

Ethics governance development: The case of the Menlo Report

Social Studies of Science
2023, Vol. 53(3) 315–340

© The Author(s) 2023



Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/03063127231151708

journals.sagepub.com/home/sss



Megan Finn¹  and Katie Shilton²

Abstract

The 2012 Menlo Report was an effort in which a group of computer scientists, US government funders, and lawyers produced ethics guidelines for research in information and communications technology (ICT). Here we study Menlo as a case of what we call *ethics governance in the making*, finding that this process examines past controversies and enrolls existing networks to connect the everyday practice of ethics with ethics as a form of governance. To create the Menlo Report, authors and funders relied on bricolage work with existing, available resources, which significantly shaped both the report's contents and impacts. Report authors were motivated by both forward- and backward-looking goals: enabling new data-sharing as well as addressing past controversies and their implications for the field's body of research. Authors also grappled with uncertainty about which ethical frameworks were appropriate and made the decision to classify much network data as human subjects data. Finally, the Menlo Report authors attempted to enrol multiple existing networks in governance through appeals to local research communities as well as taking steps towards federal rulemaking. The Menlo Report serves as a case study in how to study ethics governance in the making: with attention to resources, adaptation, and bricolage, and with a focus on both the uncertainties the process tries to repair, as well as the new uncertainties the process uncovers, which will become the site of future ethics work.

Keywords

ethics work, ethics governance, computing ethics, research ethics

Computing research has generated a range of ethical controversies, from inappropriate reuse of digital research data (Rosenberg et al., 2018) to the development of racist and oppressive machine learning tools (Benjamin, 2019). To resolve these controversies,

¹University of Washington, Seattle, WA, USA

²University of Maryland, College Park, MD, USA

Correspondence to:

Megan Finn, Information School, University of Washington, Box 352840, Mary Gates Hall, Seattle, WA 98195, USA.

Email: megfinn@uw.edu

technologists and advocates have proposed new ethics guidelines or requirements, from self-imposed research guidelines to publication requirements. Many of these projects, led by researchers and technologists, echo historical science and technology self-governance projects, such as the 1975 Asilomar conference (Berg, 2008; Hurlburt, 2015; Parthasarathy, 2015) and the 1978 Belmont Report (Childress et al., 2005; National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 2010; Stark, 2012).

To understand the dynamics that encourage such work, and to provide context for current struggles in computing ethics and governance, this paper presents analysis of a recent, lesser-known historical case study: the writing of research ethics guidelines for computer science almost a decade before the recent wave of attention to computing ethics. Beginning in 2009, a group of computer scientists, lawyers, and government officials made a sustained effort to set ethical guidelines for computer security and network measurement research, which culminated in the 2012 release of the Menlo Report in the United States' Federal Register. Both the report itself and the process of producing it were efforts to address ethical controversies in a technical field and support localized ethics work within labs and research groups through governance. Borrowing Slayton's (2021, p. 3) phrasing, the effort enlisted networks of actors to 'steer' a technological trajectory. Menlo gathered illustrative case studies of previous ethics controversies; used these to author principles meant to influence the actions of security and network researchers; and made both content and dissemination choices to recruit funders, university Institutional Review Boards (IRBs), and conference committees to exert ethical influence in security research. We call the process of bridging from controversy and localized work to plans *ethics governance in the making*. Ethics governance in the making, as we found by studying the Menlo Report, is a bricolage process situated between ethics in practice and ethics as governance. This paper offers a framework for analysing current and future governance in the making processes based on our case study of the Menlo Report.

The ethics governance in the making of the Menlo Report is of particular interest now as computing confronts ethics and justice crises in data and artificial intelligence research (e.g. Greene et al., 2019; Hoffmann, 2019, 2021; Shilton et al., 2021). Although much about the Menlo Report evoked both Asilomar and Belmont before it – multiple and protracted in-person meetings resulting in ethics guidelines like Belmont, composed predominantly of domain researchers and lawyers like Asilomar – the work and impacts of Menlo differed starkly from either. We studied the making of Menlo to answer our central research questions: What sparks a group to do the resource-intensive work of imagining governance? What challenges does governance in the making present? And how does the work of envisioning governance influence what becomes seen as ethical action and guidance for a field? Interviews with report participants help us interpret both why and how the report and its guidelines came to be, providing a study in the motivations, processes, and consequences of a technical community shaping controversy and existing localized ethics work into mechanisms for ethics governance.

Our interviews revealed that, in the case of the Menlo Report, the work of the report was shaped by forward- and backward-looking goals. Report authors had future researchers in mind, hoping to enable new forms of research through data sharing. But they were

also concerned with repairing a record of past controversial research practices and resolving an uncertainty disrupting their field: whether to treat their research data as human subjects data. To accomplish these goals, the authorship team relied on resources at hand: The group was assembled and funded through an existing technical program, and rather than developing new ethical principles for responsible network and security research, authors adapted existing principles established for clinical research. The work of ethics governance in the making looks like much of the rest of laboratory life: the bricolage of actors making sense of problems within the web of relations and materials at hand (MacKenzie, 2003; MacKenzie & Pablo Pardo-Guerra, 2014). Finally, each of these whys and hows – the circumstances of the making – shaped Menlo’s imagined governance as well as its recruitment of networks to steer computer security research. Perhaps Menlo’s greatest legacy is that, by reframing network and security research in terms borrowed from human subjects research ethics, the Report uncovered and produced new challenges and uncertainties for defining ethical research practice, prompting ongoing localized ethics work from security and network researchers.

Ethics work and ethics governance in the making

To understand the work of the Menlo Report, we draw upon a long tradition of studying controversies in science and engineering (Jasanoff, 2012). Focusing on ethics controversies unites technoscience actors and their everyday practices with larger social questions about power, outcomes, and the obligations of science or design (Ames, 2019; Rosner, 2014). Particularly relevant is the work of STS scholars who have focused on ‘constitutional moments’ (Hilgartner, 2018, 2019; Jasanoff, 2003): times when the ontological bases of ethics – what will be considered as ethical or unethical – are being renegotiated within the field. Hurlburt (2015) has argued that participants at the constitutional moment of Asilomar resolved ethical controversies by focusing on containment of recombinant DNA to scientific laboratories, defining the safety and security of this research as dependent upon the careful practice of professionals. And though Belmont established influential principles through long and ongoing ethical reflection, Stark (2012) has demonstrated that the implementation of Belmont principles through federally mandated Institutional Review Boards also reified expert practice, defining human research ethics as a matter of procedure rather than principle. Inspired by work on constitutional moments, we sought to understand what work results during these moments, and how that work can shape the content of guidelines and the impacts of resulting governance.

To understand the work of constitutional moments such as Menlo, we draw upon an intersection of previous research on *ethics work* as everyday, localized ethics in practice (Ziewitz, 2019), and *governance* as something produced by networks attempting to resolve uncertainties (with varying degrees of success) (Slayton, 2021). Concepts such as ‘ethics work’, ‘ethical work’, and ‘ethical moment’ differ in the context of use, but all highlight the difference between normative ethics and ethics in practice. Situated ethics work research is part of a larger trend within STS and anthropology (see Fassin, 2014) focused on social science contributions to understandings of ethics (Haimes, 2002). For example, Ziewitz sets forth the concept of ‘ethical work’: his research participants attempt to ‘artfully arrange themselves to cope with moral ambiguities’ (Ziewitz, 2019,

p. 707). Ziewitz discusses absence of ‘ontological security’ in daily ethics practice: the participants he studies navigate when and whether their topics and foci require discussion of good and bad, right and wrong. In a study of ethics at work in data sharing, Heeney (2017) is similarly interested in uncertainties that evoke ethical debate, using the term ‘ethical moment’ to describe: ‘an ontological controversy that allows both analyst and actor to consider ethical possibilities beyond practices and abstract moral frameworks’ (Heeney, 2017, p. 4). Heeney’s interviewees found that in ethical moments, ‘existing guidance does not adequately capture what is happening... Rather, it is a creative response to the sorts of dilemmas with which the interviewees grapple’ (Heeney, 2017, p. 19).

Ethics work, ethical work, and ethics moments are typically used to describe work that did not follow explicit ethics guidelines but instead were ethics in practice. If scholars such as Ziewitz and Heeney are examining how ethical practice evolved in the absence of explicit rules, we are studying how, in the absence of clear rules, a Menlo report authors collectively addressed ‘ethics moments’ and engage in ‘ethics work’ as they tried to find, make, adapt, and adopt rules from other domains in pursuit of *governance*: the steering towards desired outcomes by complex networks of actors (Slayton, 2021). Slayton (2021) argues that governance networks become more regime-like, and better at steering outcomes, when they not only enrol actors in their goals, but also cut ties with any actors who undermine those goals, cutting members from the network. The idea of ‘ethics as governance’ is familiar to STS researchers. For example, a review of STS research about the National Institute of Health’s ‘Ethical, Legal and Social Implications’ (ELSI) program traces how ethics programs enacted forms of governance as researchers reframed and closed scientific controversies by producing new forms of ethical expertise, and used that expertise to address uncertainties through reflection or institutional action (Hilgartner, Prainsack, & Benjamin, 2016). The process of creating the Menlo Report represented explicit and conscious ethics work to respond to controversies, shaping that work into imagined and enacted forms of governance that both enrolled the research community and cut ties with research that didn’t follow the guidelines set forth in the report. Attention to the ethics work performed while writing the Menlo report reveals key differences from previous constitutional moments in science and technology ethics – differences which shaped both Menlo’s imagined governance mechanisms and its eventual impact.

Approach: Studying the Menlo Report

Ethics work has occurred side by side with technical work in both network and computer security research for decades. The computer security research community has long debated ethical issues such as the acceptability of monitoring network traffic for research, the political consequences of e-voting security analysis, and principles for handling vulnerability disclosures. As early as the 1980s, the computer security community debated the ethics of experimentation without informed consent (Spafford, 1989, 1991, 1997, 2003). When a U.S. graduate student who sought to reveal security inadequacies in computer networks built a virus to exploit particular security defects, the community debated the appropriateness of such practices (Denning et al., 1987; Spafford, 1997).

These conversations and challenges have continued; for example, studies using intrusive methods without user consent generated controversy among researchers and program committees more recently (Burnett & Feamster, 2015; Narayanan & Zevenbergen, 2015; Sharma, 2021).

Our project began with the question of how localized ethics work coalesced into a formalized governance effort. The Menlo Report effort began in 2009 as a series of workshops attached to meetings of researchers funded under a U.S. Department of Homeland Security (DHS) Science and Technology Directorate Project called PREDICT (Protected Repository for the Defense of Infrastructure Against Cyber Threats).¹ Researchers in computer science (particularly in the areas of network measurement and network security), lawyers, and government bureaucrats drafted the report during meetings over sixteen months, organized by a DHS program officer and led by a legal scholar who was embedded with a network measurement research lab.

Though Asilomar's 'ghost' (Parthasarathy, 2015) and Asilomar-in-memory (Hurlburt, 2015) continue to shape ethics self-governance efforts in numerous scientific and technical fields (Campos, 2010), our participants didn't discuss Asilomar as a model. Instead, the Menlo authors looked to the Belmont Report. The final 14-page Menlo Report was published in 2012 (Dittrich et al., 2012) and builds directly on core principles articulated in the 1979 Belmont Report: respect, beneficence, and justice. Stark (2012) describes how Belmont's principles have become guidance for interpretation by the university Internal Review Boards mandated by the same law that commissioned the Belmont Report. She defines the implementation of Belmont's principles in the ritualized processes of review processes as 'governing by experts', because the Belmont principles and their implementation was adapted and adopted to suit the research needs and researchers of the time. The Menlo Report took Belmont's principles, which were crafted for 20th-century health research and stretched over the ensuing decades to cover social science, and attempted to fit them to guide ICT research. For example, in the Menlo Report's discussion of the Belmont principle *Respect for Persons*, the report argues: 'In the ICTR [Information and Communication Technology Research] context, the principle of *Respect for Persons* includes consideration of the computer systems and data that directly interface, integrate with, or otherwise impact persons who are typically not research subjects themselves' (Dittrich et al., 2012). The Menlo Report authors also added a fourth principle evocative of major debates in the field: 'respect for law and public interest'.

A companion document to the Menlo Report, 'Applying Ethical Principles to Information and Communication Technology Research' (Dittrich et al., 2013), was released in October of 2013. The document includes 20 case studies drawn from news articles and research publications that apply the principles set forth in the Menlo Report. These case studies, as well as a detailed appendix, document controversial network and security research discussed in the workshops that led up to the Menlo Report and underpinned discussions of specific harms about which the authors were concerned. The companion also contained more details about how to apply the Belmont principles to ICT research through 'assistive questions' for researchers.

In addition to analysing the Menlo Report documents, we sought to understand the work of the report by conducting interviews with its authors. The report identifies 15

‘authors and working group participants’ by name. We reached out to all 15 and received responses from 12. One person declined to be interviewed, citing an administrative rather than writing role in the project. We conducted interviews with the eleven other respondents in 2018, using VOIP or telephone, taking notes as well as recording and transcribing the interviews. Our semi-structured interview protocol focused on the work of creating the report: Our questions focused on how participants became involved, how the writing and collaboration process was organized and supported, the reasoning behind both adopting and adding to the Belmont principles, and the influence and legacy of the report. We coded interview transcripts and notes using an emergent thematic coding framework focusing on elements of the lifecycle of the report (inspiration and motivation, people, process, funding, conflicts, and influence) as well as themes within the content of the report (normative ideas, the influence of IRBs, Belmont, and law, and advice for other communities). Throughout the coding process, we met weekly to discuss emergent themes and findings from the interviews. We triangulated the interviews with published documents, particularly scholarly communications by authors published prior to and following the publication of the Menlo Report.

The interviews, Menlo Report, and companion document demonstrated how the work of the committee encompassed both *ethics* work, as they tried to put themselves in the place of researchers doing controversial work and attempted to figure out what constituted ‘being ethical’ (Ziewitz, 2019), and *governance* work of enrolling and cutting members (Slayton, 2021) of the network by demonstrating what was and was not acceptable research. Authors also imagined how the report would govern the research community through regulatory and gatekeeping mechanisms. Our analysis reveals that report authors were motivated to participate in translating local ethics work into a vision for ethics governance by both a perceived need for repair in the field and anticipation of new research possibilities. But in the process of repair and anticipation, the authors discovered new complexities as they reimagined the entire field of ICT research to comply with the U.S.’s clinical tradition of research ethics. We understand the work of the Menlo Report as involving five significant overlapping processes: finding resources to complete the project, repairing past ethical misjudgements, anticipating future challenges and possibilities, resolving ethical uncertainties, and closing controversies.

Resources and logistics for governance in the making

Ethics governance in the making – concretizing local ethics work into guidance for an entire field – requires substantial resources. The first challenge facing the Menlo Report organizers was how best to support and conduct the work that would be required. Report authors estimated that project meetings took place quarterly, numbering 10–12 meetings during the writing period from 2009–2011. Between meetings, groups of participants would write and iterate on drafts of the report based on the discussions. The final group of authors did not include everyone who participated in the workshops throughout the period of creating the Menlo Report, but instead a core group who had attended most of the workshops. Though two lead authors were paid for some of their time, most of the final authorship group were volunteers.

Present and absent dynamics: Who participated?

The Menlo Report conveners bootstrapped writing efforts through the U.S. Department of Homeland Security's Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) program. PREDICT was designed as a 'publicly available, legally collected, distributed repository of large-scale datasets containing real network and system traffic that could be used to advance state-of-the-art cybersecurity R&D' (Department of Homeland Security, 2013). For example, researchers working to understand cyberattacks might need data about network use generated by ISPs, but barriers ranging from norms to law could prevent ISPs from sharing that data with researchers. PREDICT provided 'administrative, legal, and ethical brokering' between data holders and data users, as well as search tools and secure hosting.

The Menlo Report was not alone in having data sharing as an impetus for discussion of the ethical. Scholars such as Heeney have discussed how data sharing in biomedical research can bring ethical discussions to the surface: 'Data sharing ... posed a challenge to what people had been doing or prompted discussion about what they would like to do' (Heeney, 2017, p. 9). Similarly, both PREDICT researchers and program officers became interested in questions of what network researchers had been doing, and what they would like to do. As Participant 11, a researcher, explained: 'We [PREDICT researchers] were essentially doing what the Menlo Report was trying to address. We were collecting data, and actually we were collecting fairly sensitive data.' The synergy between PREDICT's data sharing goals and the ethical questions engendered in such data sharing enabled financial and logistical support for the Menlo Report. As Participant 6, a DHS program officer at the time, described it: 'it just seemed like a natural extension of that [PREDICT] program to do the Menlo Report and then the accompanying document along with it'.

PREDICT enabled the Menlo Report in a variety of ways. Writing workshops were connected to PREDICT PI meetings, generally occurring a day before or afterwards. Holding the ethics workshops in conjunction with the PREDICT meetings meant that it was easy for associated researchers to attend. This co-location strongly shaped participation in the project: The people who participated in the report were primarily academic researchers and were largely from the network measurement and network security sub-fields of computer science. The researchers were joined by a handful of people recruited by PREDICT organizers, primarily lawyers with expertise in cybersecurity law. One participant remembered the initial workshops having about 50 participants, 40 of whom were computer scientists, and 'the other 10 of us were scattered lawyers or people who were members of IRBs to provide this sort of more ethical side of it'. In the final list of authors, comprised of long-term participants, six of the authors were active computer science researchers in academia or technical research institutes, four were working as lawyers or law scholars, two were employed by the Department of Homeland Security, and two were working in research protection for a research organization.

The lawyers and legal scholars invited were also deeply involved in the network measurement and network security research community, participating regularly in security conferences, and taking part in regular consultations with security researchers. These security-involved legal professionals were recruited to serve as experts in security practices and the law, but also as critics. During this time, civil society groups (including the

Electronic Frontier Foundation [EFF], represented among the report authors) were engaged in legal battles with the DHS over the USA PATRIOT Act and other data collection laws. As Participant 9, a lawyer, reasoned:

It's in a government agency's interest to understand what kinds of criticisms are going to be levied against you both on A: Are we doing the right thing, and B: Regardless of whether we're doing right thing, we should know how people are going to try to criticize or stop us from doing what we want to do.

Early organizers did make efforts to expand the group beyond PREDICT PIs and researchers, legal scholars, and working lawyers. Project coordinators reported that they had reached out to scholars in ethics-related disciplines but didn't get volunteers. Though ethicists, publics, and social scientists are routinely participants in ELSI-style ethics governance projects (see Hilgartner, Prainsack, & Benjamin, 2016), ethicists were largely absent from the Menlo Report proceedings and social scientists and representatives of the public were entirely absent in the production of the report. As Parthasarathy (2015) explains in her discussions of Asilomar, without social scientists and public representatives, the team lacked expertise on sociality, inequality, work practices, or institutional dynamics that might support the implementation of governance frameworks. The authorship group also reflected the lack of racial and ethnic diversity within computer science, limiting the standpoints incorporated into the final recommendations. By directly involving technical researchers as lead authors, the Menlo Report incorporated expertise in thorny technical problems, knowledge of existing U.S. academic structures for supporting research ethics, and meaningful influence on the security research field through subsequent service on program committees. But it was up to the lawyers in the group to challenge technical perspectives.

Authors also worried about the lack of representation from broader fields of ICT research, as well as the problem of recruiting only those already concerned enough about ethics to show up. The self-selection of researchers who cared about ethics coupled with the exclusion of researchers who 'had records that weren't really ethical' led Participant 8, a researcher, when asked what they might have done differently in retrospect, to respond: 'I would probably have a series of different focus groups' to increase the variety of perspectives and encouraging wider buy-in from the research community. Participant 9 described it this way:

I was a volunteer who wasn't paid for anything. ... If we were trying to start it up again, you would have to fund it much more seriously. You would have to get more points of view represented in the process and actually try to surface more conflicts and more of the hard questions.

Finally, the researchers who had engaged in past problematic research were not part of the conversation, leading some on the committee to think that this limited what was included in the report, and didn't enable a process where hard questions were tackled. The authorship group reflected the need to balance aspirations with practicalities: authors were concerned with the legitimacy of the process, but also with creating an authorship group that would complete the project, and a group that could help ensure that the Menlo

Report's principles would have influence. Participant 7, a researcher, summed up the process: 'I think, like [Churchill's] democracy, it was a miserable process but maybe the best we could get.'

Missing parties in the process of assembling the Menlo Report constitute 'absent dynamics' (Heeney, 2017, p. 10). As Heeney (2017, p. 19) describes, ethics moments can arise in instances where parties and relations are absent, for example when consent forms as ethics mediators instead of clinicians working directly with patients and families to discuss uses of their data. Although it is difficult to know the full impacts of the absent dynamics of the Menlo Report, the decision to adhere to an existing research ethics framework (and regulatory structure) seems one such impact. As the report presents in its introduction:

In framing the principles and applications for evaluating and applying ethics in ICTR the Menlo Report explicitly adopts the Belmont principles and acknowledges the Common Rule regime which implemented that model. As such, this Report deliberately does not explore alternate ethical paradigms, and while not discounting that there may be novel implementations of the Belmont Report principles and applications that should be considered it makes no definitive recommendations in that regard (Dittrich et al., 2012, p. 7).

The present and absent dynamics of Menlo's team facilitated its governance work and limited the novelty of the Report's ethical approach.

'Socializing' the Menlo Report

After the Menlo Report was written, resources were still needed to circulate it and engage the envisioned governance networks such as program committees and Institutional Review Boards. Menlo's transition to actualized governance was challenged by both logistics and resources. As a first step, the team took a path modelled on the Belmont Report but unusual for computer science codes of ethics: They published the Menlo Report in the *Federal Register*, the official channel for sharing and requesting public feedback on U.S. government agency rules. A public chance for comment differentiated Menlo from many science and technology self-governance projects, such as Asilomar, which have been criticized for a lack of public participation (Hurlburt, 2015; Parthasarathy, 2015). Though public representatives didn't participate in writing the Menlo Report, they had opportunity to provide comments. But even government employees among the report authors acknowledged the limitations of this dissemination approach. As Participant 6 told us: 'And even still, it's only people that follow Washington that actually know what the *Federal Register* is.' The Menlo Report was first published online in December 2011 and received sixteen public comments (Submission for Review and Comment: "The Menlo Report," 2011; Response to Comments Received for "The Menlo Report," 2012). Though the process of publishing the Menlo Report in the *Federal Register* was the start of the process for federal agency rulemaking, ultimately, the Department of Homeland Security did not complete the rulemaking process. As Participant 4, a researcher who later became a DHS employee, put it, 'Someone should

Table 1. Network measurement and security conferences with ethics requirements.

Conference	Year ethics requirement added to CFP
ACM IMC	2009
SOUPS	2011
USENIX Security	2013
NDSS	2016
ACM SIGSAC	2017
IEEE Symposium on Security & Privacy	2017

ACM: Association for Computing Machinery; SIGSAC: Special Interest Group on Security, Audit and Control; IEEE: Institute of Electrical and Electronics Engineers (IEEE Symposium on Security and Privacy is ; NDSS: Network and Distributed System Security; SOUPS: Symposium on Usable Privacy and Security; IMC: Internet Measurement Conference; SOUPS: Symposium on Usable Privacy and Security; USENIX refers to the USENIX Security Symposium.

have led the process with the rulemaking. ... We should have tried to do that lift, [but] it would have been a heavy lift.'

Sharing the report in the *Federal Register* signalled that the authors intended to recruit powerful existing federal networks for governance, but Menlo's recommendations were never formally adopted by the government agencies that fund computer science research. Instead, Menlo's primary influence was on academic networks of peer review. Conference committees could effectively steer the ethics of security and network measurement research by 'cutting' (refusing to publish) research that didn't adhere to Menlo recommendations (Slayton, 2021). As Participant 4 recounted: 'It's about changing norms – you don't see it right away. I can now point to top security conferences that require ethical statements. I consider this a clear victory.' Participant 4 went on to describe the process of enrolling academic governance networks as: 'Once it was written, then we just kind of went on kind of the socialization tour at various conferences and workshops. I know we targeted the IRB community.'

In addition to the 'socialization tour', in the years since the Menlo Report was published, conferences attended and run by Menlo authors included requirements for authors to reflect on the ethics of their methods, including whether they were subject to IRB review (see Table 1). After these conferences added the requirement for discussions of ethics and human subjects to their calls for papers, the conferences also saw an increase in papers discussing ethics and IRB. The earliest conference in these fields to require an ethics statement was the ACM's Internet Measurement Conference (ACM IMC) in 2009. Citing the controversies in measurement discussed below, the IMC call for papers stated 'Ethical standards for measurement must be considered by all IMC authors' (ACM IMC, 2009) – notable because two of the Menlo Report authors were on the program committee. Among security research conferences, the Symposium on Usable Privacy & Security (SOUPS) began asking authors in 2011 to explicitly state whether IRB approval had been obtained for their research. One of the highest status conferences in the computer security field, USENIX, included the following requirement in their call for papers for USENIX 2013:

Papers that describe experiments on human subjects, or that analyse non-public data derived from human subjects (even anonymized data), should disclose whether an ethics review (e.g.,

IRB approval) was conducted and discuss steps taken to ensure that participants were treated ethically. (22nd USENIX Security Symposium, 2012)

The ACM Special Interest Group on Security, Audit and Control (SIGSAC), the IEEE Symposium on Security and Privacy (Oakland), the Network and Distributed System Symposium (NDSS) and the Internet Measurement Conference (IMC) all went on to add requirements in 2016 and 2017. In 2019, IMC even incorporated specific language and links guiding participants to the Menlo Report: ‘Authors may want to consult the Menlo Report for further information on ethical principles and the Allman/Paxson IMC 07 paper for guidance on ethical data sharing’ (ACM IMC, 2019). These standards set by major conferences such as IMC have also been adopted by more specialized venues. For example, in 2022 the Passive and Active Measurement Conference referred participants to the Menlo Report and the Alman/Paxton paper (discussed in the next section) and noted the influence of IMC: ‘Following the standard set by the Internet Measurement Conference (from which we base this section), papers describing experiments with users or sensitive user data (e.g., network traffic, passwords, social network information) must follow basic precepts of ethical research and subscribe to community norms’ (Passive & Active Measurement Conference, 2021). The Menlo Report’s direct influence on program committees is difficult to determine, but within the fields of network measurement and computer security we can see new attention to research ethics that coincides with the Menlo Report writing, publication and circulation.

When interviewed, Menlo authors had varying opinions on whether the Menlo Report principles have successfully steered the security and network measurement research community. When one of our interview questions characterized the Menlo Report as an instance of the security community coming together, at the time of our conversation in 2018, Participant 2, a researcher, pushed back:

But I wouldn’t characterize it the way that you did, about the security community coming together and deciding to do this. In fact, I think it’s quite not that, importantly not that. The security community, to my knowledge, has still not come together to do something like this.

That is, some of the authors involved in the writing of the Menlo Report did not feel that enough of the research community had been engaged in the project for it to have the governance impact that they imagined. Most of the researchers that we spoke to regretted that there were not more financial and personnel resources devoted to socializing the Menlo Report in technical research communities. Some of the authors also regretted that the report was not given enforcement mechanisms either through sustained efforts to work with IRBs or rulemaking that would mandate its use by government funded researchers. (Other authors did not want the document to effect regulatory change, as we discuss below.) Limitations in resources shaped not only the work of creating the Menlo Report, but also its governance impacts.

While the Menlo Report was not adopted as federal regulation, the Report and the authors were part of shaping an important gatekeeping arena of academic computer science. Conference program committees write conference calls for papers and coordinate peer reviewing. This gatekeeping work is an opportunity for both enrolment into conference ethics requirements and for cutting research that does not adhere to these

requirements – where the work of the ethics governance in the making that is the focus of this paper starts to resemble governance (Slayton, 2021).

‘If he did it, we can do this’: Repair and anticipation

Resources shaped the work and impact of Menlo, but don’t explain why Menlo’s volunteer participants undertook the significant work of the report. Some participants in Menlo expressed hopes that prudent self-governance would prevent outside regulation, mirroring earlier efforts such as Asilomar (Parthasarathy, 2015). Participant 7 observed: ‘Of course, we were all working hard to avoid mistakes that would precipitate such a crisis event, so that might slow that top-down regulation.’ The respondent’s emphasis on preventing a crisis event is telling, however: While Asilomar researchers were working in the realm of largely hypothetical future harms from recombinant DNA, many Menlo participants believed harms had already been precipitated by security and network measurement research. In this section, we attend to discussions within the security and network measurement research community that predated the Menlo Report and, according to our interviewees, were of concern to the conveners. We argue that participation in the Menlo Report was inspired by, and participated in, processes of repair and anticipation bound together: As researchers defined past ‘wrong action’ in their field, they tried to build guidelines for a future that would not repeat that past. However, participants also felt they were working in a world of constantly changing norms, making the future complex to anticipate. Participant 2 told us:

And indeed, one of the things we were trying to address is that what we were observing in the field of program committees and the way research moves forward, is that program committees would find themselves in a quandary because they would get a paper to review, and they would think, ‘Eh, this is a little squirrely, but it’s good technically.’ And we don’t really have guidelines for whether something that might be above the bar technically but might make us a little nervous to publish with respect to the ethics of the methodology or the data collection.

Concerns informed the data-sharing efforts of PREDICT and in turn served as a catalyst for the work of the Menlo Report. As Participant 3 told us: ‘Others were reading in published papers how some researchers were conducting their research and using data and saying, “Wow, if he did this, we can use this approach too.”’ As suggested by this phrasing, the attention and energy put into the Menlo Report was both backward- and forward-looking: an effort to repair the past record of the field around the controversies documented in both our interviews and in the Companion to the Menlo Report (‘he did it’), as well as an attempt to anticipate and prevent new controversies (‘we can use this approach too’). Both are themes resonant with existing STS research on ethics work. For example, Jacob (2019) sees ethics governance work done by the Committee on Publication Ethics (COPE) through the lens of repair, showing that: ‘publication ethics and research records themselves get created via the language of repairing publications’, (Jacob, 2019, p. 79). Jacob attends to several ‘forms of doings’ which ‘institute an ethics of repair’ around problematic published scholarly communications. The ethic of repair operationalized in the Menlo Report was focused on avoiding the repetition of past mistakes rather than restitution for harms caused in the past.

Perhaps the clearest example of repair work was the companion document compiled by report authors. As Participant 6 explained ‘I wanted to make sure that the cybersecurity research community didn’t get these major black eyes from the [work] researchers were doing 10 years ago.’ The companion document studied 20 specific cases as exemplars of activities which ‘still comprise many of the activities that regularly do occur in academic research and serve to illuminate the ethical issues’ (Dittrich et al., 2013, p. 28). The companion document analysed these twenty cases from the perspective of report principles, reshaping these cases as exemplars of what researchers might do by re-examining and rethinking past ethical mistakes, simultaneously working to anticipate the future through repairing the past.

As researchers tried to grapple with past mistakes, they also tried to anticipate the future. The Menlo Report authors anticipated a critique of their report during the writing: that the Menlo Report wouldn’t be able to establish meaningful norms for a field in which technology and research abilities were constantly changing. Participant 2 explained:

[S]ome of the computer scientists said, ‘Look you can’t really do this because the norms are changing, and they’re different from person to person, they’re different from year to year.’ ... As technology changes, to make things easier to do, people’s sense of what’s okay changes. That was the, I would argue maybe even the prevailing view at one point in some of the rooms where we tried to shop this report.

Creating ethics guidelines for changing technological possibilities is a form of anticipatory governance (Adey & Anderson, 2012; Ananny & Finn, 2020; Guston, 2014; Shilton, 2015; Steinhardt & Jackson, 2015) tying the work of repair directly to the problem of anticipation. We interpret the project of the Menlo Report as one of many ‘forms of doings’: the process of making the Menlo Report, as ethics-governance in the making, was creative act of balancing old problems with novel and emerging problems (Jacob, 2019).

Moral panics or research scandals can be explanations for new ethics governance efforts (Fitzgerald, 2005), but the Menlo Report was more in the tradition of gradualist institutional change (Hedgecoe, 2017; Stark, 2012). Though a desire for repair was a constant theme in our interviews, report authors largely agreed that no single ethics catastrophe motivated the work of the Menlo Report, nor were violations of community norms and ethics splashed on the front pages of newspapers (as digital research ethics controversies now sometimes are). Ethics scandals were not the topic of intense civil society pressures (see Campos, 2010, p. 19 for a discussion of pressure on the ethics and implications of synthetic biology research for an Asilomar-like conference). And the Menlo Report was not part of a broader government-funded research effort into the ethical implications of the field, like the National Nanotechnology Initiative (Brey, 2012; Kaplan & Radin, 2011) or the Human Genome Project (Hilgartner, 2018; Hilgartner, Prainsack, & Benjamin Hurlbut, 2016; Hilgartner, 2019). Neither did Menlo authors feel network and security controversies raised the urgency and alarm of the examples addressed by the authors of the Belmont Report. As Participant 9 reflected on the characterization of network and security research by some of the participants:

We are not infecting people with syphilis; we’re not doing a Milgram experiment that’s going to necessarily like scar someone emotionally... there’s a removal, a distance between the

between the human beings doing the things and researcher. It was not, it felt it wasn't quite as visceral a thing.

But even these less-visceral controversies contributed to the Menlo Report participants' impression of a research record in need of repair, and the anticipation of both new research controversies and needs. First, authors noted that the growth and importance of the Internet inspired increased research using new techniques focused on measuring and monitoring digital networks, and that this increase in research occurred while the Internet was becoming more central to peoples' lives. As Participant 11 recounted, this differed from the early days of networking, when researchers would routinely monitor networks in computer science departments and use the data with the permission of network administrators or department head:

Nobody was really paying attention as to how the data was collected, how ethically it was and so forth ... [But] once the scale became larger, they reached the Internet levels, then that's when people started realizing that this is a serious measurement effort it affects pretty much everyone on the Internet.

As the scale of networks grew, the scale of network measurement data collection grew, and the ways that this data was shared became more complex. And as a key goal of the PREDICT program, with which most Menlo authors were associated, was enabling future data sharing, anticipating this complexity was an important goal for Menlo authors.

With that complexity, new controversies arose. Several papers published between 2006 and 2009 sparked concern among the Menlo Report authors about unethical and potentially illegal research practices. For example, in a paper published in 2007, a group of researchers attacked a supposedly anonymized network dataset and showed that it was vulnerable to deanonymization attacks (Coull et al., 2007). The dataset in question was shared with the paper authors by another group of researchers (Pang et al., 2006). Both the ease of deanonymizing network data as well as the perceived violation of data sharing norms alarmed researchers. The authors of the original article had not expected that their colleagues would deanonymize the shared data, and published a rebuke (Allman & Paxson, 2007): '[N]o matter how careful a [internet] provider is, they need to understand that they *are releasing more information than they think*' (p. 136, original emphasis). They reasoned that technology could not solve many of the issues around data sharing ethics: '[U]ltimately the choice about what to release, how to obscure the data, and to whom to release the data, are *policy decisions*' (p. 136, original emphasis).

Network measurement and network data sharing papers were not alone in signalling issues in need of repair and arguing that the community needed to anticipate emerging ethical challenges in their research. Allman and Paxson presented their paper on 'Issues and Etiquette' at the 2007 Internet Measurement Conference. In the same session, legal scholar Paul Ohm presented a paper he co-authored with two University of Colorado computer scientists, Doug Sickler and Dirk Grunwald, which examined how US legislation applied to network measurement researchers. It explained how legal issues went beyond data sharing norms to the legality of data collection itself, citing the Federal Wiretap Act and the Pen Register and Track and Trace Act and suggesting that computer

scientists were engaged in illegal activities. The authors offered suggestions to improve the likelihood of following the law, concluding that:

At the very least, we should proceed informally, by beginning to have conversations about what constitutes acceptable network monitoring. A codified understanding that reflects even rough consensus would be a useful tool to bring to Congress or to show to courts. It is important that these norms and rules are agreed upon from within our community, rather than dictated to us by some outside court or agency. (Ohm et al., 2007, pp. 147–148)

Ohm was not the only law scholar concerned about the legality of data-gathering techniques for network measurement and analysis. Legal scholar Aaron Burstein (who became a co-author of the Menlo Report) gave a series of presentations in 2007 warning networking researchers that when they collected data from ISPs (or when the ISPs gave them network data) that they might be in violation of the Electronic Communications Privacy Act (Burstein, 2007). These scholars advocated for an exception in the wiretap act for researchers (Burstein, 2008a, 2008b; Ohm et al., 2007). Burstein, in his review of the various laws affecting network measurement and security research showed that ‘a fog of legal and ethical uncertainty hangs over cybersecurity research’ (Burstein, 2008b).

Computer security researchers and funders were similarly concerned about research activities in the field such as studies that involved taking over spam botnets (Kanich et al., 2008). Another network science study that generated controversy and attention from people outside of the academy recorded data from Tor, a network premised on anonymity (McCoy et al., 2008). As then-reporter (and now policy advocate) Chris Soghoian recounted, recording Tor data and retaining copies of it meant that the data could be subpoenaed, raised the question of whether data collection was regulated by university IRBs, and potentially violated international law (see Soghoian, 2008).

Menlo Report authors also reported finding themselves in program committee meetings for conferences (the primary site for publishing scholarship in these fields), reviewing papers that, as Participant 2 put it, were ‘above the bar technically but might make us a little nervous to publish with respect to the ethics of the methodology or the data collection’. Participant 2 remembered that a major conference’s technical program committee rejected a paper on ethics grounds and believed that this caused confusion for the paper’s authors. A lack of clear guidelines made it difficult to interpret whether emerging work was in line with legal and community norms.

Conference committees were not the only governance bodies struggling with ethical norms in security and network measurement research. Participant 1, a researcher, described that security or network measurement researchers would sometimes apply for ethics reviews of their research by university IRBs, but too often received unhelpful guidance, or had their projects dismissed as outside of IRB purview. Lack of meaningful review from campus IRBs created challenges not only for researchers and program committees, but for funders (such as DHS) that traditionally relied on IRBs to govern research ethics. As Participant 1 recounted, ‘My own way of describing [the Menlo Report] is, [the DHS program officer] wanting to be ahead of the curve He was trying to solve some of these problems of IRB reviews inconsistent with some of the projects that he’s funding.’ Funders anticipated that consistent protocols could

enable IRBs to help the federal government mediate and enforce ethical computing research.

Network data as human subjects data

The Menlo Report team's intuition that network and security data was data about people was the central impetus behind adapting ethical principles from the Belmont Report to security and network research. To authors such as Participant 7 the analogies were obvious:

When we began at Menlo, there was a diversity of opinions about the applicability of Belmont to network security research. There's always somebody who will stand up and say, 'Well, we're not working on humans, we're just working with bytes.' I suppose, one can say, 'Well, I'm not working on a human, I'm just working with blood samples.' I think the argument is about as strong in both cases.

This ontological move – effectively recategorizing data about computers (network data) as data with an impact on people was a significant attempt to resolve ethical uncertainties in the field. Associating network data with human subjects enabled a clear way forward for constructing guidance: adopting well-established human subjects research principles. From early meetings of the Menlo Report group, the Belmont Report became a model and a guiding template. (Even the name of the Menlo Report was an inspired by the “Belmont Report”). For U.S.-based researchers, the Belmont Report is one of the foundational documents that guides clinical and social science researchers. Though the Belmont principles were shaped for and by a very specific clinical research context (Stark, 2012), the Menlo Report authors admired the durability of the Belmont principles through decades of major changes in medical and social science research. Additionally, the fact that the report had supported regulation (both in the U.S. and internationally) meant that it was effective: It had concretely changed research practices.

The redefinition of network and security data as human data suggested not only an existing set of governing *principles*, but also a codified set of governance mechanisms: IRB review. This is an ‘ethical transplant’ in the vein of ‘legal transplants’ when law in one jurisdiction is transplanted into another jurisdiction (Sandvik, 2019). This move recruited the already-existing apparatus of Institutional Review Boards to govern network and security research. IRBs are what Stark has referred to as a ‘declarative body’: experts who are empowered to make governing decisions. As she writes, ‘IRBs are declarative bodies because they are empowered to turn a hypothetical situation (this research *may* be acceptable) into shared reality (this research *is* acceptable)’ (Stark, 2012). Such declarative ethical authority provided one solution for the field of network and security research to address its ethical uncertainties. The adaption of Belmont principles was an explicit move; the recruitment of existing IRB governance mechanisms was more implicit. The Menlo Report ‘does not recommend particular enforcement mechanisms’, (Dittrich et al., 2012, p. 6) although it does explicitly name review boards as a potential and appropriate mechanism for enforcement, writing: ‘Such a framework [for ICT research] should also

support current and potential institutional mechanisms that are well served to implement it, such as a research ethics board (REB)’ (Dittrich et al., 2012, p. 5).

The relationship between Belmont principles and existing regulatory forms did not arise uncontested by any Menlo Report author. As Participant 4 relayed: ‘We had one person that disputed the whole approach saying that we were just inviting regulation.’ Participant 3 explained their objection: ‘They wanted everything to be reviewed by IRBs. ... this was going to create a huge bureaucratic structure.’ Participant 3 felt that there was already sufficient protection for network data in existing law that made adding human subjects protections burdensome and redundant. But legal scholars such as Burstein and Ohm had already suggested that existing law lacked clarity for researchers, and computer scientists such as Allman and Paxton had suggested formal guidelines to govern the discipline.

Not only was there debate as to the ontological status of computer security and network measurement data as human subjects data, the Menlo Report authors were publishing articles questioning the appropriateness of IRB reviews of network and security research (e.g. Buchanan et al., 2011; Dittrich et al., 2009, 2010, 2011; Kenneally et al., 2010). The IRB may have been governance by experts (Stark, 2012), but in the early years of this century, this rarely meant *computer science* experts. Network measurement and security researchers who had consulted their IRBs reported that the existing boards proved imperfect for resolving ethical uncertainties. As Participant 1 told us:

So, in some cases, the IRBs didn’t know the law, and researchers would do things that kind of got into the gray area, or might have actually broken a law, and the IRB had approved it. And then there were other cases where the IRBs would say, ‘Well, okay, we get the deception part, we’ll let you do that, but we’re not going to let you record any identifiable information about any of the people.’ Which means, now it becomes really hard to actually quantify and be able to come up with good research data. So there is this back and forth between IRBs specifically in these cases where social engineering is involved. How do you deal with the deception, and how do you deal with the whatever personal information needs to be collected, such that you can accomplish the research?

To IRBs, it wasn’t always clear what or who the human subjects were in computer security and network measurement research, or where the risks were.

The move to recategorize network data as human subjects data was meant to reduce uncertainty for researchers, IRBs, and conference committees, but it also produced new challenges for network measurement and security researchers. Despite early agreement that Belmont should serve as a model, Menlo participants had ongoing discussions about how heavily to rely on the earlier report. As Participant 8 described, ‘I think we probably tried too hard to mirror the structure of that [Belmont] report. Which was very specific in what it was dealing with and I think we tried to broaden it somewhat and make it more general.’ Because Belmont was conceived in the context of medical research – a decidedly different area of research from cybersecurity – the Menlo Report authors (as other research fields had before them) grappled with difficulties in how to apply the Belmont principles outside of a laboratory research model. As Participant 10, a lawyer, described:

The potential harm to subjects [of security research] is more abstract. The benefits of the research are more abstract. It seemed harder to think through some of the issues when that's the case because you don't really know how an individual might benefit from consenting to research or what impacts there might be in sort of waiving consent for monitoring network traffic or doing something like that or just relying on consent that's in the terms of service that you click through.

A particularly thorny problem produced by the reclassification of network data as human subjects data was whether IRBs would change their regulation practices to oversee more computer science research and whether IRBs had enough knowledge of computer science to understand how to regulate the research. Participant 4 told us that the Menlo Report authors had talked about follow-up work investigating IRB practices to see if and how the report was being applied, but this was never undertaken. Participant 4 suspected that few computer science studies wind up subject to IRB review, even since the Menlo Report was published.

Authors also worried that the designation of network data as human subjects data didn't capture an important form of risk: indirect harms to groups or institutions. For example, Participant 1 spoke to us about how vulnerability disclosures might be harmful, but not necessarily because of risks to human subjects:

The favourite analogy that I like to use is, cancer doesn't read the *Journal of American Medicine* and change the way that it behaves. But people doing crimes do. So, whenever you're publishing something that tries to explain how this malicious software works, how this criminal activity is occurring, [bad actors] will adjust. The risk and benefit often is not really clear, and IRB often won't understand the risk to the general public by the disclosure of something that is time critical.

Thus, while the Belmont Report and the designation of network data as human subjects data offered new stability for some of the ethical uncertainties in computing research, the invitation of IRB oversight was an imperfect solution because of the relationships between security and network researchers and 'users' were markedly different from those of medical researcher and research participant. In addition, adopting traditional research ethics understandings of risks and harms may have limited the harms researchers attended to. Recent computing governance programs have shown that the implications of computing research can go beyond individual harms, and that computing researcher sometimes poses harms to society broadly and specifically harms to people who have been marginalized (Bernstein et al., 2021; Gangadharan, 2017; Hoffmann, 2021; Li et al., 2018).

Though imperfect, the move to adopt Belmont's principles emphasizes the accountability of ICT research to the subjects of network data. However, the attempt to resolve ethical uncertainties around the status of network data also introduced new uncertainties about how to understand the status of (and risks to) human subjects in networked data. These uncertainties continue to be debated and negotiated in the field. For example, high profile ethics controversies in network measurement since Menlo have centred around researcher obligations to people who cannot be considered traditional research *subjects* but are nevertheless put at risk by network measurement research (Narayanan & Zevenbergen, 2015).

Settling controversies: Ethics and the law

A primary controversy raised by legal scholars in the years before the Menlo Report authors convened was whether some network measurement and computer security research practices were not only unethical, but illegal. To resolve controversies around legal research practices, the Menlo Report went a step farther than Belmont by adding a fourth principle of ‘respect for the law and the public interest’. The adoption of a principle which advised researchers to consider both the law and public interest reads like the compromise it was: both a cue to researchers that law might constrain their actions, and to satisfy those who felt existing law sufficiently covered security and network measurement research ethics. The inclusion of ‘public interest’ raises important questions about public benefits not protected by law, as well as about whose interests are included in ‘publics’, signaling some of the difficulties that the authors had fitting the types of societal harms that they anticipated from computing research into the types of individual harms anticipated by the Belmont Report principles. But including law and public interest in a single principle also introduces new controversies: namely that the law and public interest are not always one and the same.

Authors hoped that both ‘respect for law’ and ‘public interest’ would cue researchers to potential legal issues in their approaches and methods. As Participant 11 put it:

There are a lot of people in the community we felt were just, you know, going out and collect the data without putting a lot of thought behind what data they we're doing whether they were breaking the law, what the implications were to the users. We felt that, that was important to add as an exclusive principle.

In addition, for Menlo Report authors, ‘the law’ provided a durable expression of social norms that a researcher might adopt. As Participant 9 told us:

[Laws and public interest are a] coverable set of norms that people can assess their behavior against and that within the community of or audience that we were trying to reach it was probably thought that at least this way you can always ask – look at the law. You can ask a lawyer ‘what does this mean?’

Even though, as Ohm and Burstein had established, legal guidance for computer security research was frequently unclear, some participants, such as Participant 3, a lawyer, argued law had the advantage of being a nationally-applicable (and potentially more democratic) guide: ‘My approach was, why don't we just say you have to operate under the bounds of the law, that is something all organizations want to do and need to do and leave it at that?’ Participant 4 felt that, compared to earlier research ethics governance efforts such as the Belmont Report, ‘there was a relatively much more advanced legal infrastructure that was relevant’. That is, Menlo Report authors wanted researchers to know that existing laws in the U.S. context could provide guard rails for research. At the extreme, one Menlo Report author felt that the law, if it was followed, provided adequate guardrails for computing research and that further ethical principles were unnecessary.

Some authors we spoke with reported that the inclusion of the fourth principle was a compromise made to resolve the problem of fitting existing Belmont guidance to network

research: forcing a square peg into a round hole. As discussed above, some Menlo Report authors felt that characterizing network measurement and computer security data as human subjects data would invite burdensome new regulation when existing law and regulation was already robust enough to govern network research. Participant 1 argued: ‘There were many things that IRBs would allow that would actually put the institution at legal risk, or the researchers.’ That is, they were afraid of IRBs endorsing illegal research. We interpret the fourth principle as a compromise between the authors who thought that computer security and network measurement data should not be human subjects data and those who thought it was. The addition of that principle also further emphasized the mismatch between the norms of *Belmont* and the realities of network security research.

But the phrasing of this fourth principle also introduces one more new uncertainty for researcher to navigate: what is a researcher to do when there is a conflict between the law and public interest? In a paper for computer security researchers that predated the Menlo Report, Burstein emphasized that ‘even when the law permits a research activity, researchers may wonder whether it is ethically permissible’ (Burstein, 2008b). And David Dittrich and Michael Bailey, Menlo co-authors writing just before Menlo, described: ‘The law is in some ways a set of norms that are written to guide behavior within a society. These legal norms can codify another set of moral and ethical norms that are generally agreed upon by that society. These sets of norms are not, however, the same’ (Dittrich et al., 2009, p. 2). Participant 1 recalled: ‘Many of the meetings, they’d hit on some issue that was quite complex and was at the intersection of law and ethics, because they’re different things.’ Indeed, the Menlo Report authors were aware that the law, ethics, and the public interest could be different, yet these tensions were unresolved by the final report, leaving the challenge of navigating tensions between law and the public interest to individual researchers, conference committees, and IRBs.

Conclusion

The Menlo Report may have begun life modelled on previous constitutional moments in the governance of science and technology, particularly the Belmont Report, but the ethics work that happened during Menlo shaped distinctive content and outcomes. The work of producing the Menlo Report – ethics governance in the making – was not reasoning from first principles. Instead, it was bricolage, incorporating its own ‘ethics work’ of trying to figure out what to do. Authors relied heavily upon their expertise in law, computing research, and IRBs, and the Belmont Report itself, at that point long-established and accepted within medical and social science, to attempt to chart a way forward for the discipline. Based on our case study and our reading of STS literature, we see the bricolage ethics work of the Menlo Report as constituted by five overlapping focal points for future researchers interested in ethics self-governance efforts:

- The *resources* including the financial and logistical resources as well as the people involved, whose identity, background and expertise affect the governance outcomes and potential impacts of the report, the available resources for governance including existing networks that could be realistically recruited, and how meaningful cutting of dissenting actors can be accomplished;

- Attempts to *repair* the wrongs of the past (Jacob, 2019);
- Attempts to *anticipate* the future, and in particular, changes in technologies and practices (Brey, 2012);
- Work to *close or settle controversies* within the field (Pinch & Bijker, 1984) and *resolve ethical uncertainties* as participants tried understand what practices are acceptable (Ziewitz, 2019).
- Ethics governance efforts are *generative* in the sense that their products, on the surface a static resource for a field, generate new ethical uncertainties, controversies, and situations to repair and anticipate.

The Menlo Project engendered successes (in changes to conference requirements that predated most of computer science by a decade) as well as trade-offs and pitfalls. What the authors of the Menlo Report discovered was that they could not fully resolve the ethical challenges of security and network measurement ethics. The very process of writing the Menlo Report created new uncertainties, problems, and challenges for the research communities involved, with which both authors and the field still grapple. Authors expressed continuing uncertainty about: who should participate in ethics governance development and how the work should be done; the appropriateness of adapted Belmont research ethics guidance to network and security research; the role of IRBs in computing research; the cascade of ethics into policy and law; and how best to enroll governance networks.

The processes we observed at work during in the Menlo Report can be used as a framework not only for understanding how the development of ethics governance has proceeded in the past, but also for predicting tensions within, and perhaps improving, current and future projects that seek to bolster local ethics work with formalized governance. In the process of writing the report, the Menlo authors debated whether they should become more regime-like by enrolling – and, as Slayton (2021) terms it, ‘cutting’ – research and researchers through federal regulation, institutional oversight, or publication review committees. Instead of imagining governance solely inside of labs (as in Asilomar) or disciplines (as in early envisioning of IRBs), Menlo attempted to recruit already-established governance models: peer review processes and IRBs.

Computer science has entered an era of experimentation with ethics governance development proliferating as it attempts to grapple with the moral implications of the work done in the field. Researchers and activists are currently undertaking projects across computing to revise ethics codes, write new ethics guidelines, form new ethics committees within computer science conferences and professional associations, dictate ethics requirements for funding, and propose new ethics requirements for publication. And beyond computer science, governance of data and research practices remain challenging questions in numerous scientific fields (Hilgartner, 2018; Parthasarathy, 2015). As researchers such as Parthasarathy (2015) have pointed out, as research communities grapple with the ethics of their work and begin ethics governance projects, it becomes necessary to decide who does the work of establishing ethical guidelines and how. A framework to study ethics governance in the making can aid in the understanding and critique of these efforts.


Acknowledgements

We thank graduate students Lovely Francis Domingo and Modassir Iqbal for their help gathering information about computing conferences and their contributions to coding our interviews. Joy Rohde, Malte Ziewitz, Emanuel Moss, SIGCIS SHOT 2021 participants, and two anonymous reviewers gave us invaluable feedback on earlier drafts of the paper. We are grateful for the community of Ethics and Responsible Research (ER2) researchers and Mols Sauter and David Tomblin, who provided input on project framing.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: NSF #1634202 and NSF #2226200.

ORCID iD

Megan Finn  <https://orcid.org/0000-0002-8177-7430>

Note

1. This program has since been given a name that makes its data sharing goals more explicit: IMPACT (Information Marketplace for Policy and Analysis of Cyber-risk & Trust).

References

- 22nd USENIX Security Symposium. (2012). *Announcement and call for papers*. USENIX: The Advanced Computing Association. https://www.usenix.org/sites/default/files/sec13cfp_111912.pdf
- Adey, P., & Anderson, B. (2012). Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue*, 43(2), 99–117.
- Allman, M., & Paxson, V. (2007). *Issues and etiquette concerning use of shared measurement data* [Conference session]. Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement (pp. 135–40). ACM.
- AMC IMC. (2009). *Internet measurement conference 2009*. Internet Measurement Conference 2009, Call for Papers. <https://conferences.sigcomm.org/imc/2009/cfp.html>
- AMC IMC. (2019). Call For Papers, ACM IMC 2019, *Amsterdam, Netherlands*. Internet Measurement Conference 2019. <https://conferences.sigcomm.org/imc/2019/cfp/>
- Ames, M. G. (2019). *The charisma machine: The life, death, and legacy of one laptop per child*. MIT Press. <http://direct.mit.edu/books/book/4918/The-Charisma-MachineThe-Life-Death-and-Legacy-of>
- Ananny, M., & Finn, M. (2020). Anticipatory news infrastructures: Seeing journalism's expectations of future publics in its sociotechnical systems. *New Media & Society*, 22(9), 1600–1618. <https://doi.org/10.1177/1461444820914873>
- Berg, P. (2008). Meetings that changed the world: Asilomar 1975: DNA modification secured. *Nature*, 455(7211), 290–291.
- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity.
- Bernstein, M. S., Levi, M., Magnus, D., Rajala, B. A., Satz, D., & Waeiss, C. (2021). Ethics and society review: Ethics reflection as a precondition to research funding. *Proceedings of the National Academy of Sciences*, 118(52), e2117261118.
- Brey, P. A. E. (2012). Anticipatory ethics for emerging technologies. *NanoEthics*, 6(1), 1–13.

- Buchanan, E., Aycock, J., Dexter, S., Dittrich, D., & Hvizdak, E. (2011). computer science security research and human subjects: Emerging considerations for research ethics boards. *Journal of Empirical Research on Human Research Ethics*, 6(2), 71–83.
- Burnett, S., & Feamster, N. (2015). Encore: Lightweight measurement of web censorship with cross-origin requests. In *ACM SIGCOMM computer communication review* (Vol. 45, pp. 653–667). ACM.
- Burstein, Aaron J. “Toward a Culture of Cybersecurity Research.” Presented at the TRUST (Team for Research in Ubiquitous Secure Technology), August 10, 2007. <https://doi.org/10.2139/ssrn.1113014>.
- Burstein, A. J. (2008a). Amending the ECPA to enable a culture of cybersecurity research. *Harvard Journal of Law & Technology*, 22(1), 167–222.
- Burstein, A. J. (2008b). *Conducting cybersecurity research legally and ethically*. In Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, 8:1-8:8. LEET’08. USENIX Association. <http://dl.acm.org/citation.cfm?id=1387709.1387717>.
- Campos, L. (2010). That was the synthetic biology that was. In M. Schmidt, K. Alexander, A. Ganguli-Mitra, & H. Vriend (Eds.), *Synthetic biology: The technoscience and its societal consequences* (pp. 5–21). Springer.
- Childress, J. F., Meslin, E. M., & Shapiro, H. T. (2005). *Belmont revisited: Ethical principles for research with human subjects*. Georgetown University Press.
- Coull, S., Wright, C., Monrose, F., Collins, M., & Reiter, M. (2007). *Playing devil’s advocate: Inferring sensitive information from anonymized network traces* [Symposium]. *Proceedings of the Network and Distributed System Security Symposium*, NDSS 2007, San Diego, CA, USA. Department of Homeland Security. (2013, June 3). *Information Marketplace for Policy and Analysis of Cyber-risk & Trust* [Archived]. Department of Homeland Security. <https://www.dhs.gov/science-and-technology/cybersecurity-impact>
- Denning, D. E., Neumann, P. G., & Parker, D. B. (1987). *Social aspects of computer security* [Conference session]. Proceedings of the 10th National Computer Security Conference (Vol. 335).
- Dittrich, D., Bailey, M., & Dietrich, S. (2011). Building an active computer security ethics community. *IEEE Security Privacy*, 9(4), 32–40.
- Dittrich, D., Kenneally, E. E., Bailey, M., Burstein, A. J., Claffy, K. C., Clayman, S., Heidemann, J., Maughan, D., McNeill, J., Neumann, P., Scheper, C., Papadopoulos, C., Visscher, W., & Westby, J. (2013). *Applying ethical principles to information and communication technology research: A companion to the department of homeland security Menlo Report*. Department of Homeland Security: Science and Technology Directorate.
- Dittrich, D., Kenneally, E. E., Michael, B., Burstein, A. J., Claffy, K. C., Clayman, S., & Heidemann, J. (2012). *The Menlo Report: Ethical principles guiding information and communication technology research*. Department of Homeland Security: Science and Technology Directorate.
- Dittrich, D., Leder, F., & Werner, T. (2010). A case study in ethical decision making regarding remote mitigation of botnets. In R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, & F. Seb  (Eds.), *Financial cryptography and data security* (pp. 216–230). Springer.
- Dittrich, D., Michael, B., & Dietrich, S. (2009). *Towards community standards for ethical behavior in computer security research* (Stevens CS Technical Report).
- Fassin, D. (2014). The ethical turn in anthropology: Promises and uncertainties. *Hau Journal of Ethnographic Theory*, 4(1), 429–435.
- Fitzgerald, M. H. (2005). Punctuated equilibrium, moral panics and the ethics review process. *Journal of Academic Ethics*, 2(4), 315–338.

- Gangadharan, S. P. (2017). The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users. *New Media & Society*, 19(4), 597–615.
- Greene, D., Hoffmann, A. L., & Stark, L. (2019). *Better, nicer, clearer, fairer: A critical assessment of the movement for ethical artificial intelligence and machine learning* [Conference session]. Proceedings of the 52nd Hawaii International Conference on System Sciences. <https://doi.org/10/ggd378>.
- Guston, D. H. (2014). Understanding 'anticipatory governance'. *Social Studies of Science*, 44(2), 218–242.
- Haimes, E. (2002). What can the social sciences contribute to the study of ethics? Theoretical, empirical and substantive considerations. *Bioethics*, 16(2), 89–113.
- Hedgecoe, A. (2017). Scandals, ethics, and regulatory change in biomedical research. *Science Technology & Human Values*, 42(4), 577–599.
- Heeney, C. (2017). An 'ethical moment' in data sharing. *Science Technology & Human Values*, 42(1), 3–28.
- Hilgartner, S., Prainsack, B., & Benjamin, J. (2016a). Chapter 28: Ethics as governance in genomics and beyond by Stephen Hilgartner. In B. Prainsack, J. Benjamin Hurlbut, F. Ulrike, F. Rayvon, C. Miller, & L. Smith-Doerr (Eds.), *The handbook of science and technology studies* (4th ed, pp. 825–851). MIT Press.
- Hilgartner, S., Prainsack, B., & Benjamin Hurlbut, J. (2016b). Ethics as governance in genomics and beyond. In F. Ulrike, F. Rayvon, C. A. Miller, & L. Smith-Doerr (Eds.), *The handbook of science and technology studies* (4th ed., pp. 823–852). The MIT Press.
- Hilgartner, S. (2019). Governing gene editing: A constitutional conversation. In I. R. U. S. Braverman (Ed.), *Gene Editing, Law, and the Environment: Life beyond the Human* (1st ed., pp. 187–193). Routledge.
- Hilgartner, S. (2018). The human genome project and the legacy of its ethics programs. In S. Gibbon, B. Prainsack, S. Hilgartner, & J. Lamoreaux (Eds.), *Routledge handbook of genomics, health and society* (pp. 123–132). Routledge.
- Hoffmann, A. L. (2019). Where fairness fails: Data, algorithms, and the limits of antidiscrimination discourse. *Information Communication & Society*, 22(7), 900–915.
- Hoffmann, A. L. (2021). Terms of inclusion: Data, discourse, violence. *New Media & Society*, 23, 3539–3556.
- Hurlburt, B. (2015). Remembering the future: Science, law, and the legacy of asilomar. In S. Jasanoff & K. Sang-Hyun (Eds.), *Deamsapes of modernity: sociotechnical imaginaries and the fabrication of power* (pp. 126–155). University of Chicago Press.
- Jacob, M. A. (2019). Under repair: A publication ethics and research record in the making. *Social Studies of Science*, 49(1), 77–101.
- Jasanoff, S. (2003). In a constitutional moment: Science and social order at the millennium. In J. Bernward & H. Nowotny (Eds.), *Social studies of science and technology: Looking back, ahead*. Sociology of the Sciences (pp. 155–180). Springer.
- Jasanoff, S. (2012). Genealogies of STS. *Social Studies of Science*, 42(3), 435–441.
- Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G. M., Paxson, V., & Savage, S. (2008). *Spamalytics: An empirical analysis of spam marketing conversion* [Conference session]. Proceedings of the 15th ACM Conference on Computer and Communications Security (pp. 3–14). ACM. <http://dl.acm.org/citation.cfm?id=1455774>.
- Kaplan, S., & Radin, J. (2011). Bounding an emerging technology: Para-scientific media and the Drexler-Smalley debate about nanotechnology. *Social Studies of Science*, 41(4), 457–485.
- 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). Springer.

- Li, X., Chen, W., & Straubhaar, J. D. (2018). Privacy at the margins| concerns, skills, and activities: Multilayered privacy issues in disadvantaged urban communities. *International Journal of Communication*, 12(0), 22.
- MacKenzie, D. (2003). An equation and its worlds. *Social Studies of Science*, 33(6), 831–868.
- MacKenzie, D., & Pablo Pardo-Guerra, J. (2014). Insurgent capitalism: Island, bricolage and the re-making of finance. *Economy and Society*, 43(2), 153–182.
- McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008). *Shining light in dark places: Understanding the tor network* [Symposium]. International Symposium on Privacy Enhancing Technologies Symposium (pp. 63–76). Springer.
- Narayanan, A., & Zevenbergen, B. (2015). *No encore for encore? Ethical questions for web-based censorship measurement*. Princeton University. <http://bdes.datasociety.net/wp-content/uploads/2015/09/Encore-Case-Study.pdf>
- National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (2010). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. Department of Health, Education, and Welfare. <http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html>
- Ohm, P., Sicker, D. C., & Grunwald, D. (2007). *Legal issues surrounding monitoring during network research* [Conference session]. Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement (pp. 141–48). ACM.
- Passive & Active Measurement Conference. (2021, October 15). *PAM2022—Call for Papers*. PAM2022 - Call for Papers. <https://pam2022.nl/cfp/>
- Pang, R., Allman, M., Paxson, V., & Lee, J. (2006). The devil and packet trace anonymization. *ACM SIGCOMM Computer Communication Review*, 36(1), 29–38.
- Parthasarathy, S. (2015). Governance lessons for CRISPR/Cas9 from the missed opportunities of Asilomar. *Ethics in Biology Engineering and Medicine: An International Journal*, 6(3–4), 305–312. <https://doi.org/10.1615/ethicsbiologyengmed.2016016470>
- Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, 14(3), 399–441.
- Response to Comments Received for the “The Menlo Report: Ethical Principles Guiding Information), Science and Technology, Cyber Security Division (CSD), Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT) Project,” 77 FR 73669 (December and Communication Technology Research” (“The Menlo Report”) for the Department of Homeland Security (DHS 11, 2012). <https://www.federalregister.gov/d/2012-29818>
- Rosner, D. K. (2014). Making citizens, reassembling devices: On gender and the development of contemporary public sites of repair in Northern California. *Public Culture*, 26(1), 51–77.
- Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>
- Sandvik, K. B. (2019). Is legal technology a new ‘moment’ in the law and development trajectory? *Antipode*, Advance online publication.
- Sharma, A. X. (2021). *Linux bans university of minnesota for committing malicious code*. Bleeping Computer. Retrieved April 21, 2021, from <https://www.bleepingcomputer.com/news/security/linux-bans-university-of-minnesota-for-committing-malicious-code/>.
- Shilton, K. (2015). Anticipatory ethics for a future Internet: Analyzing values during the design of an Internet infrastructure. *Science and Engineering Ethics*, 21(1), 1–18. <https://doi.org/10.1007/s11948-013-9510-z>

- Shilton, K., Moss, E., Gilbert, S. A., Bietz, M. J., Fiesler, C., Metcalf, J., Vitak, J., & Zimmer, M. (2021). Excavating awareness and power in data science: A manifesto for trustworthy pervasive data research. *Big Data & Society*, 8(2), 20539517211040760. <https://doi.org/10.1177/20539517211040759>
- Slayton, R. (2021). Governing uncertainty or uncertain governance? Information security and the challenge of cutting ties. *Science Technology & Human Values*, 46(1), 81–111.
- Soghoian, C. (2008). *Researchers could face legal risks for network snooping*. CNET. Retrieved July 24, 2008, from <https://www.cnet.com/news/researchers-could-face-legal-risks-for-network-snooping/>.
- Spafford, E. H. (1989). Crisis and aftermath. *Communications of the ACM*, 32(6), 678–687.
- Spafford, E. H. (2003). *A failure to learn from the past* [Conference session]. Proceedings of 19th Annual Computer Security Applications Conference. (pp. 217–31). IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1254327.
- Spafford, E. H. (1991). *Computer viruses and ethics*. <http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1900&context=cstech>.
- Spafford, E. H. (1997). Are hacker break-ins ethical. In M. D. Ermann, M. B. Williams, & M. S. Shauf (Eds.), *Computers, ethics, and society* (2nd Edition, pp. 77–88). Oxford University Press.
- Stark, L. (2012). *Behind closed doors: IRBs and the making of ethical research* (1st ed.). University of Chicago Press.
- Submission for Review and Comment: “‘The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research’” (“Menlo Report”) for the Department of Homeland Security (DHS), Science and Technology, Cyber Security Division (CSD), Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT).” *Federal Register* 76 F.R. 81517 (December 27, 2011). <https://www.regulations.gov/document/DHS-2011-0074-0001>.
- Steinhardt, S., & Jackson, S. (2015). *Anticipation work: Cultivating vision in collective practice* (pp. 443–453). ACM Press. <https://doi.org/10.1145/2675133.2675298>.
- Ziewitz, M. (2019). Rethinking gaming: The ethical work of optimization in web search engines. *Social Studies of Science*, 49(5), 707–731.

Author biographies

Megan Finn is an associate professor at the Information School at University of Washington where she teaches about information policy and ethics and researches disaster informatics and data governance. She is the author of *Documenting Aftermath: Information Infrastructures after Disasters* (MIT Press).

Katie Shilton is an associate professor in the College of Information Studies at the University of Maryland, College Park. Her research uses science and technology studies, human-computer interaction, and information studies perspectives to explore technology and data ethics, and can be found at <https://terpconnect.umd.edu/~kshilton/>.