disciplinarily appropriate, robust in its ethical grounding, and responsive to the changing and malleable world of computer security research must begin early and be persistent. The REB cannot be an afterthought, and correspondingly, REBs should not consider CSs or security research as an afterthought, but should seek out opportunities to work collaboratively. Finn and Jakobsson showed the benefits of collaboration between a computer scientist and an REB chair in their research, described earlier.

At a recent Columbia University Institutional Review Board Conference, both CS and Internet research were discussed; the importance of ongoing educational efforts, bringing together researchers from nontraditional human subjects fields, was highlighted. Other REB forums have done the same, as have the OHRP Community Research Forums. PRIM&R (Public Responsibility in Medicine and

Research) has been responsive and has been including these emergent forms of research in their conferences and research agendas. These are all encouraging signs of a healthy future for REBs and researchers as they engage in and review nontraditional forms of research. Computer security research is not the first, nor will it be the last, to confound REBs; we suggest that REBs consider novel, yet analogous models, as suggested herein; those include emergency and disaster research; international research; translational medicine; and community-based participatory research. Similar to Shore et al. (2011), we encourage curricular revisions in standard research ethics trainings, such as CITIs.

Research Agenda

As more REBs encounter emergent forms of computer security research, and as computer systems and the ethical complexities inherent to the networked world of research are embodied across disciplines, strong ethical guidance is needed. We support a shared responsibility model, where researchers, REBs, and information technology experts work together to disclose, understand, and accommodate the unique ethical issues within CS research. We realize this is a paradigm shift and applaud the Harvard University Data Security Team for providing a robust example of shared responsibility and ethics. We also support Dittrich, Bailey, and Dietrich's (2011) call for a community of ethics within computer security research. In order to infuse more human subjects research ethics awareness into computer disciplines, we need to evaluate anew what ethical issues are being covered in curricula, and work with professional societies such as ACM and IEEE, along with those associations relevant to the REB community at large, such as PRIM&R (again, see Shore et al., this issue) to ensure that coverage squarely includes human subjects, and human nonsubjects ethical issues. This latter form of research will only continue to grow, and the ethics review community can both shape its future and assure a strong model of research ethics and integrity.

Acknowledgments

The authors wish to thank both anonymous and nonanonymous reviewers, including Ann Meeker O'Connell and Joan Sieber, for their insightful and helpful comments and suggestions on an earlier draft of this paper. John Aycock's work is supported in part by the Natural Sciences and Engineering Research Council of Canada. Elizabeth Buchanan's work is supported in part by the National Science Foundation, grant numbers SES-0646591 and SES-0924604. The results presented here do not represent the views of the National Science Foundation. Buchanan and Ess's work was approved under the University of Wisconsin–Milwaukee Institutional Review Board.

Author Note

Address correspondence to: Elizabeth A. Buchanan, Center for Applied Ethics, University of Wisconsin–Stout, PO Box 790, Menomonie, WI 54751. Phone: 715-232-5184; E-MAIL: buchanane@uwstout.edu.

Authors' Biographical Sketches

Elizabeth A. Buchanan is Endowed Chair and Director for the Center for Applied Ethics at the University of Wisconsin–Stout. She has served on both social-behavioral and medical review boards. She is the editor of *Readings in Virtual Research Ethics: Issues and Controversies*, one of the first anthologies on Internet research ethics and the principal investigator of two federally-funded grants related to IRE.

John Aycock is Associate Professor in the Department of Computer Science at the University of Calgary, Canada. John's research focuses on computer security, including such issues as viruses, phishing, zombies, botnets, and worms. He is the author of numerous papers and several books, the most recent of which is *Spyware and Adware* (Advances in Information Security, vol. 50, Springer-Verlag, 2010).

Scott Dexter is Professor of Computer and Information Science, Brooklyn College of the City University of New York. Scott has done extensive research into the free software movement, and is the co-author of *Decoding Liberation: The Promise of Free and Open Source Software* (Routledge, 2007). He is on the Executive Board of the International Society of Ethics and Information Technology, and is Director of the Core Curriculum at Brooklyn College.

David Dittrich is a Senior Security Engineer and researcher at the University of Washington, working in the Center for Environmental and Information Systems at the UW Applied Physics Laboratory. He is also a member of the Honeynet Project and Seattle's "Agora" computer security group. He currently serves on one of the UW's Institutional Review Boards. Dave is most widely known for his research into Distributed Denial of Service (DDoS) attack tools and host/network forensics. He co-authored the first complete book on DDoS, titled *Internet Denial of Service: Attack and Defense Mechanisms* (Prentice Hall, 2005).

Erin Hvizdak is pursuing her Master of Arts degree in Women's Studies and Gender Studies at Loyola University Chicago. Prior to this, she completed her Master of Library and Information Science degree at the University of Wisconsin–Milwaukee. She was research assistant at the Center for Information Policy Research, and project assistant to the Internet Research Ethics Commons project.

Author Contributions: Buchanan and Aycock contributed equally as lead authors (75%) and provided the overall theoretical, philosophical, and practical framework for the paper; Dexter and Dittrich provided technical expertise and guidance (20%); Hvizdak provided research assistance and editorial support (5%).

Notes

1. An *avatar* is defined as a character, graphic, or other representative persona used by an individual online; *bot*, short for "robot," often refers to a piece of code or program meant to automate work that would otherwise be done by an individual (see internetresearchethics.org for further examples); Maes (1995, p. 108) defines an *artificial autonomous agent* as "computational systems that inhabit some complex dynamic environment, sense and act autonomously in this environment, and by doing so realize a set of goals or tasks for which they are designed."
2. We refer readers to the Internet Research Ethics Commons Working Glossary at internetresearchethics.org for guidance on these and emerging terms in e-research.
3. Dittrich, Bailey, and Dietrich (2009) define botnet research as that which "centers around the detection and mitigation of large numbers of infected hosts, or bots, networked into a single distributed system, or botnet."
4. This was initially inspired by a posting regarding the Gibe.F worm (Smith, 2003).
5. The authors express their gratitude to Ms. Laura Odwazny, Senior Attorney, Office for Human Research Protections, Office of the General Counsel, Public Health Division, U.S. Department of Health and Human Services, for her unofficial guidance on this issue.

References

Albrecht, V. (2009). *Avatars and other cyber-folk: Are they human subjects?* CUNY Institutional Research Board Annual Conference, New York.

Aldrige, J., Medina, J., & Ralphs, R. (2009). The problem of proliferation: Guidelines for improving the security of qualitative data in a digital age. *Research Ethics Review*, *6*(1), 3–9.

Anti-Phishing Working Group. (2010). *Phishing activity trends report*. Retrieved from http://www.antiphishing.org/reports/apwg_report_q2_2010.pdf.

Association for Computing Machinery. (1998). *The 1998 ACM Computing Classification System.* Retrieved from http://www.acm.org/about/class/1998.

Aycock, J., Buchanan, E., Dexter, S., & Dittrich, D. (2011). Human subjects, agents, or bots: Current issues in ethics and computer security research. In *Proceedings from 2nd workshop on ethics in computer security research*, St. Lucia, February 28–March 4, 2011. Lecture Notes in Computer Science. New York: Springer.

Aycock, J. & Maurushat, A. (2007). Future threats. In *Proceedings from 17th Virus Bulletin International Conference* (pp. 275–281). Retrieved from http://pages.cpsc.ucalgary.ca/~aycock/papers/vb2007future.pdf.

Aycock, J. & Sullins, J. (2010). Ethical proactive threat research. In *Proceedings from Workshop on Ethics in Computer Security Research (LNCS 6054)* (pp. 231–239). New York: Springer.

Bell, D., & LaPadula, L. (1973). *Secure computer systems: Mathematical foundations* (MITRE Technical Report 2547). Retrieved from http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf.

Arrow Brothers, K. & Clayton, E. W. (2010). "Human non-subjects research": Privacy and compliance. *The American Journal of Bioethics*, *10*(9), 15–17.

Buchanan, E. (2010). Internet research ethics: Past, present, future. In C. Ess and M. Consalvo (Eds.), *The Handbook of Internet Studies* (pp. 82–108). Oxford: Blackwell.

Buchanan, E. (forthcoming). E-research and e-planning: Emerging considerations for transformative research. *International Journal of E-Planning Research 1*(1).

Arrow Buchanan, E. & Ess, C. (2009). Internet research ethics and the institutional review board: Current practices and issues. *ACM SIGCAS Computers and Society*, *39*(3), 43–49.

Buchanan, E., Gallant, D., Odwazny, L. & Miller, M. (2011). *Internet research ethics.* PRIM&R Annual Conference Presentation. San Diego, CA.

Arrow Buchanan, E. & Hvizdak, E. (2009). Online survey tools: Ethical and methodological concerns of human research ethics committees. *Journal of Empirical Research on Human Research Ethics*, *4*(2), 37–48.

Canadian Institutes of Health Research (CIHR), Natural Sciences and Engineering Research Council of Canada, Social Sciences and Humanities Research Council of Canada. (1998). *Tri-Council policy statement: Ethical conduct for research involving humans.* Retrieved from http://pre.ethics.gc.ca/eng/archives/tcps-eptc/Default.

Canadian Institutes of Health Research (CIHR), Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada. (2010). *Tri-Council policy statement: Ethical conduct for research involving humans.* Retrieved from http://pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/Default/.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling data in the cloud: Outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security* (pp. 85–90). New York: Association for Computing Machinery.

Denning, P., Corner, D., Gries, D., Mulder, M., Tucker, A., Turner, A., & Young, P. (1989). Computing as a discipline. *Communications of the Association for Computing Machinery*, *32*(1), 9–23.

Dias, K. (2003). The ana sanctuary: Women's pro-anorexia narratives in cyberspace. *Journal of International Women's Studies*, *4*(2), 31–45.

Dittrich, D., Bailey, M., & Dietrich, S. (2009). *Have we crossed the line? The growing ethical debate in modern computer security research* (Stevens CS Technical Report 2009-1). Hoboken, NJ: Stevens Institute of Technology. Retrieved from http://staff.washington.edu/dittrich/papers/dbd2009tr1/.

Arrow Dittrich, D., Bailey, M., & Dietrich, S. (2011). Building an active computer security ethics community. *IEEE Security and Privacy*, *9*(3), 1–9.

École Polytechnique Montréal. (2009). *Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques.* Retrieved from http://www.polymtl.ca/recherche/doc/Procedure-RisquesInformatiques.pdf.

European Commission, Directorate of General Justice. (2010). European Union Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

European Commission, Directorate of General Justice. (2010). European Union Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Retrieved from http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

Arrow Finn, P. & Jakobsson, M. (2007). Designing ethical phishing experiments. *IEEE Technology and Society Magazine*, *26*(1), 46–58.

Arrow Floridi, L. (2004). On the morality of artificial agents. *Minds and Machines*, *14*(3), 349–379.

Floridi, L. (2010). *Information: A very short introduction*. New York: Oxford University Press.

Food and Drug Administration. (2011). *Exception from informed consent requirements for emergency research.* Retrieved from www.fda.gov/downloads/RegulatoryInformation/.../UCM249673.pdf.

Garfinkel, S. (2008). IRBs and security research: Myths, facts and mission creep. In *UPSEC'08 Proceedings of the 1st Conference on Usability, Psychology, and Security*. Berkeley, CA: USENIX Association.

Gotterbarn, D., Miller, K., & Rogerson, S. (1999). Software engineering code of ethics is approved. *Communications of the Association for Computing Machinery*, *42*(10), 102–107.

Arrow Hall, T. & Flynn, V. (2001). Ethical issues in software engineering research: A survey of current practice. *Empirical Software Engineering: An International Journal*, *6*(4), 305–317.

Harvard University. (2010). *Harvard research data security policy*. Retrieved from http://security.harvard.edu/research-data-security-policy.

Arrow Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics*, *5*(3), 269–283.

Arrow Jakobsson, M., Finn, P., & Johnson, N. (2008). Why and how to perform fraud experiments. *IEEE Security & Privacy*, *6*(2), 66–68.

Johnson, D. (2009). *Computer ethics.* Englewood Cliffs, NJ: Prentice Hall.

Kenneally, E., Bailey, M., & Maughan, D. (2010). A framework for understanding and applying ethical principles in network and security research. In R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, & F. Sebé (Eds.), *Financial Cryptography and Data Security* (pp. 240–246). New York: Springer.

Arrow Krieger, N., Chen, J., Waterman, P., Rehkopf, D., & Subramanian, S. V. (2005). Painting a truer picture of U.S. socioeconomic and racial/ethnic health inequalities: The Public Health Disparities Geocoding Project. *American Journal of Public Health*, *95*(2), 312–323.

Arrow Lethbridge, T. C. (2001). Mixing software engineering research and development: What needs ethical review and does not? *Empirical Software Engineering: An International Journal*, *6*(4), 319–321.

Lung, J., Aranda, J., Easterbrook, S., & Wilson, G. (2008). On the difficulty of replicating human subjects studies in software engineering. In *Proceedings of the 30th International Conference on Software Engineering (ICSE'08)*, Leipzig, Germany, May 10–18, 2008. New York: Association for Computing Machinery. Retrieved from http://www.cs.toronto.edu/~sme/papers/2008/Lung-ICSE2008.pdf.

Maes, P. (1995). Artificial life meets entertainment: Life like autonomous agents. *Communications of the Association for Computing Machinery*, *38*(11), 108–114.

Markham, A. & Buchanan, E. (forthcoming). The distance principle and Internet research ethics "subjects." *International Journal of Internet Research Ethics*.

Moløkken-Østvold, K. (2005). Ethical concerns when increasing realism in controlled experiments with industrial participants. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005* (pp. 1–10). New Brunswick, NJ: IEEE Publications.

Myers, A. (2010). Fieldwork in the age of digital reproduction: A review of the potentials and limitations of Google Earth for archaeologists. *SAA Archaeological Record*, *10*(4), 7–11.

National Institute of Standards and Technology. (2010). *NIST cloud computing program*. Retrieved from http://www.nist.gov/itl/cloud/.

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. *Cloud '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing* (pp. 44–52). New Brunswick, NJ: IEEE Publications.

Arrow Ross, L, Loup, A., Nelson, R., Botkin, J., Kost, R., Smith, G., & Gehlert, S . (2010). Human subjects protections in community-engaged research: A research ethics framework. *Journal of Empirical Research on Human Research Ethics*, *5*(1), 5–17.

Arrow Shore, N., Drew, E., Brazauskas, R., & Seifer, S. D. (2011). Relationships between community-based processes for research ethics review and institution-based IRBs: A national study. *Journal of Empirical Research on Human Research Ethics*, *6*(2), 13–21.

Singer, J. & Vinson, N. (2001). Why and how research ethics matters to you. Yes, you! *Empirical Software Engineering: An International Journal*, *6*(4), 287–290.

Smith, R. M. (2003). Web counter in the new Swen/Gibe.F worm. Message posted to *BugTraq* mailing list, September 18.

Sweeney, L. (2003). *Navigating computer science research through waves of privacy concerns: Discussions among computer scientists at Carnegie Mellon University*. In Tech Report, CMU CS 03-165, CMU-ISRI-03-102. Pittsburgh: Carnegie Mellon University.

Tavani, H. (2011). *Ethics and technology: Controversies, questions, and strategies in ethical computing.* Boston: John Wiley.

Wright, D. R. (2006). Research ethics and computer science: An unconsummated marriage. *SIGDOC '06: Proceedings of the 24th Annual ACM International Conference on Design of Communication*. New York: Association for Computing Machinery. Retrieved from www4.ncsu.edu/~drwrigh3/docs/pubs/sigdoc06a.pdf.