Power in Computer Security and Privacy
A Critical Lens

Elissa M. Redmiles | Max Planck Institute for Software Systems
Mia M. Bennett and Tadayoshi Kohno | University of Washington

Critical theory is an approach to research focused on acknowledging and dismantling power structures. In this piece, we illustrate the ways in which security and privacy research already takes a critical approach and offer directions for increasing the criticality of our work along new dimensions.

In security and privacy, there has long existed an inherent power dynamic between the protectors (experts, governments, and corporations) and the protected (nonexpert individuals). Recently, security and privacy researchers have demonstrated increased awareness of the role of power and power structures. They also show growing recognition of the value (and necessity) of centering those with less power when evaluating the computer security and privacy properties of existing systems and when designing and implementing new systems. Whether these researchers know it or not, they are beginning to embed critical theory[10] into computer security and privacy research. Such work is important both because security systems are often promoted to make digital worlds safer for all, even though they risk reproducing existing systems of social and economic oppression, and because digital technologies are proliferating across society. Identifying and exposing the power dynamics embedded within security and privacy can help create the conditions for more just technologies.

Digital Object Identifier 10.1109/MSEC.2023.3238591
Date of current version: 15 March 2023

In this article, we provide a perspective on the application of critical theory to computer security and privacy research from the perspectives of two practitioners of computer security and privacy research and a human geographer, all of whom have used critical approaches within their fields. First, we consider what it means to pursue critical research. Second, we discuss how critical theory is already embedded in emerging security and privacy research, even if researchers don't explicitly draw the connection. Third, we discuss the value and benefits—and, we argue, essentiality—of integrating a critical approach into research in our field. Here, we also step back to draw lessons from observations about another field's growing embrace, since the 1960s, of critical approaches: human geography. We conclude by detailing lessons learned from critical theory research across disciplines and concretize what a critical practice of technical security would look like for researchers and practitioners alike.

Before elaborating, we briefly note our positionalities. Two of us (Elissa Redmiles and Tadayoshi Kohno) are computer security researchers, and one of us (Mia Bennett) is a political geographer focused on remote sensing. We have all engaged with critical theory and critical practice in our research but are not critical theorists. We aim to work with both theorists and practitioners in our respective fields to not only reveal and challenge hidden power structures within sociotechnical systems but transform them, too.

A Security and Privacy Perspective on Critical Theory

Across fields, critical theory seeks to identify power structures and set the stage for their dismantlement in pursuit of a more just and equitable society. Thus, critical theory influences research and has the potential to change society, too. Critical theorists generally go beyond examining an object of analysis in isolation—e.g., a specific group of people, a cryptographic protocol, or a security system—and, instead, carry out a holistic analysis of that subject within broader social, political, economic, and historical contexts. Moreover, critical theory tends to view social problems as rooted in structures rather than individuals. Therefore, the presumption is that unless there

 Copublished by the IEEE Computer and Reliability Societies

are intentional and explicit efforts to dismantle existing power structures, systems will, by default, reproduce them. Seen in this light, then, threats to security and privacy emerge not just from individual hackers but from how technical systems are designed along current dimensions of power (e.g., they allow those with more time, skills, and resources to engage in protective behavior).

Critical theory approaches—and related approaches, such as those based on feminist theories[19]—to computer security have been previously advocated.[8,9] These prior works, largely from outside the security and privacy community, suggest that while critical approaches for research in many fields identify relevant systems of power, such as race, class, and gender, in computer security research, it is crucial to also consider the state, the economy, and our own specialized expertise.

Due to their recognized expertise and membership in powerful institutions, computer security researchers and practitioners have the capacity to influence and shape security systems and access sensitive data, which may be inaccessible to others. Therefore, as researchers and practitioners occupying positions of relative power taking a critical approach, we must question the impacts of security systems and security work with less-empowered communities. Beyond that, we must reflect upon our own positionality (contextualizing ourselves in relation to other stakeholders) by questioning, "Whose times, whose cultures, whose spaces are implicated in constructing cybersecurity?"[8] and consider that "the crucial determinant in deciding what constitutes a security issue is the intellectually prior selection of whose security we are talking about and, crucially, who benefits, and who loses out, from particular acts of securitization."[8] In other words, we must consider how the epistemologies (i.e., ways of knowing) and interests of those in power—which often includes ourselves—impact our choices in research, design, and deployment (e.g., choices to design a particular protocol, implement or red team a particular system, and call upon a set of users to engage in a particular behavior).

A few examples illustrate how consideration of wider power structures and continuous challenging of our own assumptions around power structures, such as class, gender, race, and disability, might result in different cybersecurity systems. For example, drawing on our own works, in the design of electronic monitoring technologies, we must consider the relationship between law enforcement and people under probation and parole;[15] in the design of satellites and remote sensing applications, we must consider the effects of exposing individuals and groups who might not wish to be seen;[2] in the design of family safety technologies, we must consider the relationship between the parent and the child;[6] in the design of technologies for sex workers, we must consider the relationship between workers, clients, and platform policy.[14]

Emerging Critical Approaches in Security and Privacy

Although the security community has long acknowledged the role of the user in the design of computer security systems, e.g., Saltzer and Schroeder's 1975 paper in which they identified "psychological acceptability" as a key design principle in computer security systems, the modern era of human-centered security and privacy research took off in the late 1990s, following the publication of groundbreaking papers—e.g., Whitten and Tygar's "Why Johnny Can't Encrypt" and Adams and Sasse's "Users Are Not the Enemy"—highlighting the importance of centering users in the design and evaluation of security technologies.

Much of the early era of human-centered security and privacy research focused on users in the abstract and for good reason: even absent consideration of specific user groups and, from a critical perspective, power dynamics, the security research field had several lessons to learn about the interactions among security technologies, adversaries, and users.

In the mid-2000s, the human-centered security and privacy research field began to acknowledge that not all user and usage situations are equivalent. For example, in their 2006 paper finding that encrypting all e-mails was viewed as "annoying" by a sample of users, Gaw et al. argued that "understanding these social factors is necessary to guide the design of encryption technologies that can be more widely adopted."[12] While they do not take a critical approach in their research, their argument demonstrates that more security is not always the most desirable outcome. Their work also illustrates how security and privacy research can benefit from a ground-up approach and, ultimately, create systems that work for more people.

In the ensuing years, a subfield of human-centered security and privacy research focusing on at-risk, vulnerable, and marginalized populations burgeoned, as recently surveyed by Warford et al.[20] Although research in this subfield does not always explicitly make connections to critical theory, its undercurrents flow through much of this research. This body of work explores, for example, the societal and interpersonal factors that might contribute to an individual's security and privacy risks as well as the societal and interpersonal barriers that might impede access to and use of strong and sufficient security and privacy mechanisms.

Beyond this body of work, a significant portion of the broader

security and privacy research field has, as its core ideology, a belief in empowering individuals with tools (e.g., cryptographic mechanisms) that enable them to retain their fundamental rights, including their rights to privacy, autonomy, and self-governance, even against the will of those in power.[13] This ideology of user empowerment against those in power was embodied by both early computer security and privacy researchers as well as the adjacent cypherpunk community.[17] As we discuss in the following, we can draw parallels between this early focus on user empowerment and the movement in radical and, later, critical geography.

For example, one central thread throughout the history of modern computer security and privacy is the strength of cryptographic algorithms against states, with researchers advocating for strong cryptographic strength and elements of governments fighting for weaker algorithms. Early concerns included the cryptographic strength of the Data Encryption Standard (only 56 b of key material) and, continuing even today, whether governments should be able to decrypt encrypted data.[3] Another line of research has focused on preventing governments (and others in power) from denying people access to the Internet (censorship) and surveilling which people access what Internet content (anonymity). A shining example of modern anonymity and censorship resistance technology that has come from this line of work is Tor.[7]

These and other research directions are clear examples of the computer security and privacy research community's consideration of the impact of power structures on users and other stakeholders, and the importance of considering those structures and aspects of marginalization (and, alternatively, dis/empowerment) in the design, deployment, and evaluation of computing systems. In some cases, those in power may be the adversaries that computer security and privacy researchers consider (e.g., governments that can surveil and break the encryption of users). In other cases, those in power (and society at large) may create barriers for equitable access to security and privacy, as we observed in our work studying the security and privacy challenges for sex workers[14] and refugees.[18] Additional examples of power dynamics include the relationship between advertisers and users, the relationship between applications using deceptive design patterns and users, and the relationship between platforms and the researchers who wish to study them.

Thus, on the one hand, the computer security and privacy research community already embodies a critical approach. On the other hand, we believe that explicitly identifying and discussing the values and merits of critical theory can further advance our field's consideration of marginalized and vulnerable populations. In particular, while the computer security and privacy research community's focus on the marginalized, vulnerable, and underrepresented in computing populations is important, much of that work is piecemeal and scoped to commonly referenced power structures (e.g., government censorship) known to the field. By centering a critical approach to research, we argue that it will be possible to more systematically surface and then address a broader set of relevant—and important—power structures and axes of marginalization. To the degree that industry practice follows from research advances, such a structured, systematic, and critical approach to security and privacy research has the potential to greatly impact industry practices and, consequently, people and society. Thus, we call for a critical approach to security and privacy that identifies the actors, discourses, and power structures embedded within computer systems.

The Value of a Critical Approach: A Case Study of Geography

Geography—and specifically, human geography, or the study of how people make places out of space—is a discipline that has been deeply transformed by critical and radical approaches since the 1960s. At the time, the human geography field—historically one involving cartography, surveying, and area studies, often used in support of colonialism and imperialism—was experiencing a paradigm shift. The so-called quantitative revolution in geography was aided by the development of technologies, such as mainframe computers and satellites, and their use by the military and space industry. These advances were instrumental to the rise of remote sensing and geographic information systems, which equipped human geographers to develop statistical models of human behavior. Yet, even as geography became more "scientific," critiques were lobbed that the field was becoming overly positivist (believing that there is only one universal truth) and detached from not only social complexity but the social issues of the day. These critiques were all the more strident in the face of the civil rights movement, the Vietnam War, sexual liberation, and the growing popularity of Marxist theory in the United States in the early 1970s, particularly among geographers.

As more radical currents took off in human geography, scholars called for developing human geographic theory in support of "revolutionary struggle."[1,16] Over time, this "radical geography" would inspire the development of "critical geography" in the 1980s. This new turn was influenced by the ongoing rise of poststructuralism and postmodernism in Europe, which attended to language, discourse, and textual analysis.

Critical geography, which focuses on cultural and humanistic dimensions and small-*n* studies and which is

open to interpretivist epistemologies (those in which reality is plural and relative instead of singularly restricted to what can be directly observed), came to dominate Anglophone human geography in the 1990s, standing in contrast to positivist large-scale statistical modeling. The subfield's commitments to social and environmental justice have only solidified since. Indeed, in the wake of the COVID-19 pandemic and Black Lives Matter, human geography has become yet more radical and critical of hegemonic establishments, including the academy itself.

Taking Action

Provocations for Critical Security and Privacy

It is possible to apply the lessons of critical theory without needing to become a critical theorist. Here, we offer a set of critical theory-driven provocations to consider, be it in research or practice.

Consider the role of power. Consider how the goals of powerful entities (states and corporations) and your own proximity to power, based on your perceived expertise and proximity to these entities, may influence the directions your research and practice take. Ask, "Whose interests am I privileging and why?" Existing models using empirical tools to analyze the role of power structures in unequal distribution of resources and to identify the mechanisms that allow those power structures to remain may be useful when considering the role of power. Similarly, stakeholder analysis offers a set of tools for mapping all relevant actors in a system and prioritizing those actors by, e.g., levels of power and resources versus interests and alliances.

Engage in holistic analysis. Go beyond consideration of the role of individual factors to consider how societal structures interact with security at large. For instance, in addition to asking, "Which gender is most susceptible to spam?" we encourage engaging in intersectional analysis[5] to examine the social, political, economic, and historical reasons why gendered susceptibility may be observed. At times, this may require collaborating with academics, organizations, and individuals outside of security. It is important to also acknowledge that even a holistic analysis in one community (e.g., specific users of a technology in the United States) might not yield results transferrable to other communities. Additionally, as the relationships relevant to a holistic analysis change over time, they may require replication studies.

Be transparent. We encourage security and privacy researchers to explicitly include stakeholder and power analyses in their papers in an effort to bring transparency to their processes of identifying (and eventually addressing) previously unforeseen and unrecognized power structures. This can include describing the role of power in generating and procuring the data used, the power structures prioritized in the concepts of security used, and how the work may serve to empower and disenfranchise the interests of differing groups.

Critical theory advocates for a ground-up approach. In the computer security and privacy field, knowledge remains rarified to those with expertise in computational subjects. As the field currently stands, the building and implementation of secure systems is largely conducted among these experts, who are typically embedded in academic, government, and corporate institutions and government organizations. We must then ask, "What qualifies as expertise?" and, "How can we define and include experts by experience?"[11] We should also question whose security is most at stake and how we can involve them as peers in the process of defense. Even further, we must interrogate how security and privacy are defined and what forms of safety (e.g., technological versus bodily) are prioritized. This will require us to push past relying on user studies as our sole method for including nonexpert perspectives. Rather, with each research question, we can attempt to identify and include those without security knowledge—populations with lived experience of insecurity, the organizations that support them, and nonsecurity academics—directly in system creation.[4]

Balance partnership and anarchy. A tenet of critical theory is that enacting change requires dismantling powerful oppressive structures. In security and privacy, such efforts can begin by engaging with work that challenges traditional academia, government institutions, and large corporations. However, completely subverting these stakeholders may still inhibit progress; we may find our public influence weakened from avoiding collaboration with relevant powerful entities and may risk losing access to proprietary knowledge and funding. Ridding ourselves of powerful ties may ultimately weaken our ability to address large-scale complex security issues. A balance should thus be struck between uplifting people and concepts long deprioritized in security and leveraging the power of influential actors.

Question everything. At its extreme, critical theory asks us to question whether we ought to be securing something or someone at all, that is, to consider "desecuritizing" in certain cases.[9] As computer security and privacy researchers and practitioners, we are trained to question every aspect of a system's security to ensure that we have identified, and patched, all possible holes. Yet, we may be missing the biggest hole of all: whether the system should exist, whether it should be secure, and for whom. ■

Acknowledgment

We thank Joanne Armitage, Kevin Butler, Ryan Calo, Angelica Goetzen, Paula Helm, Susan Landau, and Sean Peisert for their feedback and contributions to this work. This work was supported, in part, through the U.S. National Science Foundation, under awards CNS-2206950 and CNS-2205171.

References

1. C. Akatiff, "The march on the pentagon," *Ann. Assoc. Amer. Geographers*, vol. 64, no. 1, pp. 26–33, Mar. 1974, doi: 10.1111/j.1467-8306.1974.tb00952.x.
2. M. M. Bennett, J. K. Chen, L. F. Alvarez León, and C. J. Gleason, "The politics of pixels: A review and agenda for critical remote sensing," *Progr. Hum. Geography*, vol. 46, no. 3, pp. 729–752, Jan. 2022, doi: 10.1177/03091325221074691.
3. M. Blaze, "Protocol failure in the escrowed encryption standard," in *Proc. 2nd ACM Conf. Comput. Commun. Secur.*, 1994, pp. 59–67, doi: 10.1145/191177.191193.
4. S. Costanza-Chock, *Design Justice: Community-Led Practices to Build the Worlds We Need*. Cambridge, MA, USA: MIT Press, 2020.
5. K. Crenshaw, "Mapping the margins: Intersectionality, identity politics, and violence against women of color," *Stanford Law Rev.*, vol. 43, no. 6, pp. 1241–1299, 1990, doi: 10.2307/1229039.
6. A. Czeskis et al., "Parenting from the pocket: Value tensions and technical directions for secure and private parent-teen mobile safety," in *Proc. 6th Symp. Usable Privacy Security*, 2010, pp. 1–15, doi: 10.1145/1837110.1837130.
7. R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," Naval Res. Lab., Washington, DC, USA, Tech. Rep. ADA465464, 2004.
8. A. C. Dwyer, C. Stevens, L. P. Muller, M. D. Cavelty, L. Coles-Kemp, and P. Thornton, "What can a critical cybersecurity do?" *Int. Political Sociol.*, vol. 16, no. 3, Jul. 2022, Art. no. olac013, doi: 10.1093/ips/olac013.
9. S. W. Evans, M. Leese, and D. Rychnovská, "Science, technology, security: Towards critical collaboration," *Social Stud. Sci.*, vol. 51, no. 2, pp. 189–213, Apr. 2021, doi: 10.1177/0306312720953515.
10. V. Fournier and C. Grey, "At the critical moment: Conditions and prospects for critical management studies," *Hum. Relations*, vol. 53, no. 1, pp. 7–32, Jan. 2000, doi: 10.1177/0018726700531002.
11. J. Fox, "Perspectives of experts-by-experience: An exploration of lived experience involvement in social work education," *Social Work Educ.*, vol. 41, no. 4, pp. 587–604, 2022, doi: 10.1080/02615479.2020.1861244.
12. S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: Adoption criteria in encrypted email," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, Apr. 2006, pp. 591–600, doi: 10.1145/1124772.1124862.
13. S. Levy, *Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age*. Baltimore, MD, USA: Penguin, 2001.
14. A. McDonald, C. Barwulor, M. L. Mazurek, F. Schaub, and E. M. Redmiles, "'It's stressful having all these phones': Investigating sex workers' safety goals, risks, and practices online," in *Proc. 30th USENIX Secur. Symp. (USENIX Secur.)*, 2021, pp. 375–392.
15. K. Owens, A. Alem, F. Roesner, and T. Kohno, "Electronic monitoring smartphone apps: An analysis of risks from technical, human-centered, and legal perspectives," in *Proc. 31st USENIX Secur. Symp.*, 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/owens
16. L. Peake and E. Sheppard, "The emergence of radical/critical geography within North America," *ACME, Int. J. Crit. Geographies*, vol. 13, no. 2, pp. 305–327, 2014.
17. P. Rogaway, 2015, "The moral character of cryptographic work," Cryptology ePrint Archive, https://eprint.iacr.org/2015/1162
18. L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno, "Computer security and privacy for refugees in the United States," in *Proc. IEEE Symp. Security Privacy (SP)*, 2018, pp. 409–423, doi: 10.1109/SP.2018.00023.
19. J. Slupska, "Safe at home: Towards a feminist critique of cybersecurity," *St Antony's Int. Rev.*, vol. 15, no. 1, pp. 83–100, May 2019.
20. N. Warford et al., "SoK: A framework for unifying at-risk user research," in *Proc. IEEE Symp. Security Privacy (SP)*, 2022, pp. 2344–2360, doi: 10.1109/SP46214.2022.9833643.

Elissa M. Redmiles is a research group leader at the Max Planck Institute for Software Systems, 66123 Saarland, Germany. Her research interests include security, privacy, and ethics. Redmiles received a Ph.D. in computer science from the University of Maryland. Contact her at elissaredmiles.com.

Mia M. Bennett is an assistant professor in the Department of Geography, University of Washington, Seattle, WA 98195 USA. Her research interests include cultures and practices of frontier making, from the Arctic to outer space and cyberspace. Bennett received a Ph.D. in geography from the University of California, Los Angeles. Contact her at cryopolitics.com.

Tadayoshi Kohno is a professor in the Paul G. Allen School of Computer Science and Engineering, University of Washington, Seattle, WA 98195 USA. His research interests include helping protect the security, privacy, and safety of users of current- and future-generation technologies. Kohno received a Ph.D. in computer science from the University of California, San Diego. Contact him at yoshi@cs.washington.edu.