Editor: Tara Whalen, twhalen@pobox.com

The Menlo Report

Michael Bailey | University of Michigan
David Dittrich | University of Washington
Erin Kenneally | University of California, San Diego
Doug Maughan | Department of Homeland Security

Research on rapidly advancing information and communication technology (ICT) has exposed gaps between what researchers *could* do and what they *should* do, thereby creating ethical challenges. Even seemingly benign research involving botnet infiltration for observation purposes, empirical analysis of fraud, or behavioral research on anonymity network users puts researchers at an ethical crossroads.

To understand significant Internet threats, researchers might actively participate in a botnet by relaying or responding to commands instructing compromised bot machines to send malicious email, initiate a distributed denial-of-service attack, or propagate malicious software to other hosts. Such active engagement lets researchers discover the botnet code's vulnerabilities, which enables the development of remote cleanup programs that execute unauthorized commands on end users' computers. Or, it might stimulate publication of the botnet code—instructions that permit the manipulation of hosts ranging from personal computers to proprietary process control devices, electronic voting machines, or medical devices. Although researchers' intent might be to empirically prove that harm in the virtual environment can manifest as harm in the physical environment, the potential harm from improper disclosure could be immediate and life threatening if malicious attackers exploit such knowledge before the vulnerabilities are remediated. Furthermore, researchers often gain access to drop zones—servers containing sensitive stolen data, such as trade secrets, bank account credentials, personal communications, and login credentials.

Experiments aimed at understanding Internet fraud dynamics, or *phishing*, might require that users be unaware they're being studied to observe their typical behavior. Obtaining informed consent prior to a study can defeat this purpose, so deception might be necessary to accurately simulate real fraudulent behavior. Researchers might redirect users from an unsuspecting malicious website to a benign site that they control and monitor. When informed consent is waived and deception is involved, debriefing after the study's completion is typically required; however, this might increase rather than decrease harm to subjects because their knowledge of being tricked can cause shame or decrease their trust in researchers' actions.

Experiments intended to understand Internet use or measure certain networks' traffic characteristics require access to network traffic. If researchers find it difficult to access the target network, they might choose to leverage user-supported networks such as Tor (the onion router), setting up entry or exit nodes from which they can collect data locally (including sensitive payload data). Such monitoring might violate the network's terms of use, contravene network users' expectations, and raise legal risks about communication privacy. Exploiting weaknesses in such networks to gain access to data or selecting subjects to avoid restrictions raises further questions.

In addition, it's sometimes unclear whether researchers consider the *could* or *should* courses of action, and if so, whether their actions are affected by opinions about the gray applications of laws or the relevance of institutional review boards to research beyond the traditional behavioral and biomedical realm. A variety of reasons attempt to explain why Internet research considers ethics less than other fields do, including a deficiency of shared values among this research community, a shortage of individual expertise in formal ethical decision-making, the inconsistent

1540-7993/12/$31.00 © 2012 IEEE Copublished by the IEEE Computer and Reliability Societies March/April 2012

application of principles, and a lack of agreement on enforcement.[1]

How should we address these shortcomings? The logical approach in the face of this dilemma is to revisit first-order ethical principles and applications. Thus, the US Department of Homeland Security (DHS) Science and Technology Directorate launched an effort that resulted in the Menlo Report, a document containing ethical principles guiding ICT research.[2]

Origins of the Menlo Report

The Menlo Report builds on the Belmont Report and shares some procedural heritage, such as publication in the *Federal Register*. However, the two processes aren't equivalent.

The Belmont Report was the culmination of years of working meetings by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, which began as part of the National Research Act defined by Congress and signed into law by President Richard Nixon in 1974. Although the Belmont Report stands alone in many researchers' and ethics reviewers' minds, it's part of a larger body of supporting documents. During its multiyear deliberation process, 26 papers were written that provide background, scientific observations, and recommendations on topics including basic ethical principles relating to research involving human subjects, boundaries between research and practice, risk/benefit criteria, and informed consent. At the same time that the Department of Health, Education, and Welfare first published this concise statement of ethical principles in 1978, it also published the hundreds of pages of papers created by and for National Commission members in two volumes of appendices.[3,4] The Belmont Report was republished on its own in the *Federal Register* the following year. This is a formal mechanism for officially announcing a proposed rule or policy to both government agencies and the US public as well as a means for soliciting comments before government actions.

The Menlo Report was created under a less formal, grassroots process that was catalyzed by the narrower ethical issues raised in ICT computer security research. Discussions at conferences and in public discourse exposed growing awareness of strong ethical debates in computer security research and that existing US oversight authorities might have been unaware of—or might not have believed they had a mandate for reviewing—some of this research.

The beneficence principle maintains that researchers should avoid harm, maximize probable benefits and minimize probable harms, and systematically assess both risk of harm and benefit.

"The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research" is the core document stemming from the series of working group meetings that broached these issues (see the "Menlo Report Working Group" sidebar).[2] Similar to the National Commission's approach, the DHS-supported working group meetings considered previously published and unpublished documents when developing the Menlo Report. This process inspired the production and dissemination of other documents intended to supplement and clarify some of the more complex and controversial aspects of the issues illuminated by the Menlo Report. In this respect, the Belmont and Menlo reports both live within larger bodies of work.

The Core Menlo Report

The working group determined that the core report should reflect the Belmont Report's simple and elegant structure, length, use of language, minimal use of references, and focus. The Belmont Report has only three main sections: the difference between research and practice in the biomedical setting, a set of three basic principles, and the associated applications of those principles. There are only three references, no definitions of terms, and little background on the issue space. Following this model, the core Menlo Report required more detail, background information, case studies, assistive questions, and references to elucidate the nuanced language and explain how ICT complicates the interpretation and application of the principles in the Belmont Report.

The Menlo Report briefly covers motivation and background. It restates the Belmont Report's principles in light of changes brought about by advances in ICT. It then describes the application of those principles in the ICT research context. Specifically, the Menlo Report details four core ethical principles: three from the original Belmont Report—respect for persons, beneficence, and justice—and an additional principle—respect for law and public interest. The report explains each of these in the context of ICT research. Respect for persons requires that

- research subject participation is voluntary and follows from informed consent,

- individuals are treated as autonomous agents, and their rights to determine their own best interests are considered and protected,
- the interests of individuals who are impacted by but not targets of research are guarded, and
- individuals with diminished autonomy and decision-making capabilities are afforded protection.

The beneficence principle maintains that researchers should

- avoid harm,
- maximize probable benefits and minimize probable harms, and
- systematically assess both risk of harm and benefit.

Justice entreats that

- each person deserves equal consideration in how to be treated;
- research benefits should be distributed fairly according to individual need, effort, societal contribution, and merit; and
- subject selection should be fair, and burdens should be allocated equitably across impacted subjects.

The principle of respect for law and public interest, similar to the Belmont Report's conception of beneficence, explicitly charges researchers to

- engage in legal due diligence,
- be transparent in methods and results, and
- be accountable for actions.

To sufficiently address all the principles and their applications, the report stresses the need to understand the relevant stakeholders. These include but aren't limited to ICT researchers, at-risk humans (be they research subjects, nonsubjects, or simply ICT users), malicious actors, network/platform owners and providers, government and law enforcement, and society at large. Such differentiation facilitates balancing benefit and harm, which is more complicated than simply maximizing all benefits and minimizing all harms. Part of this process involves balancing the competing interests of stakeholders who all deserve consideration and protection.

Menlo Report Working Group

The US Department of Homeland Security hosted a two-day workshop on 26–27 May 2009 in Washington, DC, which brought together ethicists, institutional review boards, researchers, and lawyers to discuss ethical issues in information and communication technology (ICT) research. The desired outcome of this meeting was a set of ethical guidelines that, though anchored off the original Belmont Report framework, reflects the unique questions facing ICT researchers. The subset of participants charged with creating this report became the Menlo Report working group, which subsequently held meetings over a 16-month period to create the report. The Menlo Report working group participants are

- Michael Bailey, University of Michigan
- Aaron Burstein, University of California, Berkeley
- KC Claffy, University of California, San Diego
- Shari Clayman, Department of Homeland Security
- David Dittrich, University of Washington
- John Heidemann, University of Southern California
- Erin Kenneally, University of California, San Diego
- Doug Maughan, Department of Homeland Security
- Jenny McNeill, SRI International
- Peter Neumann, SRI International
- Charlotte Scheper, RTI International
- Lee Tien, Electronic Frontier Foundation
- Christos Papadopoulos, Colorado State University
- Wendy Visscher, RTI International
- Jody Westby, Global Cyber Risk

The Menlo Report Companion

The Menlo Report's major appendage is "Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Department of Homeland Security Menlo Report."[5] At 37 pages, the companion document is still significantly less information than the Belmont Report's two volumes of appendices, but its content, references, and case studies similarly reflect working group deliberations and provide crucial adjunct details about a complex topic. The companion document wasn't published in the *Federal Register*; however, it accompanies the core Menlo Report on the DHS website.

The companion goes into greater depth on the Menlo Report's history and relationship to the Belmont Report. It expands on the application of principles, including providing assistive questions that help design and evaluate research in conformance with the stated principles. It uses a single synthetic case study to illustrate a broad range of ethical issues and contains four appendices with reference material supporting both the companion and core documents, including a representative set of case studies and references to

source materials covering industry and academic research.

Other Supporting Activities

In January 2010, an early version of the Menlo Report's principles and applications introduced an ethical impact assessment (EIA) framework intended to facilitate ethical ICT research design and evaluation.[6] In addition, working group members have participated in multiple panels, workshops, and presentations at which the Menlo Report and related topics were discussed. These include the 2010 Workshop on Ethics in Computer Security Research; the 2010 Symposium on Usable Privacy and Security; the 2010 Network and Distributed System Symposium; the Public Responsibility in Medicine and Research's 2011 Social, Behavioral, and Education Research Conference; the 1st International Digital Ethics Symposium; the 2011 Honeynet Project Public Day; the 2011 Annual Computer Security Applications Conference; and the 2011 Anti-Phishing Working Group Meeting. Feedback from these and other interim publications have helped frame the Menlo Report and its companion document, contributed insight for the evolving EIA, and spurred iterative engagement with the community to advance dialogue in this issue space.

After internal discussion and two rounds of reviews by a representative population of ethicists, practitioners, academics, and industry, the core document was published in the *Federal Register* on 28 December 2011,[7] the first at-large public release for comments on the proposed principles and applications.

Moving Forward

The Menlo Report attempts to lower the barrier to entry for researchers and oversight entities dealing with computer security research ethics. As such, it's an important first step, but it represents only part of the needed community response to existing ethical challenges.

The security research community and the larger ICT research domain (for example, network measurement, computer-human interface, and software engineering) lack shared community values, those guiding principles around which we can assess, systematize, influence, and justify research conduct.[1] The growth and persistence of debate among relevant conference program committees over the ethical propriety of certain research exemplify this disharmony. Although agreement on core principles might not be uniform, the larger challenge lies in galvanizing the principles into coherent applications and implementations.

In addition, the community faces a dearth of domain guidance and technical enablers to translate the abstract and theoretical ethics principles into practicable actions. Specifically, there is a lack of formal institutional and ad hoc peer guidance in ethical decision-making, thereby reinforcing the vacuum in which first-order ethics principles are embraced at the community level. Further, assuming the existence of guidance, researchers are in want of tools that embed, consistently reproduce, and scale such expert ethics advice. An ethics-by-design strategy for computer security researchers demands tools that operationalize the defining principles.

Finally, there is a shortage of forcing functions for implementing the applications of ethics principles. Specifically, although institutional review boards have largely shouldered the mandate to ensure ethics in research involving human subjects, many question their relevance and capabilities in computer security research. And it's unclear the extent to which other institutions, such as conference program committees or funding agencies, are able or willing to provide the oversight and quality control necessary to ensure that ethics issues are identified, applied, and evaluated in research endeavors—let alone to do so consistently.

The Menlo Report and its companion document attempt to galvanize ethics principles and their applications. This path forward is one recipe to enable the community to embrace a self-regulatory approach to embedding ethics in research by way of a more mature and community-built notion of what is ethically defensible.

An alternative is to wait for an unfortunate event to trigger hasty, top-down mandates that won't likely reflect this community's input. ■

References

1. D. Dittrich, M. Bailey, and S. Dietrich, "Building an Active Computer Security Ethics Community," *IEEE Security & Privacy*, vol. 9, no. 4, 2011, pp. 32–40.
2. "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," D. Dittrich and E. Kenneally, eds., US Dept. Homeland Security, 2011; www.cyber.st.dhs.gov/wp-content/uploads/2011/12/MenloPrinciplesCORE-20110915-r560.pdf.
3. Nat'l Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, "The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research," appendix vol. 1, Dept. Health, Education, and Welfare Publication no. (OS) 78-0013, 1979;

http://videocast.nih.gov/pdf/ohrp_appendix_belmont_report_vol_1.pdf.
4. Nat'l Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, "The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research," appendix vol. 2, Dept. Health, Education, and Welfare Publication Publication no. (OS) 78-0014, 1979; http://videocast.nih.gov/pdf/ohrp_appendix_belmont_report_vol_2.pdf.
5. "Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Department of Homeland Security Menlo Report," D. Dittrich and E. Kenneally, eds., US Dept. Homeland Security, 2011; www.cyber.st.dhs.gov/wp-content/uploads/2012/01/MenloPrinciplesCOMPANION-20120103-r731.pdf.
6. E. Kenneally, M. Bailey, and D. Maughan, "A Tool for Understanding and Applying Ethical Principles in Network and Security Research," *Workshop Ethics in Computer Security Research* (WECSR 10), Springer, 2010, pp. 240–246.
7. "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," *Federal Register*, vol. 76, no. 249, 28 Dec. 2011, p. 81517.

Michael Bailey is an assistant research scientist at the University of Michigan. Contact him at mibailey@eecs.umich.edu.

David Dittrich is a senior security engineer and researcher at the University of Washington. Contact him at dittrich@u.washington.edu.

Erin Kenneally is an information technology law specialist at the Cooperative Association for Internet Data Analysis, University of California, San Diego. Contact her at erin@caida.org.

Doug Maughan is division director, Cyber Security Division, at the Department of Homeland Security Science and Technology Directorate. Contact him at douglas.maughan@hq.dhs.gov.