Cryptography and Collective Power

Leah Namisa Rosenbloom

Northeastern University
l.rosenbloom@northeastern.edu

Abstract. This paper extends the dialogue of *The Moral Character of Cryptographic Work* (Rogaway, 2015) and *Crypto for the People* (Kamara, 2020) by examining the relationship between cryptography and collective power. In particular, it considers cryptography in the context of *grassroots organizing*—a process by which marginalized people build collective power toward effecting systemic change—and illustrates the ways in which cryptography has both helped and hindered organizing efforts. Based on the synthesis of dozens of qualitative studies, scholarly critiques, and historical artifacts, this work introduces a *paradigm shift* for cryptographic protocol design—general principles and recommendations for building cryptography to address the lived needs and experiences of marginalized people. Finally, it calls for *abolition cryptography*: cryptographic theories and practices which dismantle harmful systems and replace them with systems that sustain human lives and livelihoods.

1 Introduction

In *The Moral Character of Cryptographic Work*, Phillip Rogaway contrasts academic and "real-world" cryptography, arguing that the academic pursuit of cryptography as an end in and of itself (what Rogaway calls "crypto-for-crypto") has overshadowed the role of cryptography as a powerful tool with inherent political and moral dimensions [113]. Seny Kamara further critiques the centering of corporate and law enforcement-motivated research within academia in his invited talk *Crypto for the People*, asking, "Who benefits from cryptography?" and "Who's going to make crypto for the marginalized?" [73]. Both works draw on insight from history and lived experiences to open a dialogue about the ways in which cryptography research interfaces with, and largely reproduces, existing power structures. This work deepens the inquiries of Rogaway and Kamara by putting academic cryptography in conversation with *collective power*—the ability of people to come together and change their environment. In particular, it considers cryptography in the context of grassroots organizing.

Grassroots organizing is a process by which people work from within marginalized communities to build collective power and effect systemic change. The result of grassroots organizing is a grassroots movement, during which people leverage their collective bodies, voices, and resources. Because participants in grassroots movements, also called activists, use their collective power to dismantle and replace dominant power structures and hierarchies [47], they are disproportionately subject to suppression tactics such as police brutality, incarceration, disenfranchisement, assassination, prosecution, stalking, harassment, employment deprivation, surveillance, deception, and censorship [19,15,104,98,29,72,97,123].

Many scholars have studied the fraught relationship between activists and digital technologies [99,120,133,63,5,129,57,128,134,6,127,135,14,69,53,84,2,85,89] [97,60,116,46,47,86,8,33,16,31,39,48], and suggest that digital technologies both facilitate grassroots movements and create additional risk for movement participants. More specifically, digital technologies increase the "speed, scope, and scale" [115] of vital processes like direct action planning and community-building [97,129,33,97,85,135,130,129,33,100,101]. They also expose activists to additional surveillance systems of state and local adversaries [95,138,15,104,60,97], putting them at greater risk of harm. While cryptographic tools might afford grassroots movements some protection from surveillance, scholars and activists have critiqued cryptographers and privacy advocates for developing technological solutions to the problems of marginalized people that unintentionally reinforce dominant power structures and hierarchies, and which ignore the important historical and contemporary context of activists' lived experiences [52,7,73,113,139,47].

This work synthesizes and applies insights from studies at the intersection of grassroots organizing and digital technologies toward developing ways of studying, designing, and deploying cryptographic tools that facilitate collective power-building. It establishes a tangible relationship between cryptography and collective power as the theory and practice, or praxis, of *cryptography for grassroots organizing*: a new field with roots in both organizing and cryptography spaces. More broadly, it continues the conversation between Rogaway [113], Kamara [73], and many other scholars [132,137,110,49,71] who consider fundamental questions of technology production—"Why? For whom? And to what ends?"

Main Contributions and Organization. In order to be useful, the praxis of cryptography for grassroots organizing must be centered around activists' actual lived experiences, as opposed to those which are imagined by cryptographers. This work solidifies a *paradigm shift* in cryptography and privacy technology research, design, implementation, and education that focuses on the lived experiences of activists and marginalized populations in general. Section 2 expands on the specific ideas in the paradigm shift, while Section 4 foments the shift into a call toward *abolition cryptography*—cryptography with a liberatory ethos [11] designed explicitly to help grassroots movements dismantle harmful systems and replace them with systems that sustain human lives and livelihoods. To illustrate aspects of the paradigm shift with concrete examples, Section 3 provides an in-depth analysis of several diverse case studies of the role of cryptography and privacy technologies in grassroots movements.

The approach of this work is transdisciplinary: it considers the role of both digital and non-digital technologies in the context of many different disciplines, from the more traditional cryptography and digital privacy literature, to science and technology studies, to human-computer interaction (HCI) and human-centered computing (HCC), social science research, Black intersectional feminism, critical theory, abolitionist praxis, and beyond.

2 Paradigm Shift

This section solidifies a "cryptography for the people"[73]-inspired paradigm shift in cryptographic protocol design which foregrounds the lived needs and experiences of marginalized people. The first aspect of the shift is the design justice principle of *one size fits one* [32]: that protocol design should begin with the unique needs of the population the protocol is meant to serve. Second, *digital trust is human trust*—that digital trust is an extension of, and inextricably entangled with, complex human identities, collective trust relationships, and physicality. Third, the shift aims toward a notion of *big-picture security*—security that considers comprehensive threat models, not just technical components. And finally, a new evaluation metric for cryptographic protocols called *grassroots optimization*, which asks cryptographers to consider whether protocols are useful on the scale of communities, as opposed to corporations and governments.

2.1 One Size Fits One

It is standard practice in computer science to design protocols with the greatest generalization possible. Using a fully abstract model and leaving the target population otherwise unspecified implies a "normal" user who conforms to normative standards of race (White), class (wealthy), gender (cisgendered male), ability (able-bodied), etc. [32]. Counter to the universalist standard, the *one size fits one* approach grounds technology design in the specific needs of the population(s) the technology is meant to serve [32]. It demands generalization from the roots up rather from the top down—in the spirit of Fannie Lou Hamer and Black intersectional feminism, it is the "nobody's free until everybody's free" [55] approach to technology design, which positions universal accessibility in relation to all of the rich particulars [25] of diverse userbases, rather than implicitly in relation to a privileged minority [32]. This work considers one size fits one approach more broadly, not only as a design principle but as a general way of knowing, being, and relating in research, education, and community spaces.

There are several important nuances that arise in applying the one size fits one approach to cryptography for grassroots organizing, especially when cryptography designers and deployers are not members of the population(s) with whom they are designing. As Ghoshal, Mendhekar, and Bruckman note, the disproportionate concentration of technological skills among young, cisgender White men leads to their inequitable control of technology adoption and use in grassroots organizations [47]. The power dynamics inherent in the processes of technology production not only impact the manifestations of technology—explicit designs, artifacts, and processes—but human ways of knowing and being, producing a technology culture, or technoculture [106]. In order to counteract this technocultural power dynamic in grassroots organizing spaces, Ghoshal, Mendekar, and Bruckman propose a *grassroots culture of technology practice*—technology practices which are aligned with the existing cultures in grassroots organizing spaces. The following subsections highlight and discuss different aspects of *one size fits one* toward developing a grassroots culture of cryptography and privacy technology practice in particular.

Activists are Not a Monolith. Activists—like any other people who form a marginalized group—are not a monolith. This is a recognition that while activists come together to form communities and coalitions, they are individuals with diverse backgrounds, needs, and opinions. Human collectives according to Aimé Césaire form "a universal rich with all that is particular, rich with all the particulars there are, the deepening of each particular, the coexistence of them all" [25,18]. Césaire's formulation stands in opposition to neoliberal cosmopolitan universalism, which homogenizes human beings into identity categories when convenient for the maintenance of racialized capitalism and other dominant systems [4,11,140,142].

Historically and systemically, people with dominant intersections of identity have classified people with marginalized intersections of identity into groups for the purpose of preserving hierarchies that benefit them [140,142]. The same power dynamic renders dominant intersections of identity normative or invisible (for example the "normal" cis White male technology user discussed above), and therefore impervious to identity-based discrimination [12,11,140]. The "double-bind" of being folded into a homogeneous, stereotyped identity and simultaneously hypertargeted by oppressive power structures manifests widely in the design and deployment of digital technologies [11,22,102,88,66] and also in academic settings [12]. As observed by Aouragh, Gürses, Rocha, and Snelting, this trend continues into popular cryptography and digital privacy resources, which offer broad, static solutions to activists' privacy problems without meaningful engagement with the granularity, fluidity, collective values, labor structures, and cultures of grassroots movements [7].

In order to design cryptography and privacy technologies that counteract the double-bind, *one size fits one* practitioners can start by recognizing the context of widespread "research injustice" [59]—a scientific research culture which has historically exploited and tokenized individuals with marginalized intersections of identity. They can facilitate many one-on-one and group conversations, documenting with consent the self-chosen narratives [59] of each individual member of a group, slowly working with them to draw connections and synthesize communal aspirations and design goals. Simultaneously, practitioners must cultivate an awareness of the opposite effect of the double-bind—what Ruha Benjamin calls the *overserving* of people with privileged intersections of identity [12]—that often come with the terrain of technology "expertise." In practice, the rejection of overserving requires people in positions of power and with normative forms of expertise to step back, listen, recognize, and uplift forms of expertise that have been historically devalued in cryptography, computer science, and beyond.

Collaborative Development. Typical technology research, design, and development practices do not support "non-expert" collaboration or co-creation—they leave knowledge production processes to a privileged minority. Notable exceptions include work from organizations like the Algorithmic Justice League [83], Callisto [112,87], Data for Black Lives [43], the Detroit Digital Justice Coalition [30], the IDA B. WELLS Just Data Lab [81], the Distributed AI Research Institute (DAIR) [65], Our Data Bodies [13], the Technology, Race, Equity, and Ethics in Education (TREE) Lab [126], and more. Recently Kotturi, Hui, Johnson, Sanifu, and Dillahunt examined the sustainability of "community-based research in computing" that aims to build the technological capacity of local businesses in Pittsburgh, PA and Detroit, MI (U.S.), stressing the importance of trust and interpersonal relationships [80]. Kotturi et al. summarize the recommendations of human-computer interaction (HCI) researchers for building successful academic-community partnerships: "academic teams can volunteer in the community, familiarize themselves with local histories, reflect on their own identities and standpoints, and set expectations and mutually beneficial goals." Another HCI research team, Bray, Harrington, Parker, Diakhate, and Roberts, offer the "Building Utopia" toolkit, which "employs an Afrofuturist lens for speculative design" toward community-driven engagement with technology [20].

There are many challenges to subverting existing practices and establishing more community-centered ones in academic research, for instance financial and reputational incentive structures that encourage exploitation of community partners and rigid standards about what kind of research deserves funding. Participants in the Community Driven Approaches to Research in Technology & Society Workshop raised suggestions for how to resist "the field of computing's myopic and extractive tendencies" [80] and dismantle barriers to collaborative technology development, including establishing common language and values, respecting each community partner as an individual rather than a member of a monolithic group, offering community partners forms of currency that are valuable to them, clarifying researchers' roles and positionalities, and creating recourse for any potential harms [136].

Overall, the research methods offered by community-collaborative approaches [59], participatory design [9], participatory action research [9,23], community-based participatory research [118], and citizen science [124,12] have much to offer cryptographers and privacy technologists looking to engage in collaborative technology development with activists and beyond. These methods are, however, not without issue: in "Deconstructing Community-Based Collaborative Design: Towards More Equitable Participatory Design Engagements," Harrington, Erete, and Piper unpack participatory design workshops as "an affluent and privileged activity that often neglects the challenges associated with envisioning equitable design solutions among underserved populations" [59]. Framing their critique around the harm and historical injustice that researchers have perpetuated against marginalized communities [12,142], Harrington et al. call on researchers to consider the history and context of participating communities especially with respect to "research injustice," to encourage participants to "engage on their own terms and share narratives that they deem important" rather than looking to extract complete personal narratives, and to challenge corporate and overly-technical design mechanisms which may "devalue existing assets or environments" and create distance between marginalized communities and the participatory design process [59].

Collaborative Trainings and Teach-Ins. Borradaile, Kretschmer, Gretes, and LeClerc found that hands-on training workshops can produce sustained use of cryptographic tools for grassroots organizing, even when the tool (PGP) is notoriously difficult to navigate [16]. In general, collective co-education practices such as collaborative trainings, teach-ins, and skills shares have the potential to expand and sustain activists' use of digital privacy and security tools. As noted by Aouragh, Gürses, Rocha, and Snelting [7], and also by Ghoshal, Mendhekar, and Bruckman [47], the process of researching available tools, determining the extent to which they are useful for various tasks, and deploying them in a way that is accessible to the entire grassroots community requires an immense amount of labor [7,47]. While activists are the best people to determine the relevance and accessibility of tools for their work, they are also often already overburdened with roles and tasks, and feel as though the bar of entry to acquiring and synthesizing technical knowledge is too high [7]. This leads to stratifications that Aouragh et al. and Ghoshal et al. identify as harmful and inequitable: the control of critical technological processes to privileged minorities [47] and, more generally, the systematic separation of the sites of technological production from technologies' material use [7].

Education as a practice of freedom [44,45,62] and *abolitionist teaching* [92] are two educational lenses which are pre-aligned with grassroots culture and values—and when instantiated with technological material, could create what Ghoshal, Mendhekar, and Bruckman call a grassroots culture of technology education [47]. As part of formulating a grassroots culture of technology education, this work highlights two types of education that are common in grassroots movement spaces—trainings and teach-ins—and what they might look like when instantiated on the subject of cryptography and digital privacy.

Trainings are closest to traditional conceptions of education in that they typically involve a transfer of knowledge or skill from people with expertise and/or experience to people without expertise and/or experience. While perhaps due to this top-down structure trainings leave the most room for hegemonic structures of technical knowledge to remain active in grassroots spaces [47], they also place the least preparatory burden on participants, and at least provide space for a synchronous gathering in which collective participation, question-answering, and discussion can take place [7]. "Collaborative" trainings imply there is a higher degree of interaction and participation from everyone involved, and serve to bring the traditional notion of a training more squarely into the fabric of inclusive and democratic grassroots practices [47].

In the context of cryptography and digital privacy, effective collaborative trainings could help all participants (including the trainer) come to a common understanding of the landscape of threats that digital technologies pose to grassroots movements, provide an accessible and qualitative review of possible digital interventions, and begin to solidify the ways in which the landscape and interventions might take shape in particular contexts and communities. Rather than the directive approach taken by many digital privacy initiatives, which instruct activists to use particular technologies that may or may not apply to their specific priorities [7], collaborative trainings can help all participants build context toward one-size-fits-one digital privacy practices.

Teach-ins are also typically a knowledge transfer, though they are rooted in community spaces and are a form of direct action. In particular, teach-ins call on community members to occupy a space and to hold that space while engaging in teaching and learning as a form of political resistance. Teach-ins could be a very effective way to explore cryptography and digital privacy from within social, historical, political, environmental, economic, and other contexts of the specific issues that grassroots movements are looking to address. They also require a high degree of community contact and solidarity, as anyone participating in the teach-in is inherently participating in the grassroots movement itself. Therefore, teach-ins afford opportunities not only to democratize technical knowledge, but also to bridge the categorical gap between "tech activists" and "social justice activists" [7] toward a coalition which is demonstrably aligned in both values and practices.

2.2 Digital Trust is Human Trust

Digital trust mechanisms in cryptography and digital privacy technologies often flatten the richness of human trust relationships into binary individualized values held on devices—a singular digitized entity that is either trusted or not trusted—for the purpose of protecting digitized property. Unlike computers, humans do not operate on binary: they may or may not trust people or information within particular contexts or with respect to particular risk-related tasks, and sometimes they are simultaneously trustful and distrustful of the same person or piece of information in ways they cannot explain or quantify. Human trust can change over time, sometimes drastically from one moment to the next, and is inextricably shared between people collectively and interdependently.

Despite its murkiness and variability, trust is an essential part of the ways in which human beings relate to one another. It is also the (ill-specified) foundation of cryptographic systems for digital security and privacy in practice. As stated by Lu, Sannon, Moy, Brewer, Green, Jackson, Reeder, Wafer, Ackerman, and Dillahunt in "Shifting from Surveillance-as-Safety to Safety-through-Noticing: A Photovoice Study with Eastside Detroit Residents," "one's everyday navigation and negotiation of safety is always conditioned by inseparable relationships with other humans, including family, friends, neighbors, acquaintances, and unknown others" [93]. Rather than attempt to simplify or extrapolate the complexities of human trust into a digital medium with rigid constraints, this work proposes that cryptographers and digital privacy technologists who are interested in securing people over property ground their design thinking in the recognition that *digital* *trust is human trust.* Acknowledging that trust is inherently a human experience and cannot be fully digitized calls on us to work with, rather than around or by flattening, human-centered definitions of trust. This section discusses human-centered approaches to incorporating and evaluating trust in digital systems.

Fine-Grained, Collective Authentication. Privacy scholars and cryptographers have criticized the corporatist and individualist conceptions of trust in cryptographic knowledge systems and protocol design [7,139,113,73]. In short, conceptualizing trust and authentication procedures for digital tools as being tied to a single identity is not reflective of the ways in which human beings share tools generally, and the distinction is even more pronounced in the setting of collaborative work like grassroots organizing. Single-party authentication is instead reflective of capitalism and, more specifically, property ownership: cryptographers imagine end-users of digital tools as people who are looking to secure their individual identities and digital property from forgers and thieves, or else they imagine end-users as corporations who want to restrict people's use of hardware, software, cloud, and streaming services to one-user-per-purchase.

As part of the paradigm shift, *digital trust is human trust* asks cryptographers and digital privacy technologists to consider collective authentication, or trust mechanisms that allow for multi-party ownership, authorization, and access to digital systems. In a client-server system with collective authentication, clients may not exist to the server as individual entities; the server might not even be aware of how many entities own a particular digital artifact. To coordinate different levels of access among collective owners without relying on the server, it will be necessary to make the collective authentication process as fine-grained as possible. That way, a collective may decide amongst themselves who has access to what, and when.

Access restriction in the setting of grassroots organizing may be for the grassroots security culture principle of sharing information on a need-to-know basis. That is, access restriction might not be tied to ownership or even trust; rather, mutually trusted parties might intentionally restrict one another from accessing sensitive information that could unnecessarily incriminate them [15,2]. All of the "knobs" in a system with fine-grained collective authentication must be transparent and easy to understand. For example, designers might liken the collective ownership of a digital space to a communal safe house, and fine-grained access restriction to putting locks on particular doors or filing cabinets that only a few out of the collective owners need to access. Of course, it is up to all of the occupants of the house to collectively decide who gets access to what, when—it is not up to the service providers, for instance the lock-makers (i.e. cryptographers), the architects (i.e. protocol designers), or the bank who provides a loan on the mortgage (i.e. the server).

Digital Trust and Physicality. Research on activists' use of digital technologies to facilitate organizing has surfaced an intimate connection between activists' digital trust relationships and physical collective presence, or co-presence, in offline organizing [31,39,53,120,135,2,57]. In general, digital human trust relationships rely, for better or for worse, on perceptions of how people exist in the world physically, and physical properties can be used to authorize individuals' presence in digital spaces such as online forums and support groups [58]. In digital spaces such as public group pages, state actors and counterprotesters have been known to use fake profiles to look like credible members of grassroots organizations while spreading misinformation, inciting arguments, and attempting to destabilize grassroots movements [116,97,108,105]. To combat this, activists rely on in-person trust networks and, where in-person access is not possible, first-hand authentication of digital artifacts from people who are physically connected to the creator(s) of the artifact in question, and can vouch for them [116,33].

In other words, rooting digital trust and authentication procedures in perceptions of physicality is already something that people (and especially activists) do on an everyday basis. As part of acknowledging that digital trust is human trust, cryptographers and digital privacy technologists might actively work to accommodate people's physical-to-digital trust conversion process, making it easier for people to discern whether the owner of a particular digital artifact is someone that the viewer knows in person, either directly or through a trusted third party.

Trust in Technology. Finally, people's general understanding and overall perception of the trustworthiness of technologies factors greatly into their decisions about when and how to use those technologies. In a study of the usability of and motivation behind people's adoption of secure communication tools, Abu-Salma, Sasse, Bonneau, Danilova, Naiakshina, and Smith found that human factors such as social pressures, misunderstanding or mistrust of a particular technology's security and privacy guarantees, and misconceptualizations of security and privacy guarantees in general were more substantial obstacles to adoption than the technology's usability [1]. Ermoshina, Halpin, and Musiani likewise found that even among populations of "high-risk" users such as activists, "the properties of protocols are not understood by users" [40]. One study participant, a privacy technology designer, dreams that in the future, the "trust relationships that we are imagining match the actual trust relationship[s] that actually exist" [40].

While understanding does not necessarily imply trust, it can certainly motivate trust in a way that combats users' privacy-nihilistic perceptions that secure communications are "futile" [1], especially against powerful grassroots adversaries like state governments [116]. As discussed in Section 2.1, hands-on initiatives that encourage participants to reflect on and actively co-create technology practices can create a sustainable trust relationship between high-risk populations like activists and the technologies they use, even when the technology itself may not be the most user-friendly [16]. However, as Aouragh, Gürses, Rocha, and Snelting propose in their critique of online digital privacy education websites and as Abu-Salma et al. confirm in their reporting of study participants' misunderstanding of the EFF Secure Messaging Scorecard, more flattened, top-down digital initiatives organized by "tech activists" [7] and "knowledge brokers" [1] do not substantially increasing activists' understanding of and trust in technology. In order to foster trust and appropriate use of digital privacy technologies, cryptographers and technology designers might consider applying the definition of digital trust as human trust not only as part of the protocol design process, but also as core part of presenting the technology to its intended user-base in a hands-on and accessible way.

2.3 Big-Picture Security

Like the admission that trust is inherently human, *big-picture security* asks cryptographers and digital privacy technologists to situate security considerations firmly within the context of human lives, rather than within the easy-to-model yet reductive landscape of digital technologies. In many cases, cryptographers and privacy technologists' unfounded expectations that human conceptions of security will conform to their modeling-friendly conceptions lead to what Qin, Rosenbloom, and Shrishak call "threat modeling mismatches"—misalignments between proposed privacy technologies and lived privacy needs [111]. This section expands upon the ways in which mismatched security models end up making people less secure in digital environments.

Big-picture security aims to retain the realistic (non-digitizable) complexities of human conceptions of security, and is therefore impossible to realize through digital technologies alone. While cryptographers and digital privacy technologists will by definition not be able to account for every dimension of big-picture security in their protocol designs and implementations, keeping big-picture security in mind throughout the design process will help them create technologies that are compatible with, and therefore useful in sustaining, human lives.

Deniability and Deletion. Cryptographic threat modeling practices, security definitions, and design goals often miss the mark of capturing the lived uses and impact of the tools they produce [111,7,73]. While developers at every stage from ideation to formal security proofs to implementation and adoption might claim their tools are privacy-preserving, several factors can prevent the tools from preserving privacy in practice. Similar to how the trust relationship between people and technology discussed in the previous subsection can impact the lived functionality of digital privacy tools, developers' misunderstanding, dismissal, or deprioritization of the "big-picture" landscape of a digital tool's application can lead to a worse outcome for vulnerable populations than if they had avoided the tool altogether. To capture the ways in which researchers' priorities and mental models of desirable security and privacy properties can misalign with lived use to the detriment of marginalized populations, Qin, Rosenbloom, and Shrishak developed the concept of *threat modeling mismatches* [111].

Qin, Rosenbloom, and Shrishak cite forward secrecy [51] and deniability [24] as examples of cryptographic security properties which have received widespread attention from researchers for their usefulness in protecting marginalized populations from specific adversaries, and that have been proven insufficient for those purposes in practice. In the case of forward secrecy—which states that even if an adversary compromises a key at a particular time (for instance by issuing an “adaptive corruption” like an arrest), it cannot decrypt any messages sent before that time—anti-ELAB activists in Hong Kong found that a more pressing threat was the compromise of contacts and plaintext messages that appeared on activists’ devices in a search incident to arrest [2]. Rather than using tools like Signal with ubiquitous end-to-end encryption and forward secrecy, anti-ELAB activists chose what cryptographers would undoubtedly characterize as less-secure technologies like Telegram (whose group messages are not end-to-end encrypted) and Life360 (a stalkerware application) because those technologies allowed them more fine-grained control over determining whether someone had been arrested and, if so, remotely wiping the contents of their mobile devices [2].

Similarly, deniable encryption affords people who have produced ciphertexts as part of end-to-end encrypted communications the ability to decrypt the ciphertexts to reveal two or more plaintexts. Cryptographers purport that this process allows vulnerable people—for instance activists or whistleblowers under prosecution—to “deny” that they wrote a particular plaintext, since each of the alternative plaintexts are equally mathematically likely to have produced the ciphertext. In the practical context of compelled decryption and legal discovery, however, judges often already know some information about the underlying plaintexts. Therefore, providing decryption keys that produce completely unrelated plaintexts could lead to deeper legal trouble [111]. Yadav, Gosain, and Seamons point out that deniability “requires social and legal acceptance to be effective” as a security property, and that acceptance is far from reality. They further identify specific harms that can result if an application supports deniability without the grounding of social or legal acceptance, such as attackers forging messages that might be trusted from social and legal perspectives, or defendants falsely assuming they can deny messages in court [141]. Carefully examining these and many other kinds of threat modeling mismatches can help researchers and activists identify blind spots in the ways that digital tools are developed and presented to users.

Technology and Movement Suppression. An important part of big-picture security is acknowledging the role of digital technologies in the landscape of movement suppression tactics deployed by powerful state actors, often with the help of technology corporations and academic institutions [15,19,88,66]. What Aouragh, Gürses, Rocha, and Snelting describe as the “sneaky moment” in which grassroots organizers turned to a corporatized ecosystem of digital privacy technologies in the fallout of the Snowden revelations has underscored the cognitive dissonance of trying to use hegemonically-aligned technologies to counteract those same hegemonies and shift power toward dismantling interlocking systems of oppression [7]. For example, the process of “threat modeling” invokes the name of military procedure [7]; it has also helped grassroots organizers and marginalized populations identify priorities and decide when and how to collectively adopt digital privacy tools.

In order to create technology with what Ruha Benjamin calls a “liberatory ethos” [12], it is necessary to identify the aspects of technology which are leveraged to suppress movements, and contrast them with aspects of technology which, if wielded from within the “big-picture” context of grassroots movements, might align with and facilitate those movements. The same technologies used to suppress movements can sometimes be wielded in counter-hegemonic ways, for instance sousveillance is the process of wielding would-be surveillance technologies like publicly-uploaded footage from smartphone cameras against the people who typically exploit surveillance technologies against marginalized people, such as police officers [17]. Citizen journalist practices like filming police officers in the context of high-risk direct action and arrest can help enforce transparency and accountability of the criminal justice system where non-violent democratic processes exist, and help non-local populations understand the extent of authoritarian violence where they do not.

As Audre Lorde warns, however, “the master’s tools will never dismantle the master’s house” [90]. Reclaiming technologies that have been wielded to oppress marginalized people—including cryptography, which has roots in global military history—is a subtle art. Section 4 presents a framework of abolition cryptography, which can help cryptographers and privacy technologists re-imagine the processes of technical knowledge and production in a way that aligns with grassroots values. In short, it is not enough to build, wield, and popularize technologies of any kind, cryptography or otherwise—they must be systematically evaluated and re-evaluated in the context of shifting power dynamics.

Accessibility and Usability. Another “big-picture” consideration is that the technological systems which are the most secure in practice have large and diverse user bases that motivate a high standard of technical maintenance and greater overall attention to accessibility and usability, as opposed to smaller niche tools, which are typically built for technically-fluent users [36]. On the surface this fact could pose a challenge to sustaining the design principle of one size fits one, because it is tempting to position generalized accessibility and usability in direct opposition to the specific accessibility and usability needs of marginalized users. However, by paying attention to diverse needs within marginalized populations, cryptographers and privacy technologists can develop tools that do indeed generalize to wider populations.

Take for example a collection of grassroots organizers, who, despite having a wide array of values and practices in common, are incredibly diverse with respect to race, ethnicity, gender, sexuality, religion, age, language, ability, geographic location, and more. Recognizing activists as composed by these rich particulars [25] opens up the possibility of widening the user base of digital technologies for organizing to populations with each overlapping intersection of identity. With each protocol design aspect that is meant to increase accessibility and usability for specific intersections of the diverse identities of organizers, organizing tools become more useful for general diverse populations. Technology design and development which starts by addressing some specific need of a marginalized population and works to include more and more intersections of identity will produce technologies whose universal accessibility is comprised of rich particulars, rather than a purported universal accessibility that invisibly caters to a privileged minority [25,18,12,56].

2.4 Grassroots Optimization

It is standard practice in cryptography to pay strict attention to the problem of optimization, or making a protocol as efficient as possible. Echoing many other computer science critical scholars [132,137,110,49,71,73,113], this work asks: Optimal for whom? To what end? The material answer to these questions is typically: for corporations and governments, and to the end of protecting property—capital, intellectual, etc.—and government systems, data, and power, respectively. (Cryptographers might tell you it's because they find optimizing things fun, but materially, fun does not keep the lab lights on.)

In contrast to optimizing for corporations and governments, *grassroots optimization* is the act of optimizing for the unique needs of grassroots organizers. Cryptographically, grassroots optimization puts a new frame around constraints and possibilities—some grassroots organizations may not have sufficient computational power to run cryptographic algorithms that activists with the latest smartphones can run easily, while some of those activists might be willing to use more of their device battery to perform intensive computations over small datasets that, on a corporate scale, are prohibitively consumptive. This section considers some of the nuances of grassroots-optimized cryptography, including cases in which access to technology is limited, non-existent, or undesirable.

Devices, Computation, and Communication Complexity. Three important efficiency metrics in benchmarking new technologies are to identify the devices for which the technology is relevant, the technology's computation complexity (corresponding to how much electricity is consumed), and its communication complexity (corresponding to how much information is transmitted), both asymptotically and heuristically with respect to the relevant devices. Activists and marginalized populations all over the world use a diverse range of devices which are severely underrepresented in the cryptography and digital privacy literature. Even researchers who work directly with implementations of cryptographic protocols tend to leverage cloud providers like Amazon Web Services, cutting-edge central and graphics processors, and up-to-date operating systems, ignoring the fact that the vast majority of the world uses years-old technology. Backwards compatibility and device interoperability are seldom if ever discussed in cryptography research, and even companies and organizations who produce technologies and technology advice for practical everyday use do not generally consider the timeliness or relevance of their protocols and recommendations with respect to older devices and inconsistent network connectivity [7].

Similarly, new technologies tend to assume that access to an abundance of electricity and excellent network connectivity are givens, while the majority of the world (and many activists) are inclined to conserve energy for cost, scarcity, or sustainability reasons, and may or may not have consistent access if any to wifi or cellular networks. This may be due to a combination of corporate influence [73,7,121] and researcher privilege, as technology corporations and researchers in particular tend to have privileged access to the newest devices, big budgets for cloud computing, and reliable high-speed internet. "Grassroots optimization" asks technologists to reframe technology design and benchmarking around the realistic availability of devices, energy, and network connectivity for activists and their communities.

Censorship Circumvention. Oftentimes activists' lack of internet connectivity is not the result of a lack of general availability—state actors will intentionally create internet "blackouts" to cut off activists' internet access, forcing them to use alternate communication technologies. For example, activists participating in the Arab Spring used a combination of satellite phones and dial-up to circumvent widespread internet outages [133,63,5,64]. Authoritarian regimes in particular censor citizens' access to particular content and platforms, leaving internet connectivity intact but preventing activists from using well-known digital channels for communicating and disseminating state-critical content and information. Several information and communication technologies such as Tor [36], Bridgefy [3], Firechat [34,96], Session [40], and Briar [40] attempt to get around state censorship using peer-to-peer network connectivity, though of the privacy-preserving technologies only Tor (which is only semi-decentralized) has been consistently used and maintained over a substantial period of time, likely due to its focus on modeling security as usability [36]. Tor developers still struggle to circumvent new censorship techniques, continuously finding work-arounds to keep connectivity up for activists and other vulnerable populations facing more aggressive forms of suppression.

In places where encryption itself is illegal or suspicious, steganography—the process of concealing sensitive information by disguising it as innocuous information—can provide a form of censorship circumvention that maintains strong cryptographic security guarantees [74,70]. While steganography has been largely discounted by the cryptography and privacy technology community as being "security through obscurity," the renewed attention and rigorous treatment of steganography by Kaptchuk, Jois, Green, and Rubin [74] and Jois, Beck, and Kaptchuk [70] has the potential to offer activists cryptographically-secure communications that circumvent encryption-based censors.

Non-Digital Development. One important takeaway from the Community-Driven Approaches to Research in Technology and Society Workshop (discussed in Section 2.1) was participants' support of the *right not to be digital* [136]—that providing non-digital alternatives to digital services is an important and necessary part of ensuring equitable access. This is especially for older participants in grassroots movements living in rural localities [47].

As implied by the previous subsections on physicality (Section 2.2) and censorship circumvention (Section 2.4), non-digital considerations are of vital importance to activists, both in solidifying interpersonal trust and, as demonstrated by the Euromaidan uprising (Section 3.7) and the Dakota Access Pipeline Protests (Section 3.8), in providing the contextual shared ground upon which digital organizing becomes meaningful and effective. Even though cryptographers and privacy technologists are not experts in non-digital security, they should be aware of how the technologies they design and create fit into and work alongside physical infrastructures. When developed in parallel and for mutual benefit, digital and physical technologies have the potential to enhance one another. For example in the case of the Euromaidan uprising, activists' organization of physical IT tents for supporting protesters' digital activities led to the development of new, activist-centered technologies [14].

3 Case Studies

To illustrate and further motivate aspects of the paradigm shift, this section presents several formative case studies of activists' relationships with surveillance, cryptography, and various digital technologies. There are many examples which are not covered in depth due to time and space constraints, but which played a role in the analysis and creation of the paradigm shift: political organizing in the United States (U.S.) [99,100,101], anti-censorship protests in Singapore [120], the YoSoy132 movement in Mexico [129], political organizing in Guatemala [57], Occupy Wallstreet [128] and inspired movements [134,6,127], education and energy policy activism in Chile [135], the Gezi protests in Turkey [53], the Umbrella Movement in Hong Kong [84], Science for the People-Atlanta [46], Southern Movement Assembly [47], and trans rights [86] organizing in the U.S., the Sudanese revolution [33], and more general studies [16,31,39,48] including those which focus on "high-risk" populations including activists [54,40,35].

The paradigm shift is also strengthened by expert analyses of the historical modes of suppression of grassroots movements [19,15,123,104] that have been reproduced, reinforced, and expanded in the digital age. In addition to the case study on COINTELPRO below, Edward Snowden revealed in 2013 that military and intelligence agencies, with support from U.S. technology corporations, had widely adapted and deployed these techniques in digital spaces—and have since wielded them disproportionately against marginalized people [60,104,98,7,97]. Simone Browne [21], Ruha Benjamin [11], Antony Loewenstein [88], and many others have discussed the systematic ways in which surveillance technologies disproportionately impact People of Color and people with intersections of multiply-marginalized identities, for instance Black women [102,22], Palestinians [88,66], working-class people [42], and trans and queer people [77,78].

3.1 COINTELPRO

From 1956-1971, the United States' Federal Bureau of Investigation (FBI) illegally and extensively surveiled and intimidated civil rights activists as part of the COINTELPRO operation [29]. Though the COINTELPRO operation took place in the pre-digital era, it is an important illustration of many standard grassroots movement suppression tactics [19,15] which have been bolstered by digital technologies or adapted into digital spaces. Especially prescient is the revelation of the extent to which the FBI used psychological suppression tactics to destabilize the civil rights movement and turn activists against one another, as well as the fact that they were willing to wield violence, incarceration, and assassination against movement leaders when psychological tactics failed to deter them [72]. Each of these operations began with extensive "intelligence gathering," demonstrating the short, malleable distance between state surveillance and state violence, even against citizens in a democratic republic. Wider dragnet tactics facilitated by digital technologies like the internet and cell phones were deployed against Muslim Americans and many others in the wake of the 9/11 attacks in 2001, as demonstrated by the Snowden revelations in 2013. Since then, digital surveillance and other digitally-facilitated movement suppression tactics have become a regular part of the U.S. law enforcement playbook, as evidenced by police responses to numerous grassroots movements in the U.S., including the Black Lives Matter movement (Section 3.6) and Dakota Access Pipeline protests (Section 3.8) discussed below.

3.2 Synco, or Project Cybersyn

The Popular Unity government of Chile's *Proyecto Synco*, known as Project Cybersyn in English, was a powerful conception of an early internet which illustrates the potential of technological alternatives and "grassroots optimization." In the vision of *Synco* set forth by the Popular Unity government from 1971-1973, each site of material and later societal production (such as factories and homes) would be equipped with a computer and networked in such a way that workers could provide instant and direct feedback to the government about problems, resources, and working conditions. Rather than facilitating a corporatized and increasingly monopolized, ad-driven economy like the internet of today, *Synco* imagined an internet which would facilitate a grassroots economy, where each individual could participate democratically in distributing the wealth they helped to generate, and in making sure their environments were livable and sustainable. *Synco* was destroyed in the military coup of 1973.

3.3 Operation Vula

The first documented use of modern cryptography for grassroots organizing was the African National Congress' (ANC) Operation Vula cryptosystem, which anti-apartheid activists used to send secure communications between local and exiled ANC members in South Africa, England, Zambia, and the Netherlands from 1986-1990 [73,68]. Activists needed the system be *asynchronous* (since parties were not guaranteed to be online at the same time), *covert* (since use of encryption and computers was suspicious at the time), *correct over long distances* (since lots of errors were introduced from Lusaka to London), and *public* (since not all activists had phone lines at home).

The Operation Vula protocol was run between safe houses with computers, for instance one in Cape Town and the other in Johannesburg. Cape Town activists first encrypted their message to obtain a ciphertext. While computers were suspicious and rare at the time, public phone booths were covert and easily accessible. In order to relay the ciphertext over a public phone line without arousing suspicion, activists ran the ciphertext through an acoustic modem, which converted the ciphertext into sound waves. They then recorded the sound waves of the ciphertext into a small tape recorder, and brought the tape recorder into a public phone booth. Finally they dialed a phone with an answering machine at a safe house in London and played the tape recording into the answering machine. To retrieve the message, Johannesburg activists would dial into the London safe house's answering machine from another public phone booth, record the message on their tape recorder, and decode and decrypt the ciphertext using the Johannesburg safe house acoustic modem and computer, respectively.

The encryption algorithm was a one-time pad $\mathtt{Enc}(K, m) = \mathtt{PRG}(K) \oplus m$ with a custom-designed pseudorandom generator (PRG), where keys were seeded from books and used seeds were marked with invisible ink [73]. Activists introduced error correction into the algorithm after they realized the noise of the coins going into the pay phone disrupted the audio; they later switched from coins to phone cards to avoid the error. Despite heavy use by ANC activists—even to communicate with Nelson Mandela in jail—the Operation Vula cryptosystem ran undetected into the early 1990s.

In building out Operation Vula, activist Tim Jenkin reported, "I went to find out about secure encryption algorithms...All I discovered was that cryptology was an arcane science for bored mathematicians, not for underground activists. However I learned a few tricks and used these to develop a system to meet our security needs" [68]. Many of the most challenging aspects of the security modeling in Operation Vula were considerations, both technical and non-technical, that had nothing to do with the encryption algorithm. Rogaway notes that cryptography literature rarely explores even technical problems that are outside the scope of what cryptographers can model with traditional complexity theoretic techniques, even when the problems are highly relevant to the intended use-case [113]. While provable security provides a key component of overall security and is therefore a worthwhile goal, the story of Operation Vula invites cryptographers to widen the scope of our security notions, as ignoring the "big picture" results in incomplete and inaccessible solutions for people who need cryptography the most.

3.4 Arab Spring

Formal extensive study of digital technologies in the context of grassroots organizing largely began in 2010 as a result of the Arab Spring, which was a series of widespread anti-establishment protests in Tunisia, Libya, Egypt, Yemen, Syria, Bahrain, Morocco, Iraq, Algeria, Lebanon, Jordan, Kuwait, and many other places [133,63,5,64]. In particular, activists who participated in the Arab Spring used blogs and social media to increase the speed of information sharing among other participants and global supporters, the scope of the information they were able to share (such as personal opinions and visual evidence of authoritarian brutality), and the scale of the movement in general [115]. Contemporary studies of other grassroots movements such as the YoSoy132 movement in Mexico also commented on social media's ability to facilitate both "frontstage" and "backstage" tasks such as protest organizing and community building, respectively [129]. The word *facilitate* is important: scholars who study the role of social media in grassroots movements are careful to position it as a tool that grassroots organizers wielded to their ends, rather than a direct or independent cause of change [135,63]. Arab Spring activists' tactics and especially their fluent use of social media to galvanize a strong grassroots base inspired activists in countless movements across the world.

3.5 Anti-Corruption Foundation

In "Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices," Tetyana Lokot discusses the ways in which Russian opposition activists organizing with the Anti-Corruption Foundation use a non-mutually-exclusive mixture of conspicuous security and strategic visibility practices [89]. For example, Lokot documents activists' use of digital privacy tools like Tor and end-to-end encrypted messaging alongisde their use of YouTube to educate their supporters and spread awareness about these tools, as well as to foster a sense of organizational transparency and community. The model of encouraging radical transparency and digital security education in larger, public-facing organizational ecosystems while using digital privacy tools like end-to-end encryption among smaller collections of trusted individuals such as leaders and organizers is echoed throughout modern grassroots movements, for instance during the anti-ELAB protests in Hong Kong [2].

Activists' differentiation between platforms and group sizes for digital communications based on the function of the group (spreading public awareness v. planning a high-risk direct action among trusted parties, for example) suggests that the principle of "one size fits one" must go beyond addressing the needs of grassroots organizers in general to addressing their needs with respect to a particular task or moment in time. In other words, the ways that activists relate to one another in particular contexts such as big public groups or small private groups—both necessary for successful organizing—motivates the creation of digital technologies which are aware of and respectful of those contexts. This does not necessarily mean that one digital technology will or should cover all of the contexts, but rather that designers should take specific use cases into account when designing technologies in context. For example, incorporating end-to-end encryption into a platform designed to spread awareness of a grassroots movement may make the platform less accessible while providing no benefit with respect to confidentiality (since the information communicated on the platform is supposed to be public anyway). On the other hand, integrating anonymous communication channels into such a platform might be of great benefit, and a worthwhile tradeoff for accessibility if the activists in question are at high risk of state violence for simply accessing the platform in the first place. Context-dependent information sharing and safety-visibility tradeoffs are also a fundamental part of activists' collective security culture considerations [15,2,89], and should therefore be incorporated into analyses of "big-picture security" and "grassroots optimization."

3.6 Black Lives Matter

Following Derek Chauvin and the Minneapolis Police Department's murder of George Floyd in 2020, Black Lives Matter (BLM) activists across the U.S. and around the world organized widespread protests. The protests were planned quickly, and BLM organizers relied heavily on social media to spread the word about them. Leah Namisa Rosenbloom synthesized 50 conversations with Black Lives Matter activists in Philadelphia into an informal study [116] and found that the speed of organizing coupled with the ease of manufacturing identities, malicious content, and misinformation on social media led to higher-risk situations. For example, a group of activists reported encountering an event on Facebook that appeared to be a BLM event, but was actually organized by members of the neo-fascist White nationalist group Proud Boys posing as BLM organizers [116]. It was later revealed that Russian state actors had also attempted to disrupt and destabilize BLM organizing efforts and further stratify U.S. voters across racial lines via race-baiting, misinformation, and paid advertising on social media [108,105]. To vet the trustworthiness of digital information during the highly risky period of organizing in 2020, BLM activists turned to discussing the trustworthiness of digital artifacts from within established personal networks. Daffalla, Simko, Kohno, and Bardas observed similar practices in their study of the Sudanese revolution, reporting that activists used a form of "crowd-sourced content moderation" and reliance on "first hand sources" to verify the authenticity of digital information [33].

With respect to efficiency, the speed of organizing coupled with anti-BLM algorithmic bias [114] led to simultaneous content inundation [100,94] and content suppression, both of which made information about protests difficult to find consistently and reliably online. While an overwhelming majority of people in the informal study ($84\%, N = 50$) used social media to find information on actions in general, only 48% reported that they heard of that day's action through social media. By contrast, while only 40% of participants reported tapping personal networks to find information in general, 42% heard about that day's action through personal networks. Rosenbloom concluded that while the majority of participants used social media to find information about actions, intimate and physically-grounded discovery methods such as word of mouth had a more consistent yield of in-person participation.

3.7 Euromaidan Uprising

The interplay between physical and digital spaces formed a vital part of the Euromaidan uprising in Ukraine, which ultimately led to the ousting of Russian-backed Ukranian President Viktor Yanukovych in 2014. “Euromaidan” translates to “European Square,” evoking a combination of what the protesters were resisting—Yanukovych’s decision to defer the European Union-Ukraine Association Agreement—and where they were meeting to demonstrate their dissatisfaction: public squares all across the country. Kyiv’s *Maidan Nezalezhnosti*, or Independence Square in English, was taken over and held by an encampment of thousands of protesters who created a sustainable crowd-sourced ecosystem within it (one famous image depicts a person ladling from a gigantic cauldron of soup, barricades and a long line of people stacked behind them).

According to Tetyana Bohdanova, who wrote the study “Unexpected revolution: the role of social media in Ukraine’s Euromaidan uprising,” protesters’ occupation of Independence Square started with Ukranian journalist Mustafa Nayyem’s Facebook post: “‘We are meeting at 22:30 under the Monument of Independence. Dress warm, bring umbrellas, tea, coffee, good mood and friends. Reposts are highly encouraged!”’ [14]. Social media was later used to coordinate vital support for demonstrators: to track those who were detained or missing, provide legal advice, conduct sousveillance on police brutality, organize medical brigades, financial resources, and media campaigns, visualize protesters’ needs using crowdmapping technology, collaborate on movement art, and coordinate the motivational “online/offline information centre Don’t Ditch Maidan” to keep the movement going. Bohdanova writes, “it was the use of social media and other [information and communication technology (ICT)] tools for crowdsourcing physical and creative resources that was the most crucial for sustaining Euromaidan over a long period of time.”

One crowdsourced resource in the Euromaidan uprising that provides important insight into the potential role of cryptographers and privacy technologists in grassroots organizing spaces is that of the information technology (IT) tent: a physical space initially offering “free Internet access and computer equipment for protesters, which later evolved into a space where technology specialists met and collaborated with professional activists on a number of ICT-enabled social projects” [14]. Bohdanova warns, however, that it was “not social media but offline social ties” that formed the bedrock of the movement, and that the “loose, decentralised” nature of social media networks hindered the ability of the Euromaidan movement to form “a clear vision and a strategy” after a critical mass of people had been mobilized to participate [50].

3.8 Dakota Access Pipeline Protests

The Dakota Access Pipeline resistance (NoDAPL) protests were part of a Standing Rock Sioux- and Native American youth-led movement against the U.S. government’s ongoing theft and environmental degradation of Native Peoples’ land, sacred sites, and water sources—in this case, to accommodate Energy Transfer

Partners' multi-billion dollar, 1,172-foot underground pipeline. Similar to the important role of intersecting physical and digital spaces in the Euromaidan uprising discussed above (Section 3.7), NoDAPL protesters, also known as water protectors, organized heavily using Facebook, and their digital organizing was intimately tied to the land they were occupying.

To overcome the hurdle of spotty service in the Standing Rock reservation, water protectors established "Facebook Hill"— the closest place to their encampment with enough service to spread news in the form of first-person accounts, images, and videos to the world about what was happening at Standing Rock. As discussed by Hayley Johnson in the study "#NoDAPL: Social Media, Empowerment, and Civil Participation at Standing Rock," the remote location of the protests—and of many environmentally-centered, Native American-led protests like it—meant that "major national media coverage" was scant and second-hand [69]. The lack of traditional media coverage made water protectors' and independent journalists such as Unicorn Riot's first-hand, social media-spread accounts of their experiences at Standing Rock—pepper spray, attack dogs, sound cannons, water cannons in freezing weather, and detentions in small cages—critically important in understanding the extent of the brutality enacted upon the peaceful demonstrators by Energy Transfer's security forces and police.

When water protectors put out a call for help after hypothesizing that the Morton County Sheriff's Department was surveilling them using Facebook, over 1.5 million people all over the world used Facebook's "check-in" feature to claim that they were at Standing Rock in an attempt to stymie surveillance efforts [76]. While the Sheriff's Department was likely not using check-in data to determine water protectors' locations or movements—making the digital action largely symbolic—it showed supporters' awareness and receptiveness to aiding in counter-surveillance of grassroots movements, and that the movement was supported by people all over the world.

3.9 Anti-ELAB Movement

Finally, the anti-Extradition Law Amendment Bill (anti-ELAB) movement, also known as the Water Movement or the 2019-2020 Hong Kong protests, was a series of widepsread demonstrations against a bill which would have expanded the Chinese government's ability to extradite and arrest political dissidents in Hong Kong. The movement also sought justice for brutalized and incarcerated protesters. In their study "Collective Information Security in Large-Scale Urban Protest: the Case of Hong Kong," Albrecht, Blasco, Jensen, and Mareková conducted qualitative interviews with 11 movement participants, and found that protesters had developed intricate collective digital security culture [15] and decision-making practices which informed their choices and use of privacy-preserving technologies [2].

As discussed in Section 2.3 on threat modeling mismatches above, protesters had one key requirement that no existing end-to-end encrypted technology could meet: they wanted a way to determine whether someone had been arrested and, if so, remotely wipe the contents of their device. This firm requirement led protesters to adopt Life360—software with fine-grained remote mobile device-monitoring capabilities. Cryptographers and privacy technologists largely consider applications like Life360 to be "stalkerware" that exploits those with the application installed and fails to preserve their privacy. However, anti-ELAB activists needed to engage in a form of consensual stalking in order to keep track of one another in high-risk situations, and keep the entire group safe in the event that one person was arrested and their mobile device compromised. Similarly, activists adopted the messaging application Telegram, whose group messages are not end-to-end encrypted, because of Telegram's support for 200,000-member groups (as opposed to Signal's 1,000 and WhatsApp's 256), remote deletion of messages, polls, and live location sharing. Albrecht, Blasco, Jensen, and Mareková also found that activists perceived Telegram as the "most secure" communication platform, with one participant significantly misunderstanding the end-to-end encryption security guarantees (claiming that end-to-end encrypted group messaging can be enabled, which is not true) [2].

Like the practices of Anti-Corruption Foundation activists discussed in Section 3.5, anti-ELAB protesters also formed larger public groups and smaller private groups on digital messaging platforms for more fine-grained control over information sharing and action planning. And, similar to the inundation of content that activists experienced during the fast-paced organizing of Black Lives Matter protests in 2020 (Section 3.6), anti-ELAB protesters also faced "a sense of information overload" on their digital communication channels which "often made it difficult for them to keep up with evolving protest tactics" [2]. This led to participants making ad hoc "tactical decisions within seconds" about which information channels to close off and which to keep open in an effort to receive information on a need-to-know basis.

4 Abolition Cryptography

Phillip Rogaway states and expands upon the idea that "cryptography rearranges power" [113]. Given activists' use of cryptography and privacy-preserving technologies from Operation Vula through the present day, this work suggests cryptography has *the potential* to rearrange power, though, as Rogaway and other critics point out, cryptography as a field often reproduces norms which serve to keep hegemonic systems of power firmly in place [73,7]. While cryptography for grassroots organizing is one idea for cryptography with an ethos of rearranging power, it is not enough: there are many ways in which cryptography production systems perpetuate a status quo that elevates the security of property over people, fuels technologies such as cryptocurrencies and privacy-preserving AI (whose need for energy and precious metals poison the environment especially in the Global South [75]), and opens opportunities disproportionately to White men in the Global North. None of the issues mentioned in this section are unique to cryptography. As it says in *Pirke Avot*, we aren't required to finish the job, nor are we free to desist from it: we can use our positions to prioritize systems of knowledge production that center human well-being.

This section applies Leah Namisa Rosenbloom's *Living Framework for Abolitionist Teaching in Computer Science* [117], based on the work of abolitionist scholars Bettina L. Love [92], Jones and melo [71], and many more [82,125,10,91] [44,61,49,109,38,131,37,11], to propose the idea of *abolition cryptography*. Abolition cryptography aims to create a theory and practice (praxis) of cryptography which is values-aligned with the collective power of grassroots movements—and with marginalized people in general—by suggesting ways in which we might replace harmful technological systems with ones that sustain human lives and livelihoods. The following aspects, which mirror the aspects of the abolitionist teaching framework [117], are only a first attempt: like grassroots organizing, abolition cryptography is a collective, ongoing, and iterative process. This first iteration drawn on the work of not only abolitionist teachers, but on the work and perspectives of fellow cryptographers and privacy technologists who offer invaluable insight into the hidden intersecting forces that undergird the field.

4.1 Becoming Organizers

The work of cryptography is intimately connected with systems of power whether cryptographers recognize it or not [113], and choosing not to recognize it means tacitly supporting the status quo. In order to work ethically on systems which are enmeshed in the fabric of power, we need a better understanding of the fabric of power and of the impact our work might have on it. One of the best ways to understand the boundaries and intricacies of power is by trying to shift or rearrange power ourselves, by becoming grassroots organizers for material change in the field and in general. Organizing for change can take many different forms, some of which are discussed below.

4.2 Reframing Cryptography History and Resistance

If you ask a cryptographer about the history of cryptography, they will likely cite some combination of the following phenomena: Caesar cipher, Shannon cipher, Enigma, public-key cryptography, clipper chips, export controls, Snowden, and perhaps a myriad of more modern cryptographic research areas. While these are all valid components of cryptography history, they are not the only components, and taken together they tell a story that is decidedly rooted in While, male, Global Northern ways of knowing that ignore the stories of marginalized people—even when those stories document the application and development of landmark cryptography and privacy technology. For example, Seny Kamara was (to my knowledge) the first academic cryptographer to talk publicly about the Operation Vula cryptosystem (Section 3.3) in 2020 [73], 34 years after the project began and 30 years after it had played a significant role in ending apartheid in South Africa. How many more groundbreaking uses of cryptography to rearrange power have been ignored by cryptographers over the last 34 years? It is up to us to find out, and to learn from those stories the ways in which cryptography can help people resist systems of oppression beyond the individualist cipherpunk approach, beyond a citizen-centered “right to privacy,” and toward a cryptography resistance framework which works for the liberation of all people, collectively.

4.3 Equitable Access to Conferences, Funding, and Publication

Advances in cryptography research are primarily disseminated through conferences and their proceedings, which are organized, for example, by the International Association for Cryptologic Research (IACR). Crypto, the de facto flagship IACR conference, takes place every year in Santa Barbara, CA, U.S.—a country with some of the strictest and most exclusionary visa requirements in the world. The only other IACR conference with an A^* ranking from the International Computing Research and Education (ICORE) Conference Ranking Portal is EuroCrypt, which is always held in a similarly inaccessible European country. Several other conferences in the field such as Asiacrypt, Latincrypt, and AfricaCrypt are explicitly segregated by geographic location.

Access to funding is similarly gate-kept by multinational corporations such as the biggest sponsors of Crypto 2023: Google, Amazon Web Services, and the Technology Innovation Institute. One of the most important requirements for publication is the ability to understand and produce cryptography knowledge in English, which already severely limits access and participation in cryptography to a privileged minority. Again, these problems are not at all unique to cryptography: they appear in almost all CS disciplines and in many other scientific and academic fields in general. Taken together, it is clear that more equitable access to conferences, funding, and publication in cryptography is sorely needed.

At the rump session of Crypto 2022, Daniel Escudero called cryptographers' attention to Criptolatino, an organization that centers Latin American cryptographers' work and experiences in cryptography [41]. As part of the talk, Escudero explained that many people with accepted papers who wanted to attend Crypto could not be there because of visas and cost, that only a tiny number of countries have visa-free access to the U.S., and that people from Colombia, for example, might have to wait 696 calendar days (almost two years) for a visa. As a collective, Criptolatino offers strategies for addressing these issues: increasing visibility of Latin American students and researchers, hosting events like workshops that raise awareness and offer opportunities for students in Latin America and beyond, building networks between different regions, and creating resources in Spanish and Portuguese for better accessibility of cryptography content.

Elena Pagnin, Sofía Celi, and Akira Takahashi released a set of recommendations for the IACR, “On Creating a More Inclusive and Supporting Community,” which call attention to the need for more visa support, online accommodation, and financial assistance, pointing out that even the IACR's registration cost of 25 U.S. dollars alone corresponds to a month's worth of food in certain places in the Global South [107]. Supporting Criptolatino and initiatives like Pagnin, Celi, and Takahashi's—first by listening, talking about, and financially backing them, and then by taking organizational roles to overhaul exclusionary practices—is a great place to start working toward equitable access and accountability.

4.4 Against Surveillance Techno-Solutionism & Centering Property

The techno-complexes identified in Rosenbloom's framework [117] manifest in cryptography in many ways, for instance in surveillance techno-solutionism, which positions cryptography as the one-size-fits-all solution to surveillance, or in the techno-colonialist tendency of cryptography research to consider the security of property and devices over people. As indicated in Section 2, the idea of a one-size-fits-all, top-down solution does not adequately address the needs of the marginalized populations who may need cryptography the most [7]. Furthermore, centering cryptography in conversations about mass surveillance and focusing on individual privacy rights ignores the historical context of why and how state powers have wielded mass surveillance disproportionately against marginalized people. Cryptographic "solutions" to mass surveillance which obscure systemic issues and omit marginalized perspectives from the problem-solving conversation create a seemingly progressive "stumbling block" [79]—an incomplete or ineffective solution which masquerades as progress while failing to fix the problem, simultaneously slowing down and drawing attention away from more comprehensive, but perhaps less shiny or technically novel, initiatives. Finally, as discussed in Section 2.2, many cryptographic protocol designs prioritize the security of property over people by defining trust and ownership on an individual basis, reducing human beings to their devices for technical convenience, and optimizing applications and algorithms for the benefit of corporations seeking to protect capital and intellectual property. Centering the design principles outlined in the paradigm shift (Section 2) and continuing to learn from the people, organizations, and work that inspired them are just one way to go about resisting the techno-complexes in cryptography.

4.5 Cryptography and Creative Expression

Cryptography and privacy have deep and under-explored psychological, emotional, and spiritual dimensions. Non-technical ways of knowing and being like visual art, song, dance, creative writing, prayer, and storytelling [67,119,122,38,71] [28,103,18] therefore have a lot to offer cryptographers in the process of getting to the bottom of our relationship with surveillance, and toward a more radical understanding of privacy and security. For example, Lu, Sannon, Moy, Brewer, Green, Jackson, Reeder, Wafer, Ackerman, and Dillahunt used photovoice, a participatory technique where participants offer "photographic narratives," to discuss the "lived experiences of navigating personal and community safety" of 11 older Black members of a Detroit-area community organization [93]. The study offers "an epistemological shift from *surveillance-as-safety* to *safety-through-noticing*," radically re-imagining safety as driven by mutual community noticing which, like surveillance, involves watching and observing but, unlike surveillance, does not involve institutional power and the threat of violence. Opening up our definitions of technology to include mechanisms of creative expression can help cryptographers understand, process, and confront surveillance and systems of marginalization on a deeper level.

4.6 The ReCAP Workshop

Chator, Kamara, Qin, and Rosenbloom offer a new space and vision for cryptography and privacy scholarship in the "Re-Imagining Cryptography and Privacy" (ReCAP) Workshop. The focus of the ReCAP Workshop is Re-Imagination: "identifying the aspects of cryptography and privacy technology production that contribute to marginalization, and solidifying approaches, ideas, and designs that center marginalized voices, resist toxic aspects of technology production, and leverage cryptography and privacy tools toward dismantling systems of oppression" [27]. Like the Community-Driven Cryptography Project [26], the ReCAP Workshop "seeks to build and sustain an interdisciplinary community" and "contribute to the broadening of access to the field." Such designated spaces for re-imagination work are important, but will not carry the work through alone: we can each "start where we are" [117] in this moment, thinking, discussing, and building in our own communities toward a cryptography praxis that supports collective power for marginalized people.

5 Conclusion

This work belongs in theoretical cryptography spaces because it speaks to the moral and ethical obligation of all cryptographers to understand the lived impact of their work on systems of power [73,113]. While to date there have been few if any transdisciplinary papers published at theoretical cryptography conferences, this work argues and demands space for considerations of the real-world impact of cryptography at all levels of the cryptography production pipeline, starting with theoretical foundations. Applied cryptographers, privacy technology developers, and even activists (in the case of Tim Jenkins of Operation Vula) look to the work of theoretical cryptographers to determine what is possible—to form a basis for their ideation and implementation of cryptographic tools in the real world. Therefore, theoretical cryptographers hold a great deal of power: the ability to set the stage for future work on privacy-preserving technologies. In order to wield this power in a way that helps to break cycles of systemic harm and works toward building collective power for marginalized people, cryptographers must be literate in the language of power. By drawing closer together the worlds of cryptography and transdisciplinary scholars—who have developed rigorous theory at the intersection of technology and collective power—and by shifting our mindsets and priorities toward the self-articulated perspectives of marginalized communities, we can begin to create cryptography praxis with a lived positive impact on all human lives and livelihoods.

Acknowledgements

Thank you to Seny Kamara and Anna Lysyanskaya for affirming this work as part of my PhD in cryptography, thereby creating space for this work to exist and thrive. Thank you to Seny for ongoing reflection on and discussion of the ideas in this paper and beyond. Thank you to Lucy, Alishah, and all the participants in the Community-Driven Cryptography Seminar and the Re-Imagining Cryptography and Privacy Workshop for your insights and camaraderie. Thank you to Yash, Sofi, Daniel, the cryptographers of Criptolatino, and all those working to shift power in cryptography toward inclusion and collective well-being. Thank you to all of the people whose work I cite in this paper for inspiring me in a big way. And thank you to all my comrades, near and far, for the same reason. Finally, thank you to my family and my ancestors, for the value of questioning:

Why? For Whom? And Toward What Ends?

References

1. Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153. IEEE, 2017.
2. Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Collective information security in large-scale urban protests: the case of hong kong. *arXiv preprint arXiv:2105.14869*, 2021.
3. Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Mesh messaging in large-scale protests: Breaking bridgefy. In *Cryptographers' Track at the RSA Conference*, pages 375–398. Springer, 2021.
4. Michelle Alexander. The new jim crow. *Ohio St. J. Crim. L.*, 9:7, 2011.
5. Nezar AlSayyad and Muna Guvenc. Virtual uprisings: On the interaction of new social media, traditional media coverage and urban space during the 'arab spring'. *Urban Studies*, 52(11):2018–2034, 2015.
6. Eva Anduiza, Camilo Cristancho, and José M Sabucedo. Mobilization through online social networks: the political protest of the indignados in spain. *Information, communication & society*, 17(6):750–764, 2014.
7. Miriyam Aouragh, Seda Gürses, Jara Rocha, and Femke Snelting. Fcj-196 let's first get things done! on division of labour and techno-political practices of delegation in times of crisis. *The Fibreculture Journal*, (26 2015: Entanglements–Activism and Technology), 2015.
8. Evronia Azer, G Harindranath, and Yingqin Zheng. Revisiting leadership in information and communication technology (ict)-enabled activism: A study of egypt's grassroots human rights groups. *New Media & Society*, 21(5):1141–1169, 2019.
9. Megan Bang and Shirin Vossoughi. Participatory design research and educational justice: Studying learning and relations within social change making. *Cognition and Instruction*, 34(3):173–193, 2016.
10. Derrick A Bell. Who's afraid of critical race theory. *U. Ill. L. Rev.*, page 893, 1995.
11. Ruha Benjamin. Race after technology: Abolitionist tools for the new jim code. *Social Forces*, 2019.
12. Ruha Benjamin. *Viral justice: how we grow the World we want.* Princeton University Press, 2022.
13. Our Data Bodies. About. https://www.odbproject.org/about-us-2/, 2024.

14. Tetyana Bohdanova. Unexpected revolution: the role of social media in ukraine's euromaidan uprising. *European View*, 13(1):133–142, 2014.
15. Glencora Borradaile. *Defend Dissent*. Oregon State University Corvallis, 2021.
16. Glencora Borradaile, Kelsy Kretschmer, Michele Gretes, and Alexandria LeClerc. The motivated can encrypt (even with pgp). *arXiv preprint arXiv:2104.04478*, 2021.
17. Glencora Borradaile and Joshua Reeves. Sousveillance capitalism. *Surveillance & Society*, 18(2):272–275, 2020.
18. Daniel Boyarin. *The no-state solution: a Jewish manifesto*. Yale University Press, 2023.
19. Jules Boykoff. Limiting dissent: The mechanisms of state repression in the usa. *Social Movement Studies*, 6(3):281–310, 2007.
20. Kirsten E Bray, Christina Harrington, Andrea G Parker, N'Deye Diakhate, and Jennifer Roberts. Radical futures: Supporting community-led design engagements through an afrofuturist speculative design toolkit. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2022.
21. Simone Browne. *Dark matters: On the surveillance of blackness*. Duke University Press, 2015.
22. Joy Buolamwini and Timnit Gebru. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency*, pages 77–91. PMLR, 2018.
23. Julio Cammarota and Michelle Fine. Revolutionizing education. *Youth Participatory*, 2008.
24. Rein Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky. Deniable encryption. In *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17*, pages 90–104. Springer, 1997.
25. Aimé Césaire. Discourse on colonialism. In *Postcolonlsm*, pages 310–339. Routledge, 2023.
26. Alishah Chator, Seny Kamara, Lucy Qin, and Leah Namisa Rosenbloom. *Community-Driven Cryptography Seminar*. 2021.
27. Alishah Chator, Seny Kamara, Lucy Qin, and Leah Namisa Rosenbloom. *Re-Imagining Cryptography and Privacy (ReCAP) Workshop*. 2024.
28. Barbara Christian. The race for theory. *Feminist studies*, 14(1):67–79, 1988.
29. Ward Churchill and Jim Vander Wall. The cointelpro papers. *Boston: South End*, 1990.
30. Detroit Digital Justice Coalition. About. https://www.detroitdjc.org/about-1, 2024.
31. Ted M Coopman. Networks of dissent: Emergent forms in media based collective action. *Critical studies in media communication*, 28(2):153–172, 2011.
32. Sasha Costanza-Chock. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, 2020.
33. Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. Defensive technology use by political activists during the sudanese revolution. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 372–390. IEEE, 2021.
34. Jakub Dalek, Philipp Winter, Andrei Dranka, Masashi Crete-Nishihata, and Adam Senft. Asia chats: Update on line, kakaotalk, and firechat in china. *The Citizen Lab*, 2014.
35. Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. In encryption we don't trust: The effect of end-to-end encryption to the masses on

user perception. In *2019 IEEE European symposium on security and privacy (EuroS&P)*, pages 401–415. IEEE, 2019.

36. Roger Dingledine and Nick Mathewson. Anonymity loves company: Usability and the network effect. In *WEIS*. Citeseer, 2006.
37. WE Burghardt Du Bois. Black reconstruction in america, 1860-1880. *Racism Essential Readings*, pages 27–34, 2001.
38. Michael J Dumas and Kihana Miraya Ross. "be real black for me" imagining blackcrit in education. *Urban Education*, 51(4):415–442, 2016.
39. Jennifer Earl and Katrina Kimport. *Digitally enabled social change: Activism in the internet age*. MIT Press, 2011.
40. Ksenia Ermoshina, Harry Halpin, and Francesca Musiani. Can johnny build a protocol? co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols. In *European Workshop on Usable Security*, pages 1–13, 2017.
41. Daniel Escudero. Criptolatino: a group that advocates for cryptography research made by/for latin-americans. https://youtu.be/_qSja6VpPbQ?t=588, 2022.
42. Virginia Eubanks. *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press, 2018.
43. Data for Black Lives. Index. https://d4bl.org/, 2024.
44. Paulo Freire. Pedagogy of the oppressed (mb ramos, trans.). *New York: Continuum*, 2007, 1970.
45. Paulo Freire. Education: the practice of freedom (london, writers and readers). 1976.
46. Sucheta Ghoshal and Amy Bruckman. The role of social computing technologies in grassroots movement building. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 26(3):1–36, 2019.
47. Sucheta Ghoshal, Rishma Mendhekar, and Amy Bruckman. Toward a grassroots culture of technology practice. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW1):1–28, 2020.
48. Homero Gil de Zúñiga, Alberto Ardèvol-Abreu, and Andreu Casero-Ripollés. Whatsapp political discussion, conventional participation and activism: exploring direct, indirect and generational effects. *Information, communication & society*, 24(2):201–218, 2021.
49. Ruth Wilson Gilmore. *Abolition geography: Essays towards liberation*. Verso Books, 2022.
50. Malcolm Gladwell. Small change. *The New Yorker*, 4, 2010.
51. Christoph G Günther. An identity-based key-exchange protocol. In *Advances in Cryptology—EUROCRYPT'89: Workshop on the Theory and Application of Cryptographic Techniques Houthalen, Belgium, April 10–13, 1989 Proceedings 8*, pages 29–37. Springer, 1990.
52. Seda Gürses, Arun Kundnani, and Joris Van Hoboken. Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society*, 38(4):576–590, 2016.
53. Gulizar Haciyakupoglu and Weiyu Zhang. Social media and trust during the gezi protests in turkey. *Journal of computer-mediated communication*, 20(4):450–466, 2015.
54. Harry Halpin, Ksenia Ermoshina, and Francesca Musiani. Co-ordinating developers and high-risk users of privacy-enhanced secure messaging protocols. In *Security Standardisation Research: 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings 4*, pages 56–75. Springer, 2018.

55. Fannie Lou Hamer. *Speech Delivered at the Founding of the National Women's Political Caucus.* 1971.
56. Lelia Marie Hampton. Black feminist musings on algorithmic oppression. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, pages 1–1, 2021.
57. Summer Harlow. Social media and social movements: Facebook and an online guatemalan justice movement that moved offline. *New media & society*, 14(2):225–243, 2012.
58. Amy Harmon. Discussing blackness on reddit? photograph your forearm first. *New York Times*, 2019.
59. Christina Harrington, Sheena Erete, and Anne Marie Piper. Deconstructing community-based collaborative design: Towards more equitable participatory design engagements. *Proceedings of the ACM on human-computer interaction*, 3(CSCW):1–25, 2019.
60. Eyako Heh and Joel Wainwright. No privacy, no peace: Urban surveillance and the movement for black lives. *Journal of Race, Ethnicity and the City*, 3(2):121–141, 2022.
61. bell hooks. *Teaching to transgress. Education as a freedom of practice.* Routledge, 1994.
62. bell hooks. *Teaching to transgress.* Routledge, 2014.
63. Philip N Howard, Aiden Duffy, Deen Freelon, Muzammil M Hussain, Will Mari, and Marwa Maziad. Opening closed regimes: what was the role of social media during the arab spring? *Available at SSRN 2595096*, 2011.
64. Philip N Howard and Muzammil M Hussain. *Democracy's fourth wave?: digital media and the Arab Spring.* Oxford University Press, 2013.
65. Distributed AI Resesarch Institute. About. https://www.dair-institute.org/about/, 2024.
66. Amnesty International. Automated apartheid: How facial recognition fragments, segregates and controls palestinians in the opt. 2023.
67. Judy Iseke. Indigenous storytelling as research. *International Review of Qualitative Research*, 6(4):559–577, 2013.
68. Tim Jenkin. *Tim Jenkin: Talking with Vula.* Mayibuye, 1995.
69. Hayley Johnson. # nodapl: Social media, empowerment, and civic participation at standing rock. *Library Trends*, 66(2):155–175, 2017.
70. Tushar M Jois, Gabrielle Beck, and Gabriel Kaptchuk. Pulsar: Secure steganography through diffusion models. *Cryptology ePrint Archive*, 2023.
71. Stephanie T. Jones and natalie araujo melo. We tell these stories to survive: Towards abolition in computer science education. *Canadian Journal of Science, Mathematics and Technology Education*, 21(2):290–308, 2021.
72. Seny Kamara. *COINTELPRO.* Algorithms for the People, 2020.
73. Seny Kamara. Crypto for the people invited talk. https://www.youtube.com/watch?v=_qSja6VpPbQ, 2020.
74. Gabriel Kaptchuk, Tushar M Jois, Matthew Green, and Aviel D Rubin. Meteor: Cryptographically secure steganography for realistic distributions. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1529–1548, 2021.
75. Siddharth Kara. *Cobalt red: How the blood of the Congo powers our lives.* St. Martin's Press, 2023.
76. Merrit Kennedy. More than 1 million "check in" on facebook to support the standing rock sioux. *NPR. org*, 2016.

77. Os Keyes. The misgendering machines: Trans/hci implications of automatic gender recognition. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–22, 2018.
78. Os Keyes. Counting the countless: Why data science is a profound threat for queer people. *Real Life*, 2, 2019.
79. Martin Luther King. Letter from birmingham jail. https://kinginstitute.stanford.edu/sites/mlk/files/letterfrombirmingham_wwcw_0.pdf, 1963.
80. Yasmine Kotturi, Julie Hui, TJ Johnson, and Tawanna Dillahant. Sustaining community-based research in computing: Lessons from two tech capacity building initiatives for local businesses. 2024.
81. IDA B. WELLS Just Data Lab. About. https://www.thejustdatalab.com/about, 2024.
82. Crystal T Laura. *Being bad: My baby brother and the school-to-prison pipeline*. Teachers College Press, 2014.
83. Algorithmic Justice League. About. https://www.ajl.org/about, 2024.
84. Francis LF Lee and Joseph Man Chan. Digital media activities and mode of participation in a protest campaign: A study of the umbrella movement. *Information, Communication & Society*, 19(1):4–22, 2016.
85. Francis LF Lee, Michael Chan, and Hsuan-Ting Chen. Social media and protest attitudes during movement abeyance: A study of hong kong university students. *International Journal of Communication*, 14:20, 2020.
86. Ada Lerner, Helen Yuxun He, Anna Kawakami, Silvia Catherine Zeamer, and Roberto Hoyle. Privacy and activism in the transgender community. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.
87. Ryan Little, Lucy Qin, and Mayank Varia. Secure account recovery for a privacy-preserving web service. *Cryptology ePrint Archive*, 2024.
88. Antony Loewenstein. *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*. Verso Books, 2023.
89. Tetyana Lokot. Be safe or be seen? how russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society*, 16(3):332–346, 2018.
90. Audre Lorde. The master's tools will never dismantle the master's house. *The Personal and the Political Panel*, 1979.
91. Audre Lorde. *Sister outsider: Essays and speeches*. Crossing Press, 1984.
92. Bettina L Love. *We want to do more than survive: Abolitionist teaching and the pursuit of educational freedom*. Beacon Press, 2019.
93. Alex Jiahong Lu, Shruti Sannon, Cameron Moy, Savana Brewer, Jaye Green, Kisha N Jackson, Daivon Reeder, Camaria Wafer, Mark S Ackerman, and Tawanna R Dillahunt. Shifting from surveillance-as-safety to safety-through-noticing: A photovoice study with eastside detroit residents. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2023.
94. Alice E Marwick and Danah Boyd. I tweet honestly, i tweet passionately: Twitter users, context collapse, and the imagined audience. *New media & society*, 13(1):114–133, 2011.
95. Alexandra Mateescu, Douglas Brunton, Alex Rosenblat, Desmond Patton, Zachary Gold, and Danah Boyd. Social media surveillance and law enforcement. *Data Civ Rights*, 27:2015–2027, 2015.

96. Luke P Morrison, Brian Team, Brian Nguyen, Senthil Kannan, Nathan Ray, and Gregory C Lewin. Airchat: Ad hoc network monitoring with drones. In *2017 Systems and Information Engineering Design Symposium (SIEDS)*, pages 38–43. IEEE, 2017.
97. Marcia Mundt, Karen Ross, and Charla M Burnett. Scaling social movements through social media: The case of black lives matter. *Social Media+ Society*, 4(4):2056305118807911, 2018.
98. Andrew Neef. Infrared aerial surveillance used at standing rock to monitor and track protesters. 2019.
99. Rasmus Kleis Nielsen. The labors of internet-assisted activism: Overcommunication, miscommunication, and communicative overload. *Journal of Information Technology & Politics*, 6(3-4):267–280, 2009.
100. Rasmus Kleis Nielsen. Mundane internet tools, mobilizing practices, and the coproduction of citizenship in political campaigns. *New Media & Society*, 13(5):755–771, 2011.
101. Rasmus Kleis Nielsen. Mundane internet tools, the risk of exclusion, and reflexive movements—occupy wall street and political uses of digital networked technologies. *The Sociological Quarterly*, 54(2):173–177, 2013.
102. Safiya Umoja Noble. *Algorithms of oppression*. New York University Press, 2018.
103. Fikile Nxumalo and Kihana Miraya Ross. Envisioning black space in environmental education for young children. *Race Ethnicity and Education*, 22(4):502–524, 2019.
104. Stephen Owen. Monitoring social media and protest movements: Ensuring political order through surveillance and surveillance discourse. *Social Identities*, 23(6):688–700, 2017.
105. Donie O'Sullivan and Dylan Byers. Exclusive: Fake black activist accounts linked to russian government. *CNN Business*, 28, 2017.
106. Arnold Pacey. *The culture of technology*. MIT press, 1985.
107. Elena Pagnin, Sofía Celi, and Akira Takahashi. *On Creating a More Inclusive and Supporting Community*. 2023.
108. Jason Parham. Russians posing as black activists on facebook is more than fake news. *Retrieved August*, 22:2018, 2017.
109. Lorgia García Peña. *Community as rebellion: A syllabus for surviving academia as a woman of color*. Haymarket Books, 2022.
110. Thomas M Philip, Megan Bang, and Kara Jackson. Articulating the "how," the "for what," the "for whom," and the "with whom" in concert: A call to broaden the benchmarks of our scholarship. *Cognition and Instruction*, 36(2):83–88, 2018.
111. Lucy Qin, Leah Namisa Rosenbloom, and Kris Shrishak. Where do threat models come from? challenging implicit assumptions. https://namisa.art/Threat_Modeling_Mismatches_condensed_slides.pdf, 2023.
112. Anjana Rajan, Lucy Qin, David W Archer, Dan Boneh, Tancrede Lepoint, and Mayank Varia. Callisto: A cryptographic approach to detecting serial perpetrators of sexual misconduct. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, pages 1–4, 2018.
113. Phillip Rogaway. The moral character of cryptographic work. *Cryptology ePrint Archive*, 2015.
114. Kevin Roose. Social media giants support racial justice. their products undermine it. *The New York Times*, 2020.
115. Leah Namisa Rosenbloom. Toward secure social networks for activists. In *Moving technology ethics at the forefront of society, organisations and governments*, pages 491–502. Universidad de La Rioja, 2021.

116. Leah Namisa Rosenbloom. Activists want better, safer technology. *arXiv preprint arXiv:2209.01273*, 2022.
117. Leah Namisa Rosenbloom. A living framework for abolitionist teaching in computer science. In *Proceedings of the ACM Conference on Global Computing Education Vol 1*, pages 133–139, 2023.
118. Herman Saksono and Andrea G Parker. Socio-cognitive framework for personal informatics: A preliminary framework for socially-enabled health technologies. *ACM Transactions on Computer-Human Interaction*, 31(3):1–41, 2024.
119. Aman Sium and Eric Ritskes. Speaking truth to power: Indigenous storytelling as an act of living resistance. *Decolonization: indigeneity, education & Society*, 2(1), 2013.
120. Marko M Skoric, Nathaniel D Poor, Youqing Liao, and Stanley Wei Hong Tang. Online organization of an offline protest: From social to traditional media and back. In *2011 44th Hawaii International Conference on System Sciences*, pages 1–8. IEEE, 2011.
121. Lawrence C Soley. *Leasing the ivory tower: The corporate takeover of academia.* South End Press, 1995.
122. Daniel G Solórzano and Tara J Yosso. Critical race methodology: Counter-storytelling as an analytical framework for education research. *Qualitative inquiry*, 8(1):23–44, 2002.
123. Amory Starr, Luis A Fernandez, Randall Amster, Lesley J Wood, and Manuel J Caro. The impacts of state surveillance on political assembly and association: A socio-legal analysis. *Qualitative Sociology*, 31:251–270, 2008.
124. LaToya Strong, Atasi Das, and Danny Morales-Doyle. Abolition science praxis (part 1). https://www.abolitionscience.org/home/2018/11/27/abolition-science-praxis-pt-2-dr-danny-morales-doyle, 2018.
125. LaToya Strong, Atasi Das, and Robert P. Robinson. The history of abolition. https://www.abolitionscience.org/home/2018/9/4/historically-grounding-abolition, 2018.
126. Equity The TREE Lab: Examining Technology, Race and Ethics in Education. Home. https://tree.northwestern.edu/, 2024.
127. Yannis Theocharis, Will Lowe, Jan W Van Deth, and Gema García-Albacete. Using twitter to mobilize protest action: online mobilization patterns and action repertoires in the occupy wall street, indignados, and aganaktismenoi movements. *Information, Communication & Society*, 18(2):202–220, 2015.
128. Mark Tremayne. Anatomy of protest in the digital era: A network analysis of twitter and occupy wall street. In *Social Networks and Social Movements*, pages 110–126. Routledge, 2016.
129. Emiliano Treré. Reclaiming, proclaiming, and maintaining collective identity in the #yosoy132 movement in mexico: An examination of digital frontstage and backstage activism through social media and instant messaging platforms. *Information, Communication & Society*, 18(8):901–915, 2015.
130. Emiliano Treré. The banality of whatsapp: On the everyday politics of backstage activism in mexico and spain. *First Monday*, 25, 2020.
131. Sojourner Truth. Ain't i a woman? *Feminist theory: A reader*, page 79, 1851.
132. Eve Tuck and K Wayne Yang. Toward what justice. *Describing diverse dreams of justice in education. Abingdon: Routledge*, 2018.
133. Zeynep Tufekci and Christopher Wilson. Social media and the decision to participate in political protest: Observations from tahrir square. *Journal of communication*, 62(2):363–379, 2012.

134. Temple Uwalaka, Scott Rickard, and Jerry Watkins. Mobile social networking applications and the 2012 occupy nigeria protest. *Journal of African Media Studies*, 10(1):3–19, 2018.
135. Sebastián Valenzuela. Unpacking the use of social media for protest behavior: The roles of information, opinion expression, and activism. *American behavioral scientist*, 57(7):920–942, 2013.
136. Suresh Venkatasubramanian, Timnit Gebru, Ufuk Topcu, Haley Griffin, Leah Namisa Rosenbloom, and Nasim Sonboli. Community driven approaches to research in technology & society ccc workshop report. 2024.
137. Shirin Vossoughi and Sepehr Vakil. Toward what ends? a critical analysis of militarism, equity, and stem education. In *Education at war*, pages 117–140. Fordham University Press, 2018.
138. Kandrea Wade, Jed R Brubaker, and Casey Fiesler. Protest privacy recommendations: An analysis of digital surveillance circumvention advice during black lives matter protests. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2021.
139. Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. " we hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.
140. Isabel Wilkerson. *Caste: The origins of our discontents*. Random House, 2020.
141. Tarun Kumar Yadav, Devashish Gosain, and Kent Seamons. Cryptographic deniability: a multi-perspective study of user perceptions and expectations. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3637–3654, 2023.
142. Tukufu Zuberi. *Thicker than blood: How racial statistics lie*. U of Minnesota Press, 2001.