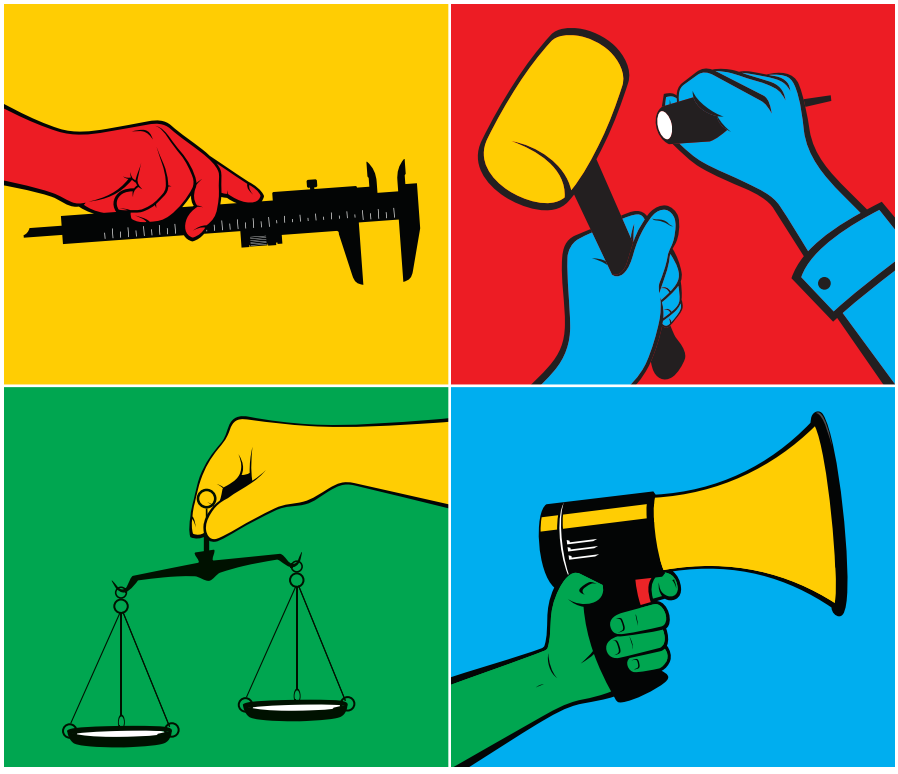
DOI:10.1145/3486639

Katie Shilton, Megan Finn, and Quinn DuPont

▸ **Susan J. Winter,** Column Editor

Computing Ethics
Shaping Ethical Computing Cultures

Lessons from the recent past.



IMAGERY BY JAMESBIN

Public concern about computer ethics and worry about the social impacts of computing has fomented the "techlash." Newspaper headlines describe company data scandals and breaches; the ways that communication platforms promote social division and radicalization; government surveillance using systems developed by private industry; machine learning algorithms that reify entrenched racism, sexism, cisnormativity, ablism, and homophobia; and mounting concerns about the environmental impact of computing resources. How can we *change* the field of computing so that ethics is as central a concern as growth, efficiency, and innovation? There is no one intervention to change an entire field: instead, broad change will take a combination of guidelines, governance, and advocacy. None is easy and each raises complex questions, but each approach represents a tool for building an ethical culture of computing.

To envision a culture of computing with ethics as a central concern, we start with the recent past, and a subdiscipline—computer security research—that has grappled with ethics concerns for decades. The 2012 *Menlo Report*[3] established guidelines for responsible research in network and computer security. After *Menlo*, new requirements for ethics statements in computer security and network measurement conferences illustrate the use of governance for centering ethics in computing. Historically, a volunteer organization, Computer Professionals for Social Responsibility (CPSR), engaged in advocacy beginning in the 1980s to shape a more ethical future of computing, and influenced many of today's leading Internet watchdog and activist groups.[4]

Each of these efforts represents a different way of doing ethics beyond the scale of individual decision making, and each can be adapted in areas such as data science, social media, IoT, and AI. But as shown in Table 1, these cases also illustrate the difficult questions, trade-offs, and compromises required for culture change, and the challenges of work left to be done. Moving beyond the reactive "techlash," tech workers and computing researchers interested in systemic ethical change can be inspired by these efforts while appreciating the trade-offs and understanding the

uphill nature of organized, sustained, and collective ethics work at scale. To illustrate each method, three examples are described in Table 1.

Setting Research Guidelines: *The Menlo Report*

Recent calls for codes of ethics for data science and social media research echo similar concerns that roiled computer security research in the 2000s. In response, the U.S. Department of Homeland Security (DHS) organized funded researchers and invited legal experts to collaboratively develop guidelines for ethical network security research. Our interviews with 12 of the 15 primary *Menlo Report* authors found the effort made smart use of existing resources, including funding for a related research program and existing ethical guidelines from other domains. But the authors faced at least two difficult challenges. First, *who* should set ethical guidelines for a field? Because the Menlo work was involved and long-term, it largely fell to a group already funded under a DHS network security program. Second, *how* does a volunteer group set guidelines that people know about, ascribe to, and follow? The *Menlo Report* did not produce large-scale regulatory changes and authors we spoke with lamented the lack of resources for long-term education and training to support and evaluate the Report's impact.

The limited reach of *Menlo* is demonstrated in persistent computer security research controversies. Recently, cybersecurity researchers at the University of Minnesota caused an uproar with research that exposed vulnerabilities in the socio-technical system for approving Linux patches. Though their aim was to study Linux contributors' ability to detect security vulnerabilities, they believed their research did not involve human subjects (a judgment with which their Institutional Review Board agreed). The Linux community, however, reacted with anger reminiscent of the fallout from the famous Sokal Hoax, calling the work a "bad faith" violation of the community's trust.[8] This case illustrated exactly the kinds of uncertainty at the intersection of humans and systems that *Menlo* was written to address. Following *Menlo* guidance might have helped the researchers craft a clearer statement of their ethical deliberations and decisions, and might have helped the IRB identify the human stakeholders at the center of the research. As this example illustrates, expanding the reach of guidelines like the *Menlo Report* is a formidable challenge.

Recent calls for codes of ethics for data science and social media research echo similar concerns that roiled computer security research in the 2000s.

Research Governance: Conference Ethics Statements

Another model computer security researchers are using to create more effective organized, sustained, and collective action is to build ethical guidelines into gatekeeping processes. Conference peer review can help govern research ethics by only publishing work that meets a higher standard, effectively defining ethical reflection as a necessary part of security research processes. To encourage researcher reflection and compliance, many of the top computer security and network measurement conferences now require an explicit declaration of ethical considerations. In 2012, USENIX, one of the top conferences in computer security, included a requirement in their Call for Papers that researchers "disclose whether an ethics review ... was conducted and discuss steps taken to ensure that participants were treated ethically." Other important security and network measurement conferences soon followed.[a] After instituting these requirements, more conference papers now discuss ethical research practices.

But post hoc reflection and conference reviewing alone does not ensure ethical research—this governance takes place after the work is done. In a recent survey of computer security re-

a Network and Distributed System Security Symposium (NDSS), IEEE Symposium on Security and Privacy (Oakland), the ACM Conference on Computer and Communications Security (CCS), and the Conference for the Special Interest Group on Security, Audit and Control.

Table 1. The work and challenges of ethical change methods at scale.

	Guidelines: Menlo Report	**Governance:** Security conference ethics statements	**Advocacy:** CPSR
Ethics Work	▸ Adopting principles and norms	▸ Reflection, rethinking and changing research design, writing	▸ Co-education, writing, publishing in popular press
Hard Questions	▸ Who sets the principles and norms (and what expertise is needed?) ▸ How to make people notice and follow guidelines without enforcement mechanisms?	▸ Who educates researchers? ▸ Do discussions of ethics in scholarly papers enhance ethical research? ▸ How to incorporate voices of stakeholders underrepresented among researchers?	▸ How to get people involved despite professional risks? ▸ How to keep volunteer efforts focused on achieving similar goals? ▸ How can computer professionals act responsibly?

searchers we conducted, a majority of respondents remain concerned about ethical practices in their community. Many computer security researchers engage legal experts, but lawyers are not well-positioned to help researchers work through ethical conundrums and what is legal is not always ethical. Instead, we found most computer security researchers learn about ethical research through interpersonal sources, such as graduate supervisors and university colleagues, so frequent and respectful discussions of ethics among colleagues are important.[2] In many computer security research labs these discussions are ongoing, but more need to take place.

Narrow perspectives are another important issue facing research governance. Though members of marginalized communities are frequently unfairly impacted by technical systems, they are too often underrepresented on program committees and guideline-setting bodies. Consequently, narrow perspectives restrict the frameworks, methods, and remediations that researchers consider in both developing systems and in designing governance instruments like conference policies. In addition to broadening participation in computing, classroom education can help introduce disparate technological impacts and train future computer researchers to "attune"[1] their work to issues of power, exclusion, and inclusion. Collectively, tech workers and computing researchers can change the culture of computer science by developing policies that both empower and are informed by people who are marginalized in technology research and development.

Advocating for Limits: Computer Professionals for Social Responsibility

Building a sustainable advocacy organization is a third model for collective action. Computer Professionals for Social Responsibility (CPSR) was an early exemplar. CPSR started in 1981 as a listserv at Xerox PARC, incorporated as a non-profit in 1983, and soon grew in size and influence, with chapters across the U.S. Fear of nuclear annihilation was the original motivating factor, but the organization also advocated for broad ethical changes in tech research and practice, including prioritizing privacy, participatory design, and community networking.[4] During the Cold War, CPSR drew upon the technical expertise of its members to argue for limiting when and how computing could be used in war. CPSR members studied military technology research agendas, educated each other, and—mobilizing their expertise—publicly critiqued plans for computerized nuclear weapons. They argued that the government and military exaggerated the power of computers and identified limits to the reliability of weaponry software that could not be tested in realistic situations. To spread this message and create policy change, CPSR members distributed flyers at computing conferences, hosted meetings and speakers, studied policies and plans, gave interviews, and published analysis in their newsletters, bulletin boards, email, reports, academic papers, books, traveling slideshows, trade and local press, and the national media.

Each of these models for doing ethics at scale has opportunities and limitations.

CPSR built a broad coalition of experts who leveraged their status to convince the public about the limits of computing technology for nuclear war. By arguing against using computers for nuclear war, CPSR members took risks that put them outside the mainstream of their field, potentially jeopardizing job opportunities and research funding. And the work of running a nonprofit was challenging: there were always financial worries, challenges attracting and managing volunteer members, and concern about keeping the organization focused on core values. Tech workers and computing researchers can change the culture of computer science through advocacy but must be willing to take personal and organizational risks.

Ethics Work Going Forward

Responding to computing industry crises of ethics, tech workers and researchers are uniting to develop new guidelines for responsible computing, new forms of governance, and new advocacy groups. Each has advantages and challenges, as shown in Table 2.

Computing researchers and professionals concerned with reforming their industry should join in:

- Crafting and deploying *guidelines* such as ACM's updated computing code of ethics (see https://bit.

Table 2. Advantages and challenges.

	 Guidelines	 Governance	 Advocacy
Advantages	▸ Can bootstrap from existing resources ▸ Can be tailored to technical work	▸ Influential because enforceable ▸ Can translate best practices to regulation	▸ Can be influential and satisfying ▸ Democratic, bottom-up motivations
Challenges	▸ Expensive in time and effort ▸ Reflect the concerns of those in the room ▸ If voluntary, can be ignored	▸ Hard to assess real vs. bureaucratic change ▸ May not account for a diverse range of experiences	▸ Expensive in effort and resources ▸ Outcomes can be hard to assess ▸ Professionally risky

The work of doing computer ethics is crucial, but it is never complete.

ly/2XtN4Kq) and IEEE's recommendations for ethically aligned design (see https://bit.ly/3tEMDbU);

- Supporting *governance* through environmental, social, and governance (ESG) criteria, hiring of Chief Ethics Officers,[5] and new developing new approaches to support ethical behavior;
- Pairing *governance* and *advocacy* (for example, unionizing tech workers and researchers to influence corporations and universities);
- *Advocating* for the computing profession by hiring and supporting Black, Indigenous, and people of color in the profession, and engaging in antiracist projects;
- Establishing *governance* through new credentialing requirements in the field, such as certifications in computing, information or data ethics;
- Using design *guidelines* (for example, participatory design in UX and FACT guidelines in machine learning) that incorporate input from minoritized publics and increase transparency and accountability;
- Engaging in *advocacy* that helps the public understand the limits of computing (for example, campaigns that have resulted in restrictions of the use of AI in public spaces by government agencies and private companies;[6] and
- Establishing *governance* by encouraging publication venues to require explicit reflection on ethics.

As earlier models from computer security indicate, each of these models for doing ethics at scale has opportunities and limitations. And we add one last lesson from our research into ethics in computer security: these efforts depend on sustained work on Sisyphean tasks. In studying these cases we spoke with dozens of participants; none felt that their work was complete. Many had regrets and worried that they had "dropped the ball" at some point or that their task was overwhelming. Cultural change for ethics and responsibility is slow, non-linear, and requires multiple—sometimes even competing—tactics. We worry that ethics efforts will slow as new guidelines fail to influence everyone, as new modes of governance controversially exclude some forms of innovation or overlook stakeholder groups, and advocacy groups struggle to raise funds or stay relevant as the news cycle turns.

Conclusion

We end with a plea to persevere through the imperfectness (and sheer difficulty) of ethics work. The work of doing computer ethics is crucial, but it is never complete. Researchers and professionals—we drew our examples from CPSR members, *Menlo* participants, and conference review committees—have engaged in change despite knowing its limitations. We hope more will follow their examples. C

References

1. Amrute, S. Of techno-ethics and techno-effects. *Feminist Review 123*, 1 (2019), 56–73.
2. Bruckman, A. "Have you thought about . . .": Talking about ethical implications of research. *Commun. ACM 63*, 9 (Sept. 2020), 8–40.
3. Dittrich, D. and Kenneally, E. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research.* Department of Homeland Security, 2012.
4. Finn, M. and DuPont, Q. From closed world discourse to digital utopianism: The changing face of responsible computing at Computer Professionals for Social Responsibility (1981–1992). *Internet Histories 4*, 1 (2020), 6–31.
5. Metcalf, J. et al. Owning ethics: Corporate logics, Silicon Valley, and the institutionalization of ethics. *Social Research: An International Quarterly 86*, 2 (2019), 449–476.
6. Metz, R. Portland passes broadest facial recognition ban in the US. CNN. (2020); https://cnn.it/3zakCKG
7. Sharma, A. Linux bans University of Minnesota for committing malicious code. *BleepingComputer* (2021); https://bit.ly/3tHFoQD
8. Wikipedia contributors. 2021. Sokal affair. Wikipedia, *The Free Encyclopedia*; https://bit.ly/3EiFy5F

Katie Shilton (kshilton@umd.edu) is an associate professor at the University of Maryland, College of Information Studies (iSchool), College Park, MD, USA.

Megan Finn (megfinn@uw.edu) is a Fellow in the Center for Advanced Study in the Behavioral Sciences at Stanford University Palo Alto, CA, USA, and an associate professor, Information School, at the University of Washington Seattle, WA, USA.

Quinn DuPont (quinn.dupont@ucd.ie) is an assistant professor in the School of Business at the University College Dublin, Dublin, Ireland.