TECHNOLOGIES FOR LIBERATION

Toward Abolitionist Futures

RESEARCH ACTION DESIGN
ASTRAEA LESBIAN FOUNDATION FOR JUSTICE

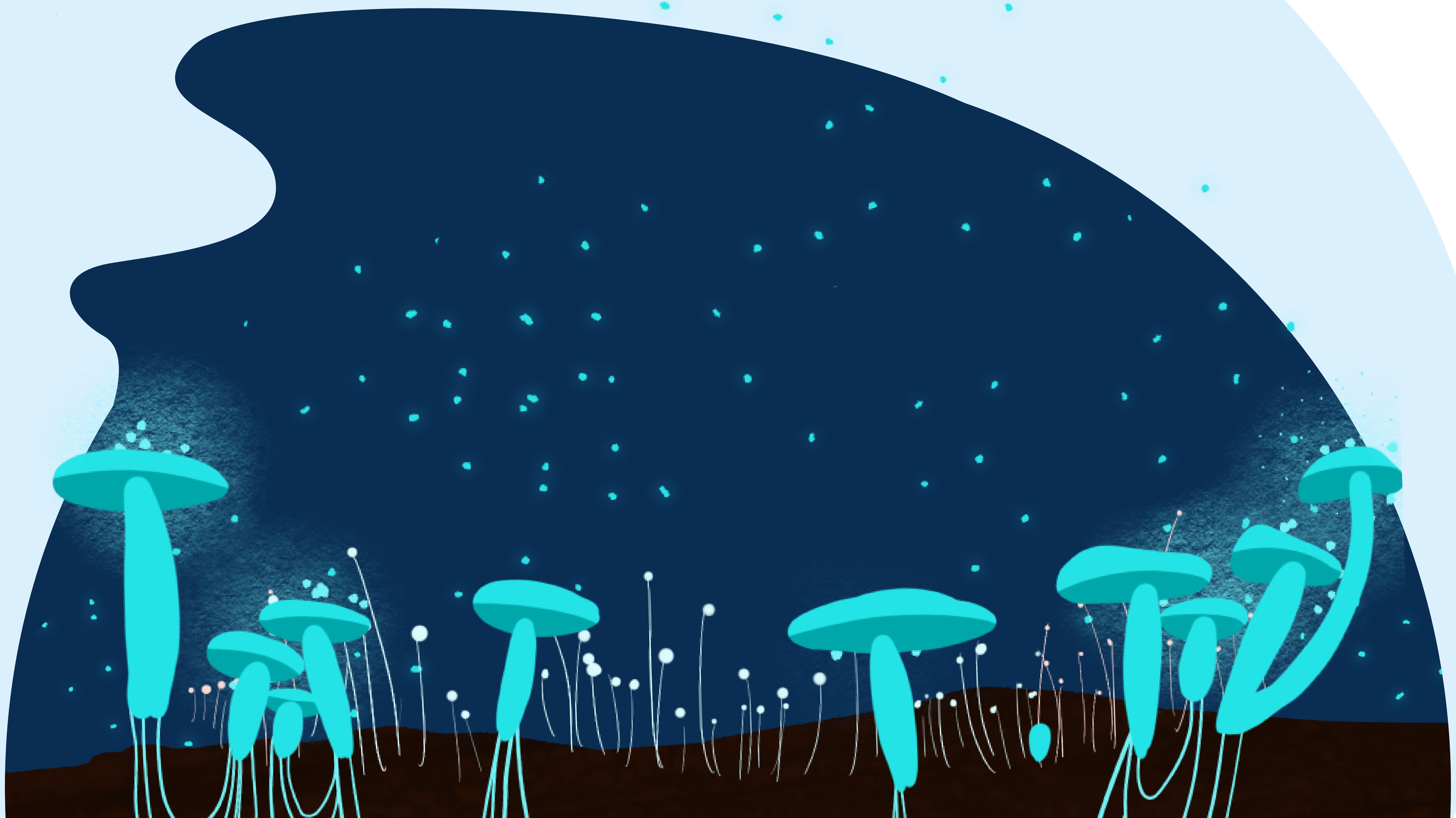
RESEARCH ACTION DESIGN

ASTRAEA LESBIAN FOUNDATION FOR JUSTICE

TECHNOLOGIES FOR LIBERATION

Toward Abolitionist Futures

info@astraeafoundation.org - www.astraeafoundation.org



GRATITUDE TO OUR PARTNERS

mijente

MediaJustice

Detroit Community Technology Project

hacking//hustling

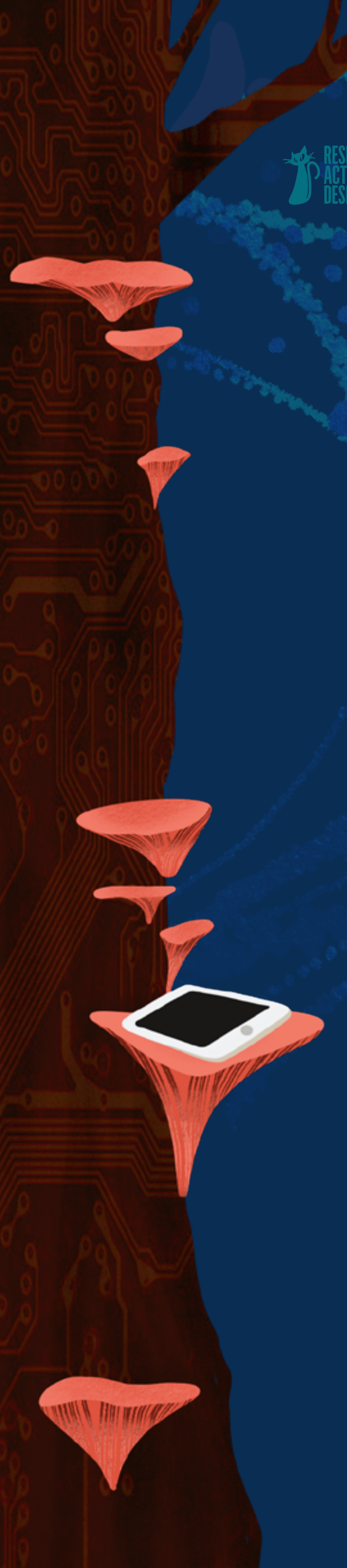
DETROIT DIGITAL JUSTICE COALITION

Digital Defense Playbook
Community Power Tools for Reclaiming Data

STOP LAPD SPYING!

RESILIENT JUST TECHNOLOGIES

TABLE OF CONTENTS



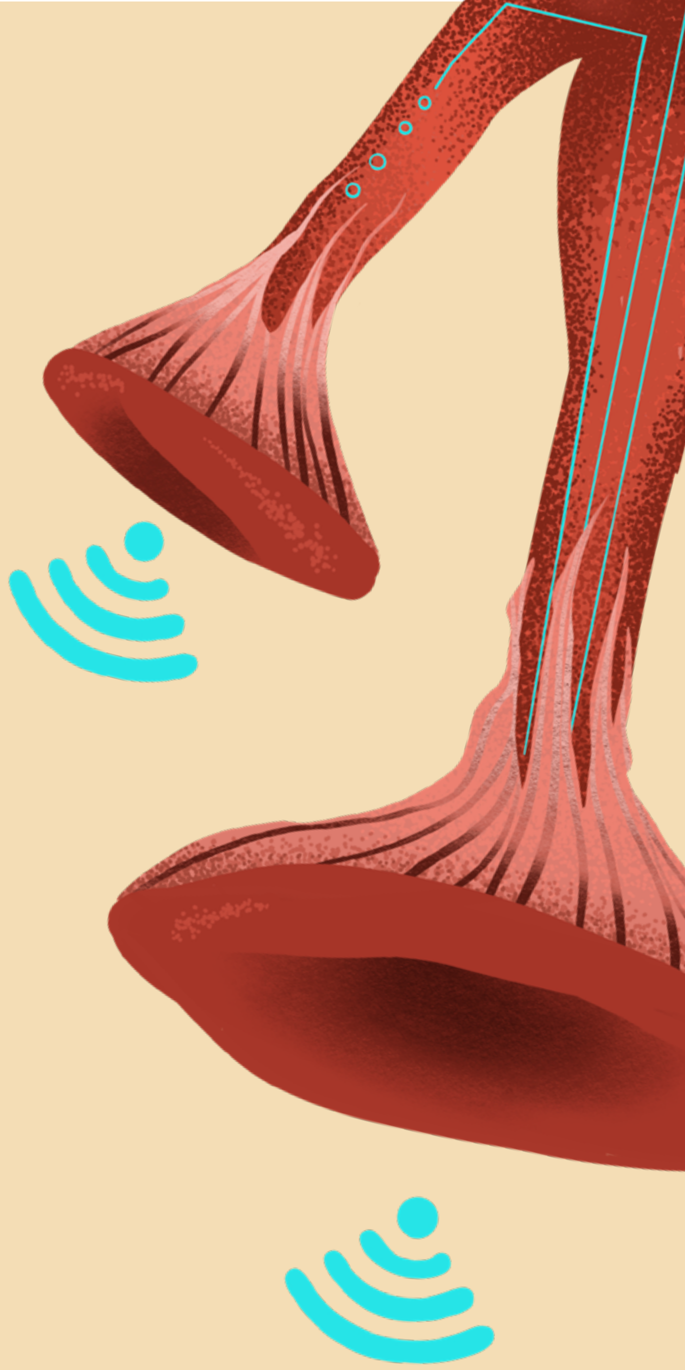
FOREWORD

EXECUTIVE SUMMARY

TECHNOLOGY & CRIMINALIZATION

MOVEMENT STRATEGY, RESPONSE, & RESISTANCE

FOREWORD



Dear Friend,

We are being called upon to radically reimagine our societies: to collectively envision a future that is safe for us all; a future that does not tolerate the violent surveillance, policing and imprisonment of our communities. In recent months, it has been incredibly inspiring to witness dialogue around abolition and the defunding of police become more mainstream in the United States. Simultaneously, the aggressive expansion of the webs of criminalization, surveillance, racism, and white supremacy continue to be a terrifying reality for many of our communities. The global COVID-19 pandemic – which disproportionately impacts LGBTQI, incarcerated, low-income, migrant, Native, Black, and Latinx communities – also disproportionately demands their labor at the frontlines, despite these same populations being among the most vulnerable to housing, food, health care and employment insecurity.

Technologies for Liberation: Toward Abolitionist Futures is rooted in the groundwork of visionary abolitionists who fight to end policing, criminalization, and carceral logics and technologies in all their forms. It holds the central idea of abolition as a vision and a political strategy. Hope and a more just vision for the future lies within the powerful resistance and abolitionist work of communities of color here in the United States. Movement organizers respond to increasing levels of surveillance and state violence with incredible ingenuity and resilience. The growth of community-controlled technologies, of mutual aid and care support networks remind us: surveillance, prisons and police don't keep us safe. **We keep us safe**.

This report emerged out of the need to better understand the ways in which Queer, Trans, Two-Spirit, Black, Indigenous, and People of Color (QT2SBIPOC) communities are disproportionately impacted by surveillance and criminalization at all levels—from the state-endorsed to the corporate-led—and to resource these communities to push back. Our research amplifies the movement interventions and responses that organizers are employing to create safety for the people they serve. Committed to their vision of collective liberation, they are pushing the boundaries to decolonize technology and place it in service of movement building. In doing so, organizers are shifting the narrative around safety and violence/justice.

Yet, despite the fact that their work is groundbreaking and their resistance is powerful beyond measure, there is an immense gap in resourcing for this type of liberatory organizing. Philanthropy has an essential role to play in funding, fueling, and sustaining those working for liberation at the intersections of technology and criminalization. It also holds a responsibility to break down the silos in funding of movement building, technology, criminal justice, racial justice, climate change, and more. With this report, we challenge you to engage more deeply with the work of brilliant organizers and movement technologists who are forging visions for demilitarized, community-driven technologies to sustain and support the future of movements for liberation. We invite you to prioritize support for those who are leading responses rooted in abolition, and imagining and building systems of care and interdependence, grounded in transformative justice and healing justice—and we offer concrete ways to do so.

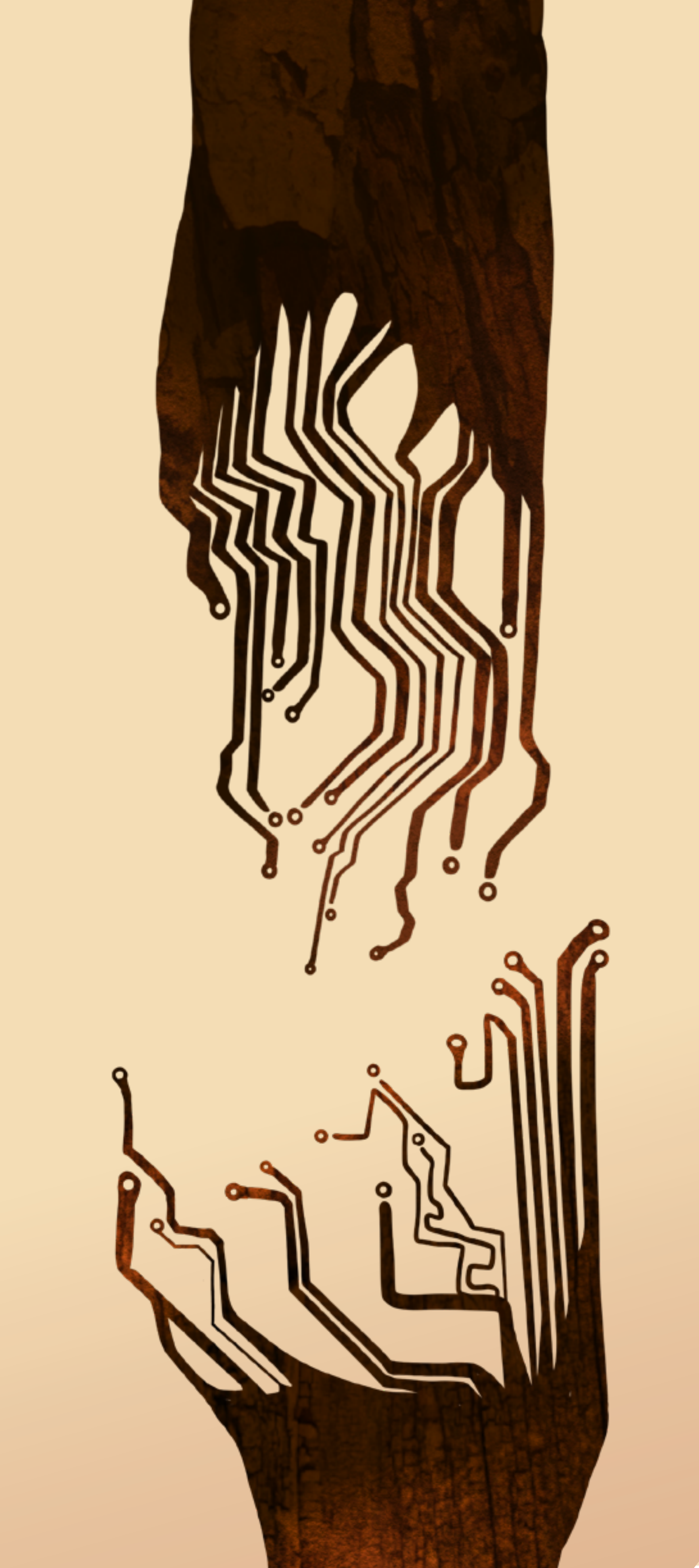
Technologies for Liberation: Toward Abolitionist Futures is based on rich interviews and engagement with movement technologists, organizers, researchers, and policy advocates about what liberation from surveillance and criminalization can actually look like. We thank them for contributing their invaluable time and insights. By no means is this report a complete picture of the myriad issues surrounding technology and criminalization. Astraea and Research Action Design (RAD) created this report as a resource for funders to understand what is at stake and what opportunities exist to support critical organizing at the intersections of decriminalization and technology. Throughout this report, you will read about surveillance, carceral technologies, criminalization, and policing. In some instances, we speak about these practices in tandem, and, in others, we hone in on one to provide deeper insight, but please bear in mind that these processes and practices—and their consequences—are inextricably linked.

We honor and are grateful for the legacy of abolitionist activists, organizers, and policy writers, whose work has challenged us to step away from the carceral state and a politics of punishment, and instead imagine transformative responses to injustice. We are delighted to share this report with all of you as a roadmap to understand both the impacts of surveillance and criminalization, along with our collective efforts of better supporting those who have a clear vision of the possibilities for transformation and justice.

In solidarity,

Brenda Salas Neves,
Astraea Senior Program Officer

Mihika Srivastava,
Astraea Communications Program Officer



EXECUTIVE SUMMARY

Introduction

Since the founding of the United States, there has been a dovetailing of technology and criminalization targeted at communities of color. Historically, the state used technology as a tool to repress movement-building efforts and amplify the systems of oppression and violence that communities of color in the US experience. Today's surveillance technologies and practices have roots in older forms of policing, incarceration, and colonial control dating back to the inception of the US nation-state. The logic behind predictive policing software derives from slave patrols, lantern laws, and stop and frisk.[1] Facial recognition algorithms can be traced back to the eugenics movement.[2] Biometric data monitoring was first introduced with colonization.[3] In the late twentieth and twenty-first centuries, technological developments have accelerated the US government's monitoring of communities of color, and, specifically, progressive and radical Black, Indigenous, and QT2SBIPOC movements. By relying on racist tropes and fear, the state has been able to continue these actions through invoking 'white slavery' myths, and rationalize mass surveillance laws (such as the PATRIOT ACT) by invoking fears of 'foreign' attacks on domestic soil. These historical connections make it plain that the state's racist use of technology for the purposes of criminalization is not new and is cemented into the foundation of this country. What is new, however, is the rate and scale at which the development of surveillance technology is propelling mass criminalization in the US and Puerto Rico.

Mass surveillance has resulted in the hyper-policing of entire communities by law enforcement and government agencies.[4] Mass incarceration in the US emerged within a context where surveillance served as a racializing mechanism of white supremacist statecraft.[5] Surveillance practices established a way of coding enslaved African bodies as criminal and therefore subject to constant oversight (from which the term surveillance derives), confinement, and punishment in the form of slave patrols and biometric tracking.[6] Safety and security are often conflated within state narratives to justify the use of these mass surveillance and other carceral technologies on the public. As we see with police surveillance of organizers, these narratives frame state-surveillance technologies as "smarter" methods to protect public safety and national security from a perceived 'threat'. The racial biases of the creators are deeply embedded within the technologies themselves. Mass criminalization upholds and bolsters this network of practices with emergent surveillance technologies that have expanded the reach of the carceral state beyond physical confinement. In its current manifestation, mass incarceration is understood to be a set of policies that has caused an enormous rise in the number of Black and brown people in prisons and immigration detention centers.[7] In 2020, more than two million people are currently incarcerated due to this system[8].

The collaboration of state and corporate actors has pushed mass criminalization into overdrive. The longstanding secretive state-based tactics used to track and surveil migrant communities,[9] protestors, and sex workers,[10] serve as an example of the ongoing threats that communities face. The current US administration's increased attacks on open-source technologies that movement organizations rely on for safety intensifies the threat of state-based violence.[11] "Surveillance capitalism" propels and extends the structure of mass criminalization of communities of color in the United States.[12] For example, in recent months, as a response to the COVID-19 pandemic, governments have begun using contact tracing technology—the use of personal location data on cell phones—to track the virus.[13] Without safeguards, this technology can be repurposed to further surveil and repress organizers, particularly at protests[14]. Internet shutdowns in the Global South in response to COVID-19 are further examples of the ways in which governments have co-opted technology to repress citizens, exacerbating inequalities in accessing timely health and other critical information.[15]

> “
>
> We're trying to think about how to confront mass criminalization, recognizing there are two million people in cages, but seven million more under some kind of surveillance. There are other systems through which people are criminalized, the child welfare and immigration systems, so many ways that criminalization funnels people into those cages but also creates cages outside of prisons.
>
> ”
>
> **researcher and policy analyst**

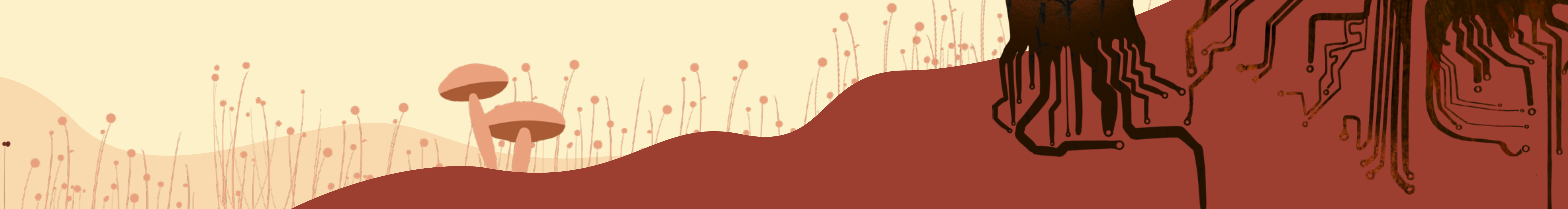
Frontline organizers are responding to these attacks with resilience and vision, creating intersectional strategies that shift power into the hands of the people who are historically denied it. They advocate for the investment in community-based solutions over carceral ones, while simultaneously fighting to demilitarize and defund the police[16] and move resources to meet community needs. The massive mobilization in support of Black Lives in 2020 and calls to #DefundPolice are built upon years of Black-led organizing efforts to redefine public safety and accountability as needing to be led by communities rather than law enforcement agencies. For example, the recent corporate moratorium of facial recognition technologies being sold to police by companies like IBM, Amazon, and Microsoft illustrates a powerful movement win that is a direct result of organizing efforts.[17]

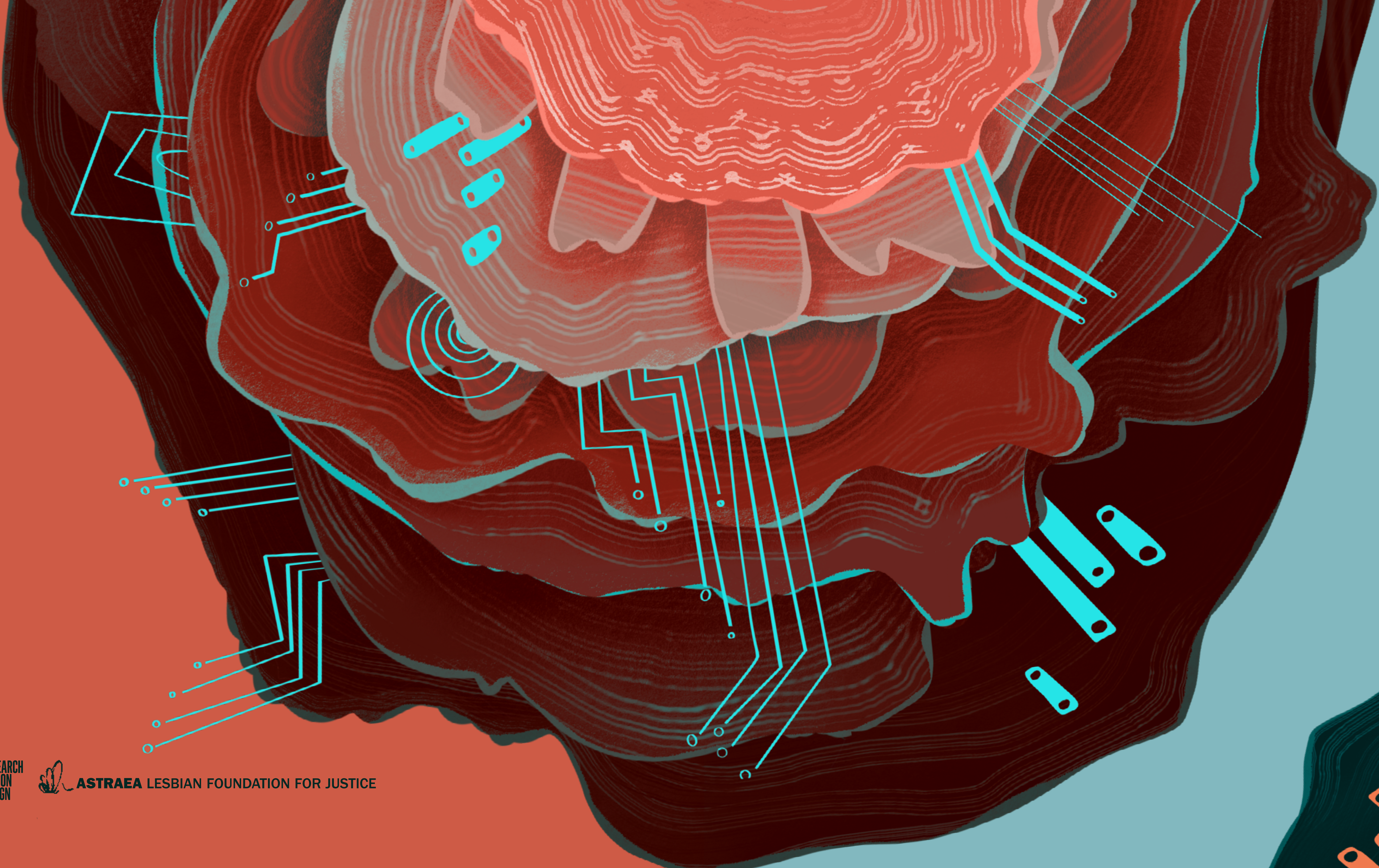
Drawing from historical lessons and legacies of resistance, many organizers use an abolitionist approach which strives to eliminate policing and prisons and transform the social conditions that lead to and feed oppressive, violent systems of policing, punishment, and incarceration.[18] The movement organizations highlighted in this report are reshaping the narrative around what it means to keep their communities safe and who gets to define

what safety looks like. They are expanding the definitions of technology, and helping communities control and safeguard their personal data from the systems built to exploit it. Since this data is often used by the state to incriminate and bring harm to individuals' bodies, such work is not merely valuable, but central to resistance and freedom.

However, there is a dearth of long-term funding to support the creation and development of movement-led infrastructure and to partner with these communities to design, test, and evaluate new technologies. Shifting power to communities to imagine abolitionist narratives of safety is critical. Calls for sustainable and long-term funding for political education, trauma-informed resources, movement-based research, safer communications, movement-technologies, and support for a free and open web, are needed now more than ever. This work requires help from forward-thinking funders who understand the need to couple support for innovation with support for the grassroots organizing that creates it.

This report, *Technologies for Liberation: Toward Abolitionist Futures*, lifts up the power of movement building and the ways in which organizers are innovating to create safe technologies and systems for the people they serve, centering QT2SBIPOC communities. This research is based on in-depth interviews with movement organizers, researchers, policy advocates and technologists; these and other data were collaboratively analyzed during a 3-day participatory analysis convening held in San Juan, Puerto Rico in 2019. Through these and other conversations, we identified key findings about some of the ways in which movements in the United States and Puerto Rico combat technologies in the service of criminalization, and how they are building transformative futures. We share our recommendations for funders prepared to support communities proactively transforming and re-imagining new futures outside of criminalization.

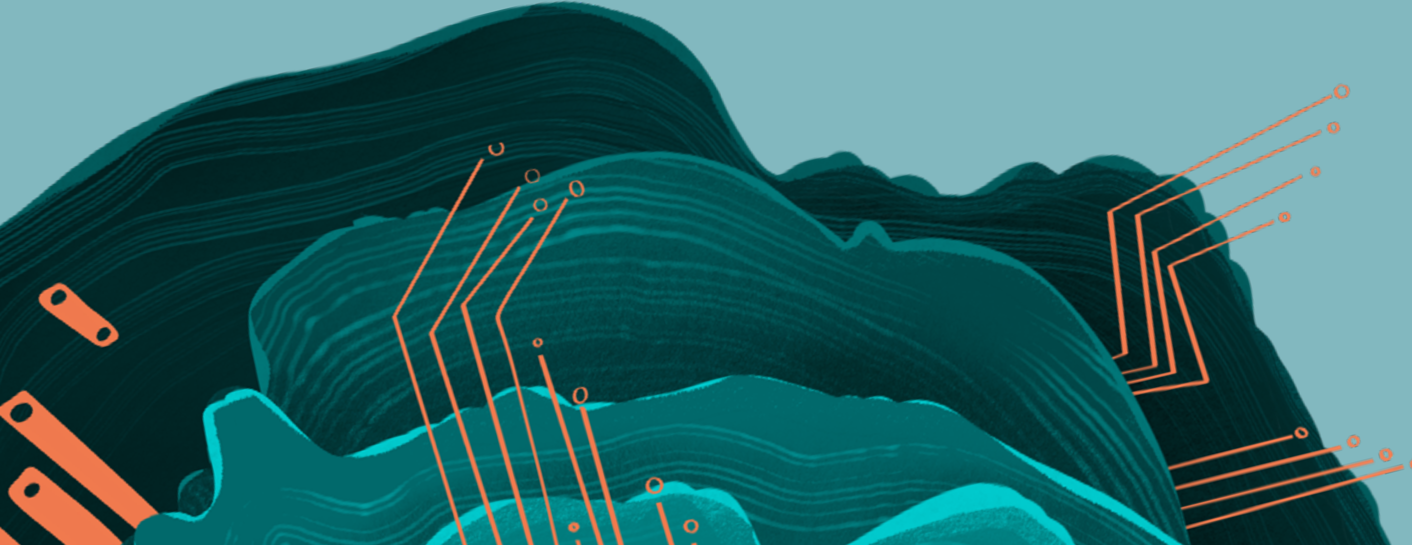




Key Findings

Technologies designed to collect personal information are deployed to control, police, surveil, and limit the flow of money and power to QT2SBIPOC communities.

These systems of surveillance range from government databases, police body cameras, private security cameras, social media targeted ads, and consumer profiles to predictive policing. These technologies are often deployed without community knowledge, consent, or accessible understanding of the interactions between the state and private companies. Private corporations such as Amazon, IBM, Microsoft, Salesforce, and Palantir are profiting from technologies used in the development and deployment of tech software to target, detain, and deport migrant communities. At the same time, the criminal justice system is increasingly reliant on artificial intelligence (AI) and is rapidly expanding the reach of the carceral state. Carceral technologies move into public spaces through the expansion of e-carceration where personal technologies and surveillance are being offered as 'alternatives' to incarceration.



Safety and security are often conflated within state narratives to justify the use of surveillance technologies on the public.

As we see with police surveillance of organizers, these narratives frame state-surveillance technologies as "smarter" methods to protect public safety and national security from a perceived 'threat'. When we investigate who has the cultural and political capital to make these tools, we understand how the racial biases of the creators are deeply embedded within the technologies themselves. Communities of color are increasingly hyper-policed with these technologies and entangled within the criminal justice system, perpetuating the racist history of policing. There are myriad ways that technology amplifies mass criminalization through a process that may first appear to be 'unbiased', but is used for criminalizing and surveilling communities of color. This technology includes artificial intelligence such as facial recognition, predictive policing software, risk assessment algorithms, and platform moderation and surveillance tools like drones, automated license plate readers, and data collection and sharing via third-party agreements between government agencies and private tech companies.

Movements are redefining safety for their communities.

They are building transformative visions through the use of abolitionist frameworks and anti-carceral technologies. Organizers are transforming relationships with one another and within communities, with technology, with corporations, with the police and the state, dismantling a capitalist system that is rooted in oppression. Abolition is this vision.

Movements are responding to the shifting landscape of carceral technologies with community-centered, intersectional strategies.

From policy advocacy, to research, to political education, to new emergency responses, to movements led by communities of color are fighting the impacts of criminalization and surveillance in their communities. For example, sex worker organizers must quickly adapt to losing access to financial technologies and adopting new ones while organizing and sharing money for mutual aid. Black and Latinx feminist organizations in the South identify intensifying digital security threats as an emerging battleground for reproductive justice, and are holding community-led trainings on physical and digital security strategies to defend against right-wing doxing and website hacking. Migrant justice organizers describe how the border has become a primary testing ground for new surveillance technologies, and they are running powerful advocacy campaigns to demand accountability from private technology companies invested in the detention of migrant communities.

Movements are creating interdependent care networks to disrupt state-led conceptions of safety that justify the use of surveillance technologies on the public.

This work challenges the state's reliance on punishment via the use of prisons, policing, and surveillance. The holistic technologies movement organizers use include rapid response networks, police de-escalation, bad-date lists, intergenerational healing and storytelling circles, as well as the call for redirecting funding from the prison industrial complex into community resources like health, education, and anti-violence programs. By centering healing justice, communities are creating rapid response networks to care for each other after acts of police brutality. These networks include community members who are trained as listeners, police de-escalators, street medics, jail support, and healers. These strategies highlight the power of community organizing and building new transformative models of care and safety.

Movements are centering decarceration and decriminalization strategies.

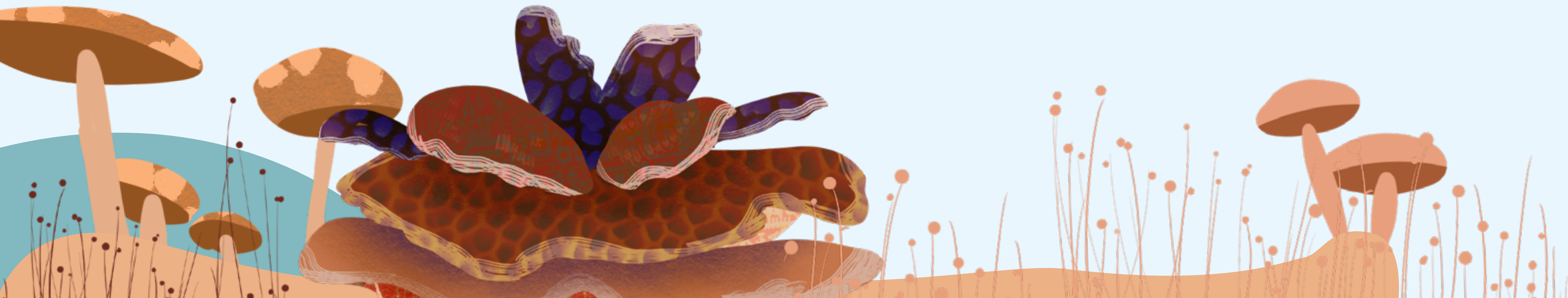
From fighting e-carceration and the use of "smarter" technology to further criminalize communities, to cash bail being replaced by carceral penal technologies like risk-assessment algorithms, movement organizations are standing against reforms to the criminal legal system, and are seeking to dismantle the prison industrial complex altogether.

Movements are reimagining technology and creating more sustainable ecosystems as tools for liberation.

Organizers are building *movement technologies* in response to the increased use of technology as a tool for criminalization. Viewing technology as limited to digital resources, machines, and tools stems from white supremacy and erases and invisibilizes the technologies of radical community organizing. Through broadening our understanding of technology, we are able to more clearly see how the state deploys technology to oppress, and how communities fight back and use technology for liberation. Centering *design justice*, community-driven technology, and holistic digital and physical care, organizers are re-envisioning technology to support movement values such as consent, ownership, community self-determination, access, privacy, and resource sharing. Organizers are creating popular education programming to help community members learn about the hidden flow of personal data between government and corporations and other private interests, creating interactive workshops that aim to break down digital literacy barriers and bring data collection methods into the physical and tangible realm.

Movements are developing infrastructures and platforms to combat surveillance and meet the needs of their communities.

Organizers are using justice-based principles to envision alternative liberatory futures and co-create accessible and relevant technology tools with their communities. From solar-powered local wireless mesh networks to high speed internet antennas, movement technologists are helping communities control and protect their data while staying connected in times of crisis and rebuilding. For example, organizers in Puerto Rico connect the need for community-owned technology infrastructure with decolonizing recovery efforts and creating political change and stability in the Puerto Rican archipelago. Organizers are also employing feminist data collection strategies and participatory community-based research methods to assess the needs of their community so often misunderstood or ignored by the academy and policy makers. We see this in the sex working community, as they assess the damage done by internet legislation like FOSTA, which signed under the pretense of stopping trafficking, but – in reality – increases surveillance, criminalization, and violence against sex workers, survivors, and sex-working survivors.



Movements are navigating the contradictions and barriers of using mainstream, open source, and solidarity platforms.

Organizers navigate various contradictions when it comes to employing technology for building campaigns, relationships, and visibility. Organizations must weigh the potential benefits and harms of using mainstream platforms, which have extensive reach but carry the risk of exposing members to corporate and state surveillance, or utilizing open source and solidarity platforms, which have less reach but may offer more protection. Presently, organizers employ both options.

At present, movements face significant financial barriers to implementing and maintaining digital safety strategies and community-owned technologies.

Movement organizations lack the resources necessary to develop their own technologies when they feel they are most needed. Many lack sufficient resources to upgrade their existing equipment and software in order to use mainstream tools safely and securely. Funding barriers may also reinforce movement organizations' reliance on corporate-owned technologies and experts from outside of the communities they serve. Organizations are rarely supported to maintain in-house technical staff or to access trusted movement technologists.

Recommendations for Funders

Few funders address these issues head-on. Social justice funders are working to deepen their understanding of technology's harms and possibilities. Technology funders may not bring a social justice or anti-criminalization lens. The complexity of how lives are mediated by criminalizing technologies calls for an interdisciplinary approach to funding, and requires all funders to stretch beyond our philanthropic silos, think holistically, and find creative ways to deepen support for the organizations building the transformative futures we need.

Here are Astraea's recommendations for other funders:

Invest in abolitionist futures

Ending the criminalization of QT2SBIPOC communities requires dismantling the state's architecture of surveillance and the systems upon which it depends, from policing to prisons to immigration enforcement. Movement organizations are organizing in and with their communities to keep people safe and meet the needs of the community.

Increase core support to organizations working to abolish or ban technologies used to criminalize and police communities with military equipment and tactics. When making a grant, some helpful questions to guide your grantmaking decisions include:

- Does this grant challenge the existence of criminalizing systems?
- Does this grant reject surveillance technology as a way to ameliorate the violence of a criminalizing system?
- Does this grant promote community-based narratives of safety?
- Does this grant aim to curtail expansion of the state's network of surveillance?
- Does this grant support efforts to divest in structures of criminalization and reinvest those resources into community-centered projects for safety and wellbeing?
- Does this grant uphold "abolitionist steps in policing" to promote community safety, or does it default to "reformist reforms"?[19]
- Does this grant prioritize holistic safety as a framework that emphasizes sustainability and centers community-based safety[20] and well-being?

Invest in organizations with multi-year, sustained funding. Ending the surveillance and criminalization of communities will not happen overnight. Organizations need flexible funding that enables communities to sustain resistance and build alternatives.

Listen to and follow how organizations' define and measure impact. Expand how you measure impact. Activists need flexibility around what counts as a concrete "win." Their definitions of "wins" also often include building the knowledge, resilience, and power of directly impacted communities. Activists are organizing under constantly evolving and developing levels of surveillance and criminalization. Funding streams need to be flexible to keep up with the rate of new technologies and means of surveillance. This paradigm-shifting work takes time and requires many steps.

Fund healing justice.

Healing builds individual and collective power and resilience. Invest in collective care, wellness, and healing justice strategies. The trauma experienced by people who have been criminalized must be addressed to build lasting community power.[21]

Center the knowledge and vision of frontline movement organizers.

Movement organizers are the experts of their experiences and know better than anyone what they need to sustain their work.

- **Ask grantee partners directly about their needs** around holistic safety and movement technology. Then work to meet them.
- **Respect and support collective community-based reparations work** that doesn't lead to further criminalization.
- **Learn from global movements and Global South organizations** that have deep expertise in organizing under oppressive regimes and deploying community-based technology in response to state surveillance.

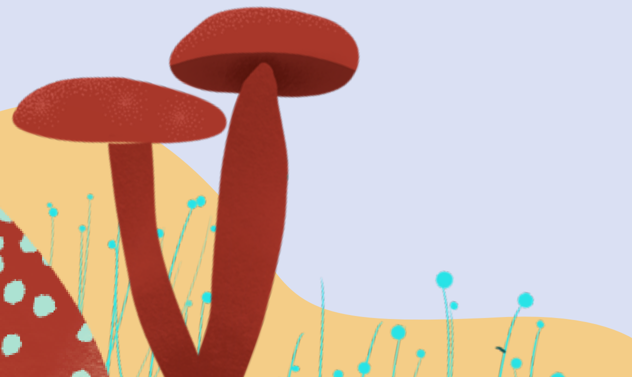
Invest in political education and career pipelines for community-based technologists.

Movement organizations, organizers and technologists play an important role in helping community members navigate their relationship to technology, both to reduce the structures and harms of surveillance and to utilize technology for grassroots organizing.

- **Fund ongoing political education for activists, funders, technologists, and policymakers around issues of privacy, safety, and security.** These issues are complex, constantly changing, and often hidden and inscrutable. Everyone—especially the communities most impacted by criminalization—needs to better understand the impact of technology and criminalization on individual lives and on whole communities.

- **Invest in movement-based community research** that deepens understanding of the role of surveillance technologies and builds communities' capacity to resist them.

- **Build and broaden the long-term technology capacity of movements, investing in people.** Fund community-centered technology professional development and mentorship for people within communities and organizations to train to become technologists for their communities and organizations. One-off digital security training does not get the job done. Having more community technologists supports organizational digital security and mitigates the risk of burnout for individual technologists.



Fund the development, implementation and long-term maintenance of movement technology.

Grounded in self-determination, organizers are creating and adapting community-owned technology and infrastructure to respond to their communities' needs.

- **Provide dedicated funding for movement technology as part of larger organizing and sustainability strategies.** Developing community-centered technology tools for movement work is resource intensive but builds capacity for sustainable movement work.

- **Sustain movement technology beyond the startup phase and norms of startup culture.** Developing any technology to the point of usability and adoption is a long term project that necessitates long term funding beyond the start-up phase. Long term support is needed to support the engineering side of creating platforms and tools and the organizing side of working with community members to design, test, evaluate and deploy. Funding needs to be fluid to reflect the rapidly evolving surveillance technologies and the relationships heavily policed communities have with them.

- **Support grantee partners' technology needs.** Organizations' needs include their efforts to shift from mainstream corporate platforms to more secure digital spaces and practices, operational technology and technical innovations.

Tighten your own safety protocols and policies to reduce risks to grantee partners, their allies and their communities.

Ensure that application forms are encrypted, reconsider what data is collected and whether people are able to apply without revealing personally identifying information that might put them at risk or make communities most at risk of criminalization more hesitant to apply. Use holistic security practices across the funding landscape to decrease grantees' risks of being surveilled. Consider the safety and security of the technology and platforms used for grant applications and other interactions. Be sensitive to the particular surveillance risks that organizations and potential grantee partners may face.

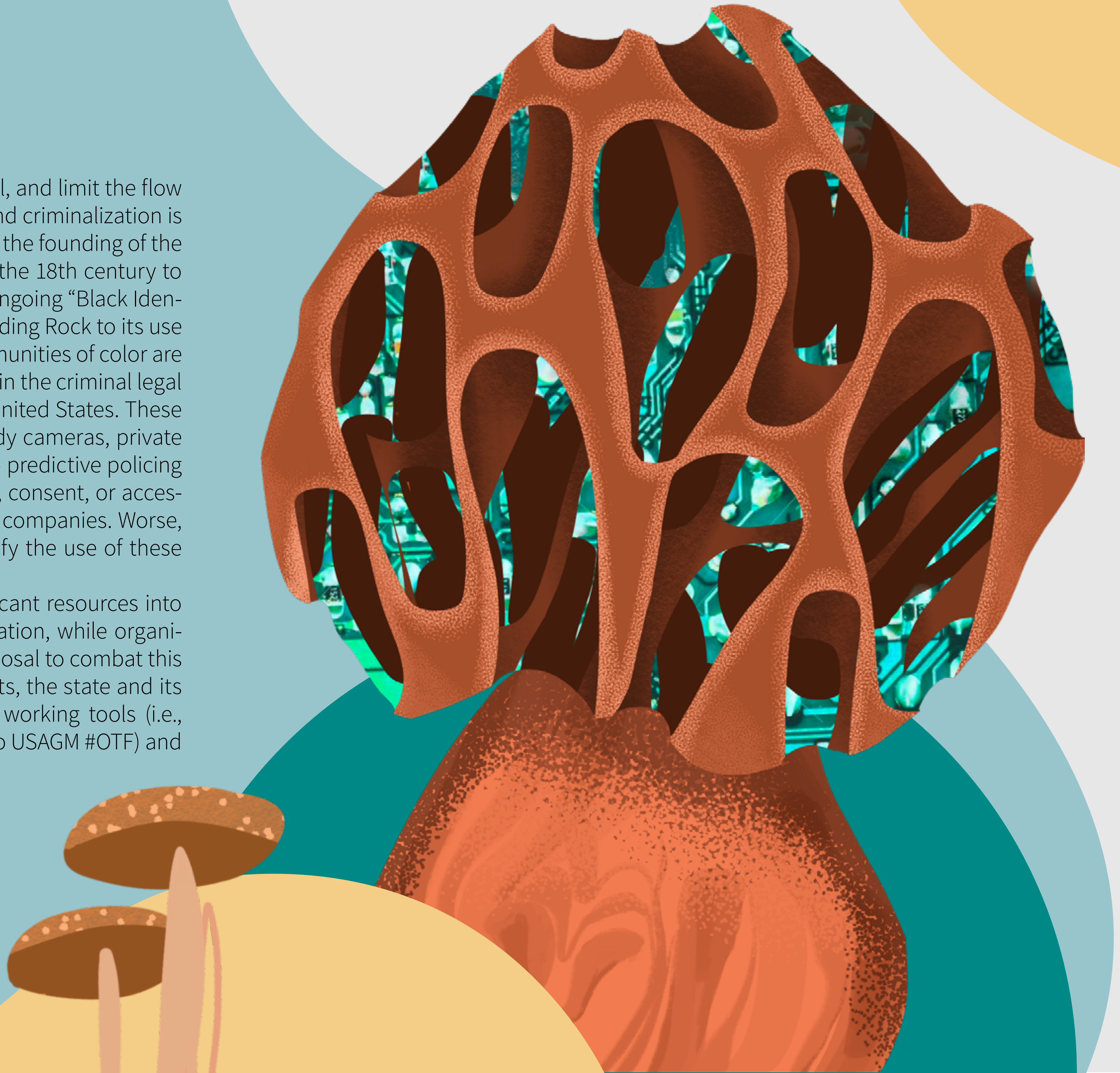
Support interdisciplinary funding streams that transcend philanthropic silos.

Funding needs to reflect the complexities of the ways that marginalized communities are policed and surveilled. This means that funding needs to come from technology, LGBTQI, and racial justice funders.

TECHNOLOGY & CRIMINALIZATION

The carceral state deploys technologies to control, police, surveil, and limit the flow of money and power to communities. The dovetailing of technology and criminalization is not new—it is something communities of color have experienced since the founding of the US. This has included methods from the lantern surveillance laws of the 18th century to COINTELPRO in the 1960s, from the Federal Bureau of Investigation's ongoing "Black Identity Extremist" designation and its past surveillance of protests at Standing Rock to its use of facial recognition software to identify activists and protestors. Communities of color are increasingly hyper-policed with these technologies and entangled within the criminal legal system, perpetuating the racist history of policing and prisons in the United States. These systems of surveillance range from government databases, police body cameras, private security cameras, social media targeted ads, and consumer profiles to predictive policing and beyond. Most are often deployed without community knowledge, consent, or accessible understanding of the interactions between the state and private companies. Worse, safety and security are often conflated within state narratives to justify the use of these surveillance and other carceral technologies on the public.

Government agencies and private tech companies invest significant resources into developing surveillance technology to broaden the web of criminalization, while organizers use what digital tools and other technology they have at their disposal to combat this violence in movement building spaces. As a result of these investments, the state and its co-conspirators simultaneously erode communities' access to safer working tools (i.e., through legislation like FOSTA, EARN IT, and the controversies related to USAGM #OTF) and make them more vulnerable to often lethal policing and surveillance.



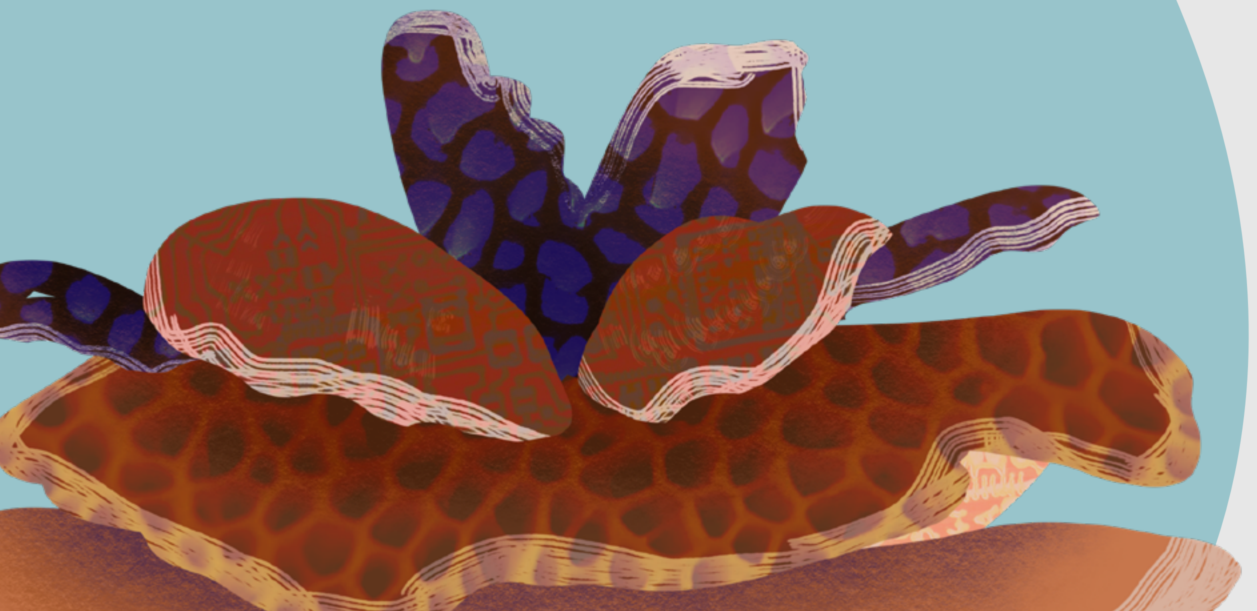
> "We're seeing this conflation of safety and security that has caused a great deal of harm. Law enforcement and city government, they tout increasing safety for communities and almost always they use the security mindset to do that. We're trying to drive home the narrative that surveillance is not safety. Safety is knowing who your neighbors are. Safety is a resource community center. Safety is thriving public education. Safety is making sure that your neighbors have water and food. Those are things that are safe."
>
> **organizer & researcher**

Peddling Surveillance Society

Dominant, pro-surveillance narratives peddle surveillance technology as a "smarter" method of social control to "protect" public safety and national security.

Under this pretext, the state has historically shaped the discourse around what criminal behavior looks like, and thus, justified the need for heightened surveillance and other discriminatory law enforcement practices. Policies such as Jim Crow[22], Broken Window Policing[23], and California's Three Strikes Law[24] serve as examples of how a population is vilified to justify extreme levels of surveillance and policing. As the state increasingly uses technological means to expand the scale and scope of its carceral apparatus, we have witnessed a shift in the public narrative to justify government agencies' use of technology to criminalize communities of color and other populations seen as inferior to white, capitalist, patriarchal, and imperial conquests.[25] By stoking fear in primarily white, suburban, upper class communities of certain populations, the state has been able to gain approval of pro-surveillance interventions that impact everyone. Rhetorical arguments calling for "law and order" have underscored this justification.[26] It is vitally important that QT2SBIPOC communities have the necessary resources to counter narratives of militaristic security. A narrative shift is required, a shift that centers communities' definitions of safety, and supports their fight against violent surveillance and criminalization practices deployed in the name of safety.

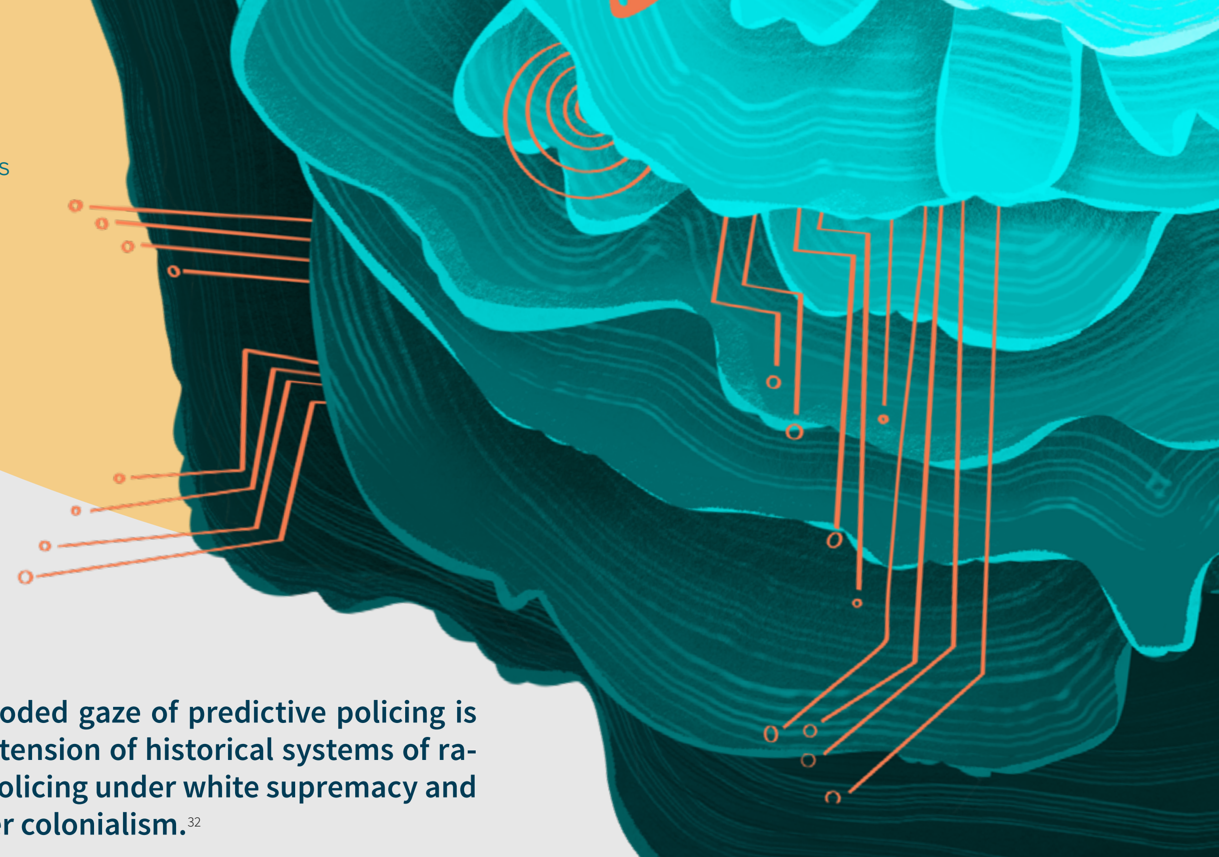
> “
>
> You think about how facial recognition software is biased in so many ways. It misgenders Black women in a way that's very much connected to the masculinization of Black women in this country, for generations. Thinking about what that means for queer, non-binary, and trans people. Do the builders of AI value queerness? For me, queerness is antithetical to AI because it falls outside of any data sets that try to define how you are going to move in this world. The makers of these technologies are getting more and more support. What does this mean for LGBTQI People of Color and how these technologies are used against us? It worries me a lot.
>
> ”
>
> **developer & digital security educator**



Automating Injustice: AI, Facial Recognition, Predictive Policing, & Pretrial Risk Assessments

AI and decision-making algorithms are becoming a common feature of tech-driven policing and detention systems.[27]

AI technologies such as facial recognition software, predictive policing, and pre-trial risk assessment algorithms perpetuate criminalization through racial and gender bias and have become what Joy Buolamwini of the Algorithmic Justice League calls the “coded gaze.”[28] These algorithms are biased because these types of automated systems are designed within an already discriminatory system shaped by the white gaze, as programmers and designers encode their judgements into technical systems.[29] What many call algorithmic bias may be more appropriately described as algorithmic *violence* because of how it brutally targets Black and brown communities.



One of the most dangerous forms of community-level algorithmic violence is “predictive policing,” a range of data-driven surveillance practices that turn entire neighborhoods into vectors of criminal probability.

This technology involves the use of software to determine who is considered “criminal” and where crime is “likely” to happen. According to a study of 13 jurisdictions that currently use predictive policing systems, the data on which these systems are built is deeply flawed due to “systemic data manipulation, falsifying police reports, unlawful use of force, planted evidence, and unconstitutional searches.”[30] However, the Stop LAPD Spying Coalition says the problem is not simply dirty data–it's the fact that predictive policing AI is fundamentally designed to police Black and brown bodies, communities and land.[31]

The coded gaze of predictive policing is an extension of historical systems of racist policing under white supremacy and settler colonialism.[32]

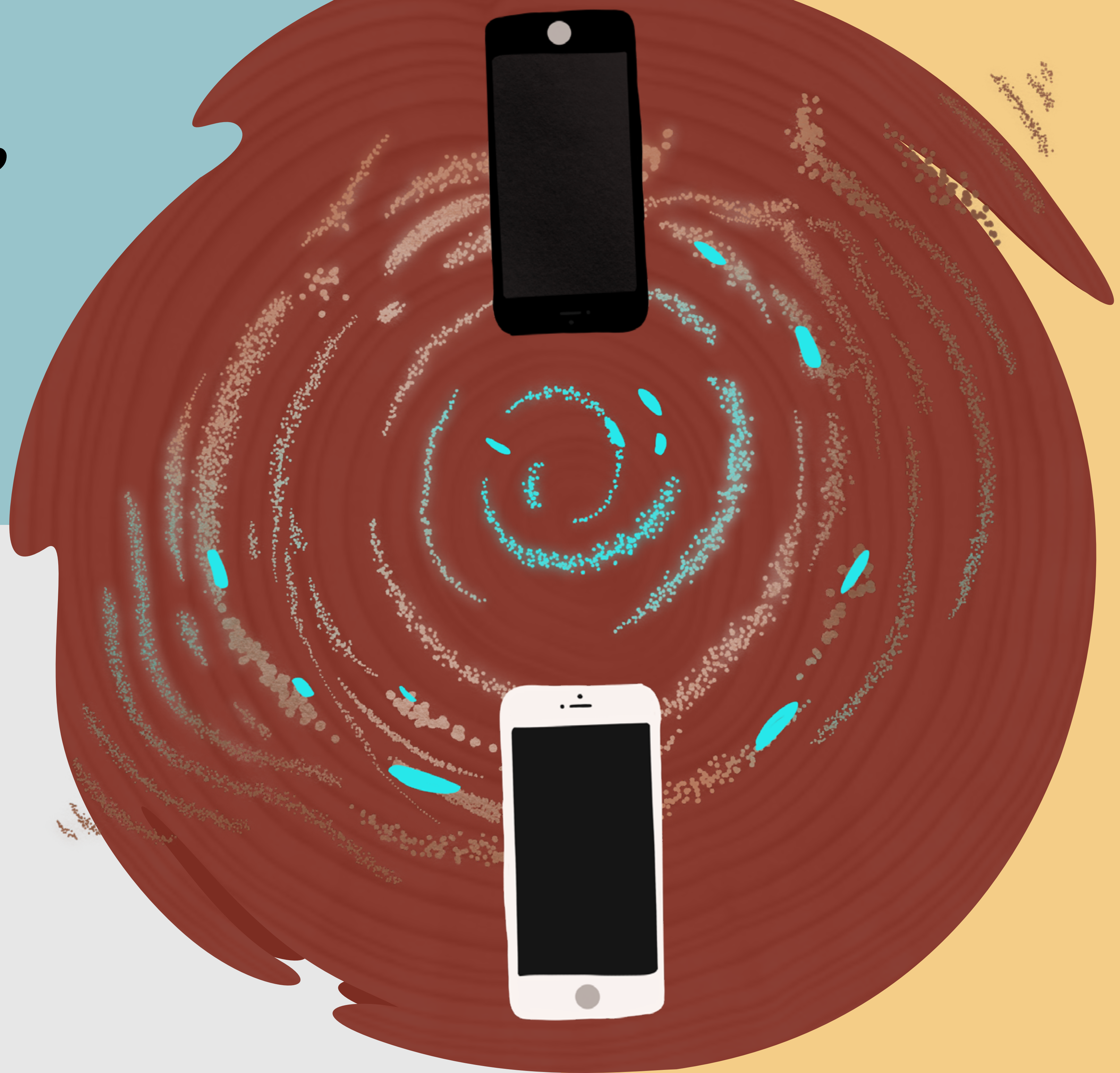
This system is not broken, it is working exactly as intended, now with modern technologies to facilitate and automate these processes. Over the last decade in Los Angeles, the LAPD hired Predpol, a predictive policing vendor, to create a statistical model for predicting crime in geographic zones with low-income communities of color, which it labeled “hot spots”. The LAPD combined this with a mapping system, LASER, to create Chronic Offender Bulletins (COBs), which identify people for targeted surveillance. COBs are then analyzed by Palantir, a data-mining search platform that cross-references information from multiple databases and automated license plate readers (ALPRs).

Palantir assigns a “score” to persons on the COB list according to gang affiliation, parole or probation status, arrests, and other so-called “quality” police contact.[33] Both Predpol and Palantir operate in other cities where police departments have significant records of racist brutality and misconduct.[34] Contrary to promoting community safety, the Stop LAPD Spying Coalition argues that, “a feedback loop is created where an increasingly disproportionate amount of police resources are allocated to historically hyper-policed communities.”[35]

> “ I view the march of technology rather than policies being a threat. Pretrial risk assessment instruments are a particularly stark example [of] the threat of technology on marginalized communities. There’s been a huge movement to end cash bail around the country...but is being substituted by these automated instruments that will gauge people’s risk, whether they’re a flight risk or a public safety risk. In California, SB10 recently passed, which would end cash bail and also bring in this new era of risk assessment. We believe this has the very real potential of hardening a lot of the racial disparities that we’re seeing. It won’t actually lead to decarceration. It might actually do the opposite ”
>
> **technologist, researcher, & policy analyst**

The criminal legal system’s growing reliance on pre-trial risk assessment algorithms deepens carceral control and racist biases over people’s lives.

The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), an algorithmic system for predicting recidivism rates among pre-trial defendants, has erroneously predicted “high-risk” for Black defendants and “low-risk” for white defendants.[36] Much like electronic monitoring (discussed below), pre-trial risk assessment algorithms are presented as an alternative to traditional detention policies like cash bail. Yet, they threaten to further entrench people’s entanglement in the criminal legal system due to the racial biases and decades of racist criminal history data embedded within these tools. Between the continuous development of surveillance technologies and the expansive, often unmitigated carceral reach of the state, it is paramount to connect historical legacies of criminalization with contemporary inequalities regarding mass incarceration.



Electronic Monitoring: All the World a Prison

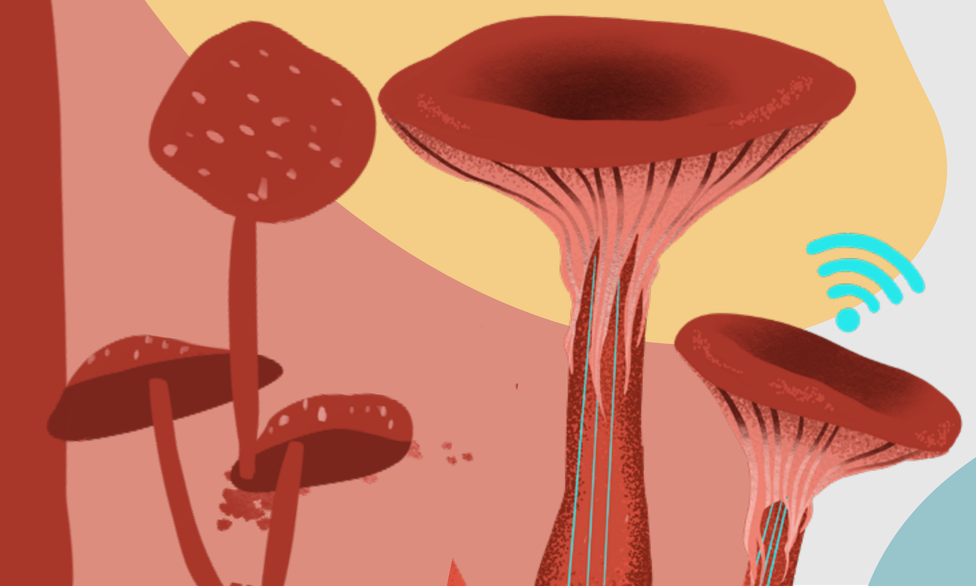
Surveillance technology is extending the reach of the carceral state beyond physical prisons by normalizing what MediaJustice (MJ) calls “e-carceration”

—the use of wearable electronic monitors, such as ankle monitors, that restrict the freedom of movement and agency of individuals on parole and probation and convince the public that the government should be permitted to track people accused of and convicted of crimes.[37] The sharp rise in the number of people on parole and probation has accompanied mass incarceration; approximately 4.5 million people in the US are under some form of correctional supervision outside of formal jails and prisons.[38] More and more systems, including immigration and juvenile detention, are using electronic monitoring devices.[39]

GPS tracking data from electronic monitors can be incorporated into other agencies’ databases, casting an even wider net of surveillance over a person’s every move.

Business is complicit in the explosive development of location surveillance phone apps that may ultimately replace ankle technology. For example, over the last year, BI, the world’s largest electronic monitoring company, has doubled the number of people under ICE supervision with SMARTLink, a social media electronic monitoring app.[40] Governmental agencies and the industries producing electronic monitoring devices have responded to critics of ankle monitoring by going mobile.[41]

> “This technology is being put out there as the tool of the future to restructure the criminal legal system. We’re going to have a lot more people under a whole range of technological surveillance and carceral technological control. It’s not so widespread in usage right now that it couldn’t be stopped, but if we don’t do something about it, we risk setting up another system of incarceration.”
>
> **researcher & educator**



While reform advocates tout electronic monitors as an alternative to incarceration, **carceral technologies actually widen state surveillance and punitive control over formerly incarcerated people’s lives. They effectively create “digital prisons” that further mass criminalization.**[42] The majority of people under e-carceration are confined to their houses and are not allowed to leave without a court order or permission from a parole officer.[43] This type of virtual, often solitary confinement greatly affects the mental and physical health of QT2SBIPOC people. A Black trans woman living in Chicago shared her story of e-carceration with MediaJustice, reporting that while she was under electronic supervision, she was denied permission to leave her house to buy food and fill prescriptions for HIV medications she requires daily.[44] In emergency situations, people are forced to choose between risking going back to prison for unauthorized movement or, for example, taking a sick child to the hospital.

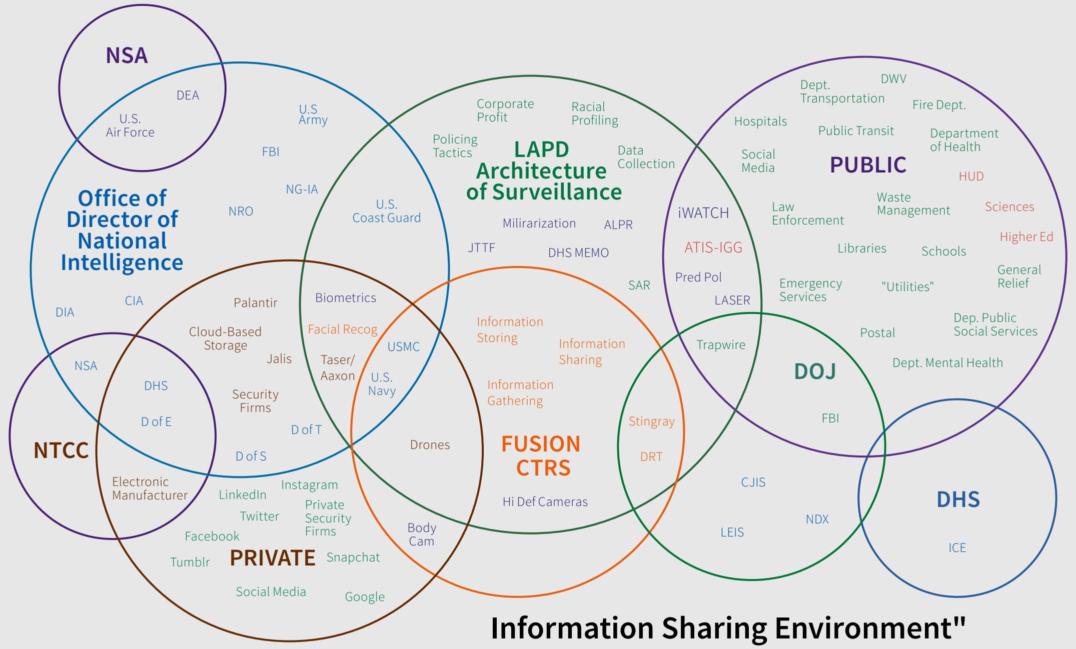
E-carceration also creates barriers to employment because the restriction on movement prevents people from going to job interviews or working in environments like concrete buildings that may interfere with the monitor’s signal. Electronic monitoring further harms communities already vulnerable to mass incarceration, contributing to financial and other material dependence on the families and social networks of those on parole and probation[45].

Electronic monitors spread carceral logics into other spaces of society, including the surveillance of workers in factories and of public areas. This expansion of surveillance extends mass criminalization’s reach to low-wage workers. Technology companies that develop surveillance technology already deploy these products on their own workforce. Major companies—like Amazon and Fitbit—have begun using surveillance technology that tracks the motions of its warehouse workers,[46] who are disproportionately Black, migrant, and People of Color in low-wage positions.[47] In outdoor spaces, monitoring devices facilitate “e-gentrification” and create de facto segregation by restricting those who are forced to wear them from entering certain areas.[48] As a researcher and educator interviewed noted, these exclusion zones apply to people who face criminalization in particular ways, such as those on the sex offender registry, who are banned from going within a certain perimeter of public parks. That electronic monitors come programmed with exclusion zones sets a dangerous precedent for other devices that people use daily. This is becoming more apparent with the fear of stingray cell simulators[49] and contact tracing of COVID-19 being used to track down organizers at the 2020 mobilizations in support of Black Lives.[50]

> “There’s a surveillance ecosystem that is emerging that we need to be very, very mindful of in terms of the ways in which some of these companies are capitalizing off of our movements to end bail. As a trade off, people are agreeing to much higher surveillance with digital cages that confine people to a particular neighborhood, that confine them in terms of what times of day they can be out, etc. That would become more of the norm rather than the exception. When you think about people who go in for a ticket or who didn’t pay a fine...where the previous answer was three days in jail, it is now perhaps a month with an ankle monitor and consistent surveillance. This is a huge trade off...it’s the new redlining, frankly.”
>
> **technologist & digital educator**

> “
>
> Since most people have some kind of GPS device anyway, it doesn’t seem like a huge leap to put some kind of controlling technology in those devices where there are exclusion and inclusion zones. You can only go where the technology permits you to go during certain hours of the day. That’s one of the fears I have about how this technology can control people’s movements in a much more systematic way than what we see at the moment.
>
> ”
>
> **campaign organizer**

Surveillance Economies & the Rise of the “Stalker State”



Information Sharing Environment"
Stalker State"

Source: The Stop LAPD Spying Coalition

Understanding the hidden ways in which data flows from our personal and private devices to state-based agencies helps us understand the extent to which our communities are being policed and surveilled.

The Stop LAPD Spying Coalition defines the **“stalker state”** as a network of overlapping data-sharing systems between social media corporations, private security firms, public service institutions, military departments, federal agencies, and local law enforcement.[51]

It enables data-sharing among state and local police, intelligence agencies, and private companies while also fueling profit-driven tech development as positive progress. A prime example of the stalker state’s reach and impact on a public narrative about safety is the political debate surrounding the militarization of the US border—what so-called progressive politicians espouse as the “smart border”—a surveillance network of AI, drones, cameras, and infrared sensors, as a more humane alternative to the Trump administration’s draconian border wall project.

Tech companies are complicit in developing facial recognition technologies.

For example, companies like Thorn and Marnius Analytics have programs that scrape data from escort ads, without consent, to use in the design of new facial recognition technologies targeting sex workers.[52] Under the pretext of “anti-human trafficking” initiatives, companies are enlisting lower-wage workers to surveil sex workers and share data with law enforcement,[53] as one interviewee shared, “this suite of AI tools as well as anti-human trafficking trainings at Uber and Marriott on how to “spot” human trafficking survivors encourage some of the lowest-paid employees of these companies to snitch on sex workers, creating a dynamic where workers are snitching on workers. Sometimes these reports at Marriott and Uber lead to calling of ICE. Once you’re in this system, the state can surveil you using these technologies, harming workers all around.”

US government agencies and local law enforcement are capturing and weaponizing personal and community-level data to increase surveillance and repression of movements.[54]

As more data is captured and shared, it is becoming a potent weapon the state wields to disrupt movements. This is happening within the larger international context of US military wars and inter-governmental and inter-agency data sharing in militarized zones such as the US-Mexico border. These practices are then applied by police at the local level in cities across the US. During protests and direct actions, police use surveillance devices like “stingrays” to disrupt activist communications, steal people’s data from their cell phones, and track their physical locations.[55] At least 75 police agencies in 27 states use these devices to capture personally identifying information, which is then shared with other agencies to profile and monitor organizers.[56] These technologies have especially targeted the Black Lives Matter (BLM) movement. During the Eric Garner protests in New York, the NYPD infiltrated BLM and gained access to organizers’ text messages[57]. In 2017, an FBI intelligence assessment surfaced a new designation of security threat, the so-called “Black Identity Extremist” (BIE)[58]. In 2020, police used facial recognition technology and the surveillance of social media to identify and arrest activists who were at protests in support of Black Lives.[59] For example, using Clearview AI, activists in New York City and Miami were arrested after participating in the summer protests.[60]

> “ We really have to understand that some of these technologies and data practices are basically created for war zones or for imperialist intervention models. They are brought to a militarized border and start to seep through into the rest of the US and police overall. ”
>
> **campaign organizer**

Battle for privacy-first policies and technologies includes protecting access to technologies like end-to-end encryption and protection from digital attacks.

Encryption technology is an important safeguard against state surveillance and is under threat. Recent US legislative efforts (i.e.,the EARN IT Act, the LAED Act and the PACT Act),[61] coupled with subsequent defunding of open-source encrypted technologies, show the US government's transparent desire to access communities' private communications and do away with access to technological tools employed for privacy like end-to-end encryption[62] (E2E). If signed into law, it will have a global impact on civilian access to encrypted technologies. The loss of this protection would mean that the state would be able to monitor all communications from any device, anywhere. This would imperil the digital security not only of social movements, but of all. The end of E2E would create a backdoor for law enforcement, and also make it easier for civilians with malicious intent (such as abusers, people spreading revenge porn, etc.) to access previously secure communications. The government is also moving toward targeted malware attacks, known as the Network Investigative Technique (NIT) and dragnet malware to capture data from large groups via a single warrant.[63] Additionally, the government is funding tech companies to design malware products that destroy built-in security mechanisms, which millions of people—including organizers—depend upon. QT2SBIPOC organizers report that the state is using these methods to break into their cell phones and personal devices to try to gain access to their data.[64]

Social media intelligence (SOCMINT) companies have found a lucrative niche in contracting with federal and state agencies to spy on organizers.

Private firm ZeroFOX monitored the social media accounts and geolocation[65] of BLM organizers during the Freddie Gray protests in Baltimore, referring to organizers as "threat actors" in intelligence reports to law enforcement.[66] Similarly, Geofeedia obtained user data from Facebook, Instagram, and Twitter to monitor activists during the Michael Brown protests in Ferguson.[67] Movement organizations often rely on social media to communicate with members and promote their campaigns and events, which makes them vulnerable to surveillance, infiltration, and data poaching. They acknowledge that a major contradiction they face in using mainstream platforms is what some call the "network effect." That is, as organizers reach more and more people on these platforms, they also become more dependent on corporate infrastructure for their organizing work. This, in turn, reinforces the status of mainstream platforms as the "default" venue for all communications. Organizers interviewed for this research even report that police and federal agents have used fake social media accounts to pose as activists and try to gain access to personal and organizational information. The ways that private companies collaborate with state actors is often opaque, but the consequences of these collaborations are very real.

Targeting Migrant & Native Communities at the Border

Customs and Border Protection's (CBP) deployment of surveillance technologies—which it uses to monitor and detain migrants—impacts migrants and Native communities whose land is divided by the border.

The US-Mexico border crisis spotlights the interlinked struggles between Native land sovereignty and migrant justice. Border surveillance perpetuates colonial dynamics, offering modern means to maintain historical oppression. The Tohono O'odham Nation, located in southern Arizona/northern Sonora, has been under "wide-area persistent surveillance" since 2006 when CBP began building surveillance towers, flying drones, and using cameras and motion sensors within Tohono O'odham territories. Tribal members say this impedes their relationship with their land and sacred sites.[68] Meanwhile, these technologies further harm the lives of people migrating across the border and erode civil rights protections within the 100-mile inland border zone where most people live in the United States.

"It's been really, really dangerous. Because ICE agents now have more resources from the federal government for surveillance, they have more time on their hands to be able to do more things. You have agents doing the in-person surveillance, so following people, stalking people's homes, threatening people's family members... but then you also have the digital surveillance where they're able to map out family trees and find addresses to conduct their raids based on information from private data brokers. We're really seeing it on all levels."

campaign organizer

Third-party agreements between government agencies and data-brokering companies facilitate the interlinking of digital and physical threats.

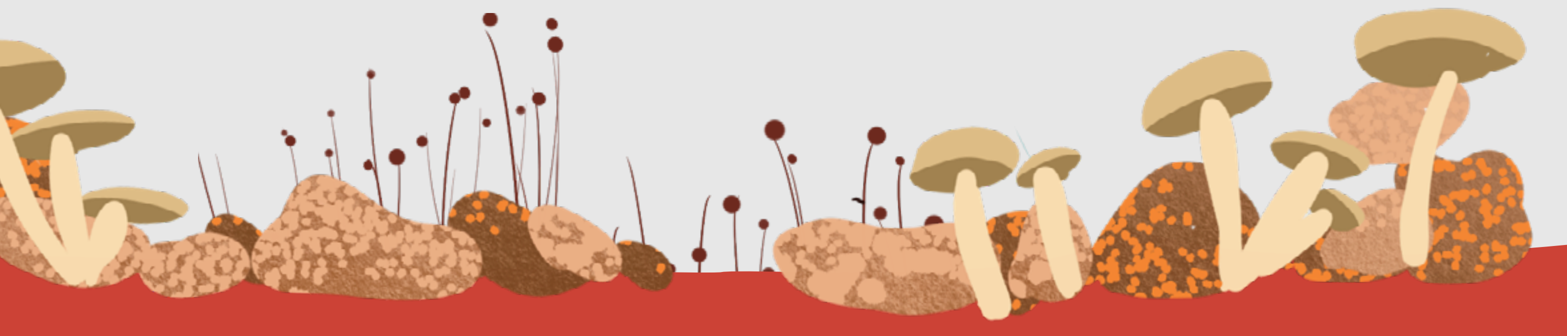
Border agents now commonly ask people for their social media accounts upon entering the US and there are reports of sex workers being denied access at border crossings because of social media and escort ads.[69] Migrant justice advocates warn that immigration authorities monitor queer and trans asylum seekers' posts on platforms like Facebook and use their social media content to argue against their asylum cases. The linkage of digital and physical surveillance through third-party data sharing has enabled ICE to conduct targeted raids based on people's addresses, social media posts, and location data.[70] In response to concerns about ICE raids in Puerto Rico, some organizers reported having to close their social media accounts, avoid posting about their activism, or cover their faces during protests to avoid being deported.

The increasing collaboration between the US government and private tech companies is fueling a system where corporations are profiting from surveillance products.

This is a clear example of how 'surveillance capitalism' works in the service of criminalization. The Department of Homeland Security (DHS), CBP, and ICE are spending billions of taxpayer dollars annually on contracts with tech companies to target immigrants of color.[71] Nowhere is this more apparent than with the escalating arrests, detentions, and deportations that comprise the US administration's ongoing war against migrant communities. This war, which also includes the geographical and biometric surveillance of immigrants and their communities, represents what has been called ***crimmigration:*** the intersections of criminalization and immigration.[72] As with other forms of criminalization, the use of technology to consolidate power and capital is well documented within the policing and militarization of the US borders and immigration system.

The growing technical interconnectedness between federal agencies and local police departments is eroding protections granted by "sanctuary cities" that have historically limited the use of federal immigration detainers for a person of undocumented status in custody.[73]

Due to inter-agency data sharing and police use of social media, ICE agents are surveilling and arresting migrants in churches, courtrooms, hospitals, and other public spaces with greater frequency.[74] This restricts the movement of people of undocumented status and prevents them from accessing much needed health, legal, and social services for fear of being detained and deported.



Surveillance Economies and the Criminalization of Migration

- Palantir, for example, produces software for ICE agents to profile and arrest families of undocumented status, playing a direct role in taking migrant children away from their parents and caging them in privately run detention facilities.[75]

- Tech companies are ramping up surveillance along the border through an initiative known as the **"smart border"**, for which Congress approved a $100 million budget in 2019.[76] For example, Elbit Systems, a subsidiary of Israel's largest military company, signed a $26 million contract with CBP to build a network of massive surveillance towers with night vision cameras, thermal sensors, and ground-sweeping radar. There are currently more than 400 such towers along the US-Mexico border.[77] Anduril Industries is working with US border agents to test a new surveillance system called Lattice, which combines AI, cameras, drones, and LIDAR, and operates miles beyond the border.[78]

- By networking databases and search tools between CBP, ICE, and US Citizenship and Immigration Services (USCIS), the Continuous Immigration Vetting (CIV) program, which collates information from immigration benefit applications throughout the entire application period, casts a wider net over those without citizenship status.[79]

- Amazon Web Services (AWS) provides cloud hosting to the federal agencies and local police departments who share information with DHS.80 DHS stores data from its Automated Biometric Identification System (IDENT), a repository of 230 million unique identities based on fingerprint, iris, and facial records, on the AWS cloud.[81]

- Cloud hosting also supports ICE's Integrated Case Management (ICM) system created by Palantir. Not only does ICM collect, store, and analyze massive volumes of personally identifiable information, it also creates the ability to share data across systems at all levels of government.[82]

- Over 9,000 ICE agents have access to an automated license plate reader (ALPR) database run by Vigilant Solutions, a company with which ICE has a $6.1 million contract.[83] The ALPR database allows ICE to follow migrants across 5 billion points of location data.[84]

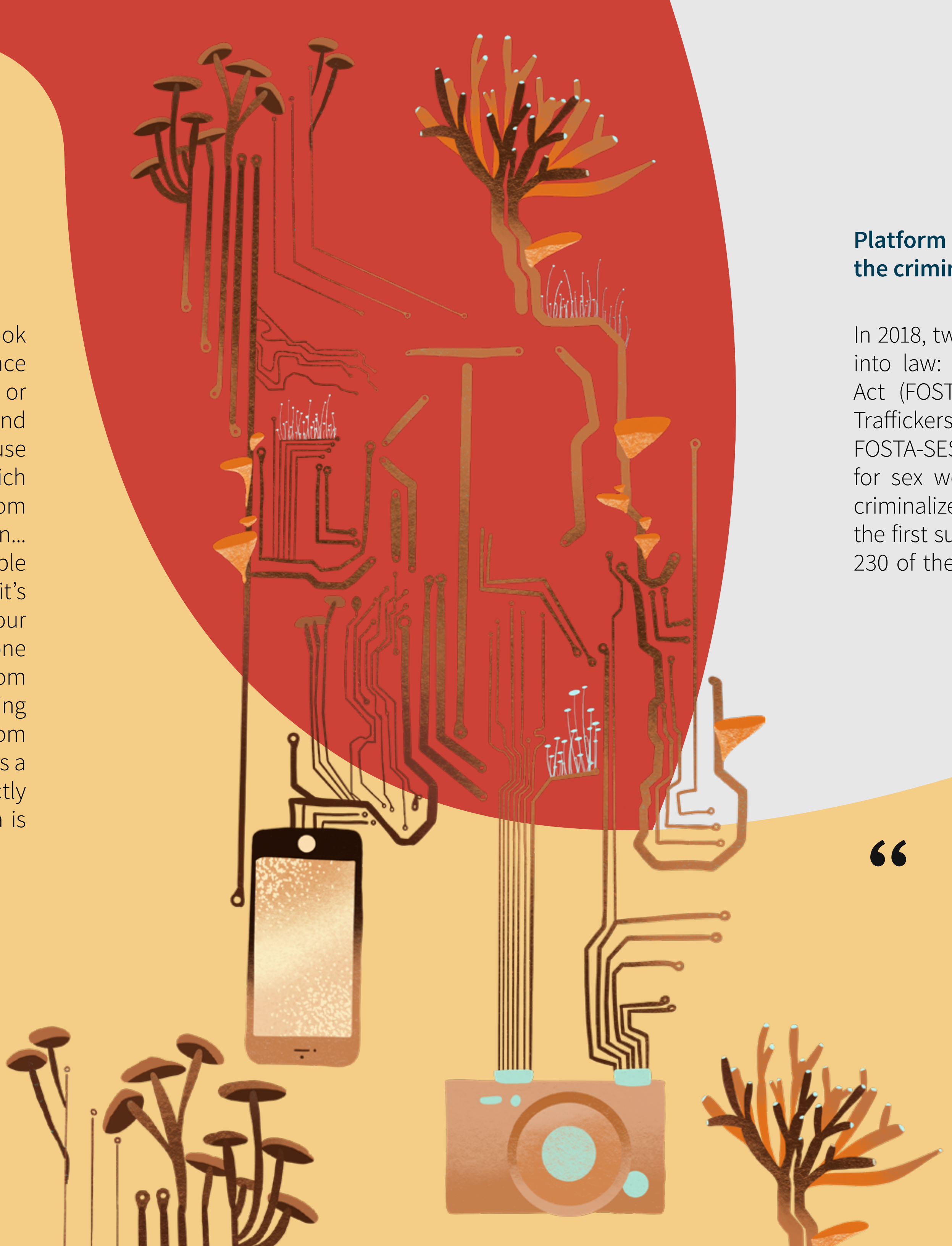
Surveillance & Control of Mainstream Social Media Platform Users, Data & Content

Social media companies are letting police, federal agencies, and third-party tech companies surveil QT2SBIPOC communities and organizers via their platforms. Access to mainstream social media platforms is often severely limited for Black, trans, and sex worker communities because of the ways in which these identities are policed and restricted by algorithms that are inherently racist, transphobic, and whorephobic.[85]

For example, as a result of content moderation practices, sex workers report difficulty finding each other on social media,[86] Black femmes and people who are coded as sex workers, are banned from Instagram at a higher rate,[87] real name policies prevent sex workers and trans folks from using platforms.[88] Community members are forced to decide if they will risk use of and reliance on specific platforms, which includes facing the risk of removal by the platform moderators who may delete accounts without reason. These removals not only disrupt economic opportunities and community connection, they also make community building, organizing and mutual aid more difficult.

> “
>
> We see corporations like Facebook acting as arms of surveillance and providing all kinds of data or opportunities for law enforcement and corporations to capture data and use it in punitive ways. The way in which surveillance impacts people whom I call the criminalized population... Black, brown, LGBTQIA, native, people of color broadly...for those people, it's not about somebody snooping in your email or eavesdropping on your phone calls. It's really about blocking you from employment opportunities, blocking you from education, blocking you from housing, blocking you from travel. It's a whole range of ways in which it directly impacts your life when all this data is weaponized to be used against you.
>
> ”

researcher & educator



Platform moderation, or the policing of a platform's content, is a critical site where the criminalization of sex work intersects with threats to internet autonomy.[89]

In 2018, two congressional bills were signed into law: the Fight Online Sex Trafficking Act (FOSTA) and the Stop Enabling Sex Traffickers Act (SESTA). Together known as FOSTA-SESTA, they make platforms liable for sex work related content and further criminalize sex workers.[90] FOSTA-SESTA was the first substantive amendment to Section 230 of the 1996 Communications Decency Act, which protected internet platforms from liability for the content users produce and post to their platforms. Many technology experts argue that Section 230 allowed for the growth of the free and open web that we use today.[91] But FOSTA-SESTA overrides Section 230's "safe harbor" clause by increasing platform liability, in effect imposing broad internet censorship and a chilling effect.[92]

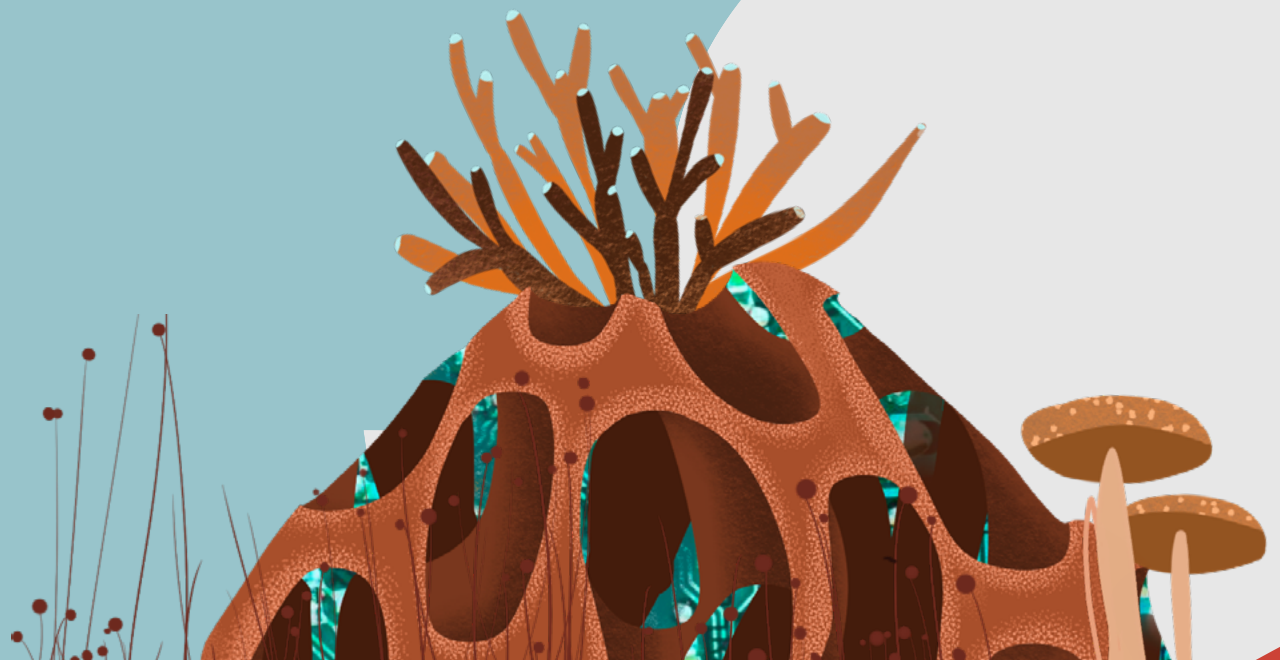
> “ The passage of SESTA and FOSTA has shutdown spaces for people to do work digitally. It's impacted people very negatively, here in DC specifically. The people who've been most impacted are trans women of color, Black trans women, because now more and more people have to do street work, which is more dangerous in a lot of ways, including because police are out here. It's easier for people to be arrested and go into the criminal legal system. ”

developer & digital security educator

FOSTA-SESTA further polices sex work online and exacerbates existing platform policies and practices that censor online sex work and suppress digital organizing efforts, such as shadowbanning,[93] content moderation, and deplatforming.[94]

This means that they do not have the same access to the tools non-sex working folks use to build business and to organize.[95] Like many entrepreneurial businesses, many sex workers rely on an online presence, marketing, and creating their own online content to conduct business, and FOSTA-SESTA threatens to eliminate this capacity.[96] FOSTA-SESTA also harms the freedom of movement and economic opportunity for migrant sex workers. With the Department of Homeland Security and the FBI raiding adult services' ad platforms and seizing servers containing user IDs and personal data, migrant sex workers, especially those who are of undocumented status, are unable to find work and live in fear that the government will use this data to track, arrest, and deport them.

> “
>
> I was very shadow banned, so I wasn't showing up in searches. We did a lot of organizing around this hashtag, #LetUsSurvive. Looking at the statistics for this hashtag, though the numbers are there, it does not show up as trending.
>
> ”
>
> **researcher & educator**



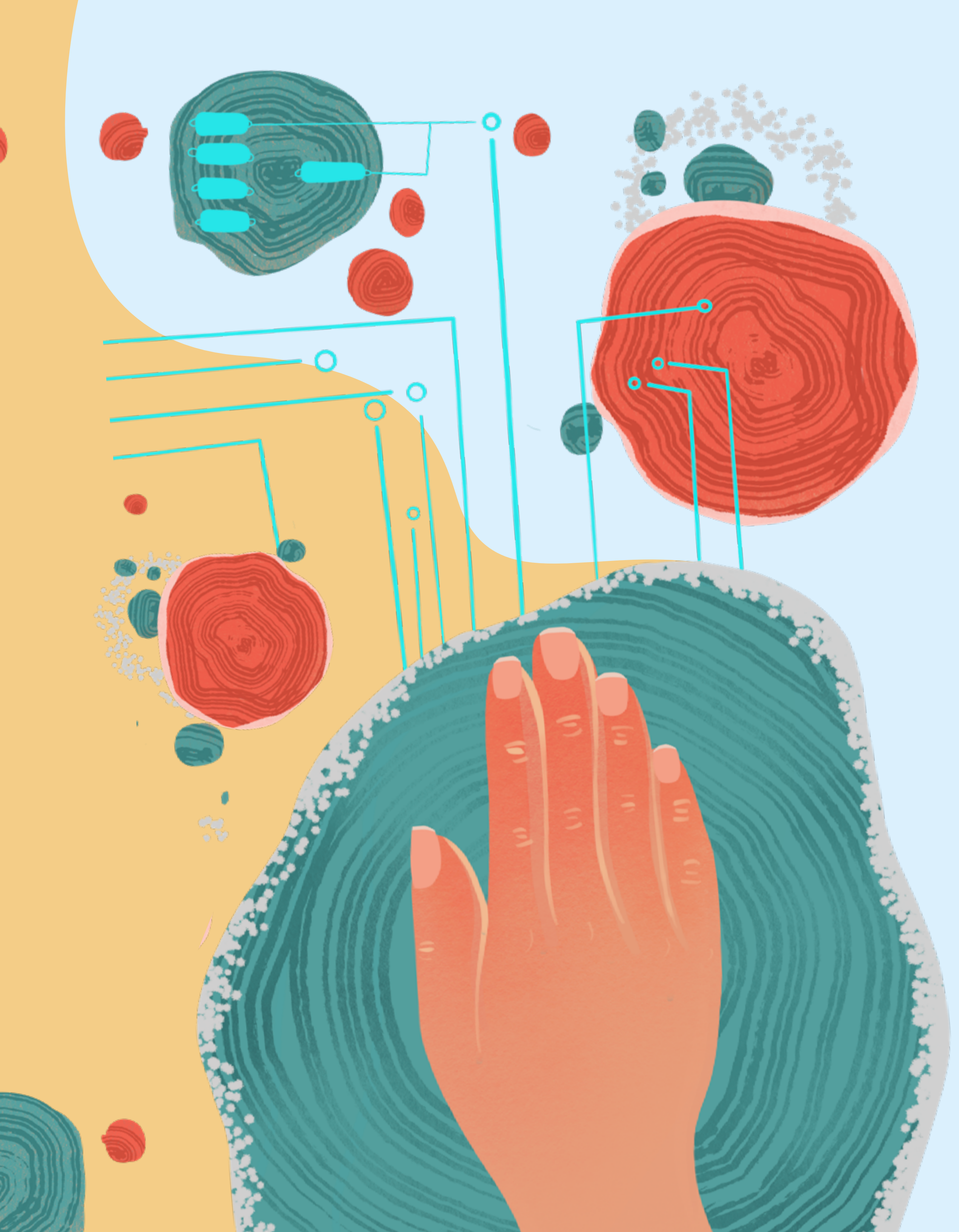
FOSTA-SESTA limits the resources that movement organizers need to combat harmful legislation, as many organizers fund their unpaid labor with money earned from sex work.

In Hacking//Hustling's new report on content moderation in sex worker and activist communities in the wake of the 2020 mobilizations in support of Black Lives, they found that individuals who engaged in both sex work and activism work experienced significantly more negative effects of platform policing than individuals who did either just sex work or just activism work.[97] This suggests that there is a compounding effect where platforms more harshly police, censor, and deplatform activists who support their organizing work through sex work.

MOVEMENT STRATEGY, RESPONSE, & RESISTANCE

Embodying power and resilience, organizers and communities employ new and old strategies to identify and resist criminalization while dreaming up new worlds free from state violence and control. The movement responses shared in this report are built out of longings for freedom from the state's carceral apparatus, and from colonial and contemporary restrictions on identity, geographical movement and connection to land, and economic exploitation; they are built out of longing for communal liberty, resilience and sovereignty.

Organizers are using a myriad of strategies that range from organizing, to policy and advocacy, to political education, to somatics, to technology developments and beyond. These strategies demand decarceration and decriminalization, divestment from surveillance economies, harm reduction in platform moderation, exposing the extent of carceral systems and technologies. They also include building concrete community structures driven by the needs, safety and direct engagement of communities. Acknowledging the destructive principles of the prison industrial complex, and its reliance on punishment and surveillance technologies, organizers forge intersectional analyses that center abolition, healing justice, and community-based interventions in their work. These adaptations represent movement technologies that point towards a future beyond policing, creatively circumventing systems of criminalization and extractivist practices.



Abolition is the Vision

Critical Resistance defines abolition as the goal and practice of ending the prison industrial complex, which the organization describes as "the overlapping interests of government and industry that use surveillance, policing, and imprisonment as solutions to economic, social, and political problems." According to Critical Resistance, abolition is not simply about eliminating physical prisons, but about transforming the social conditions of oppression that give rise to violent systems of policing and incarceration.[98]

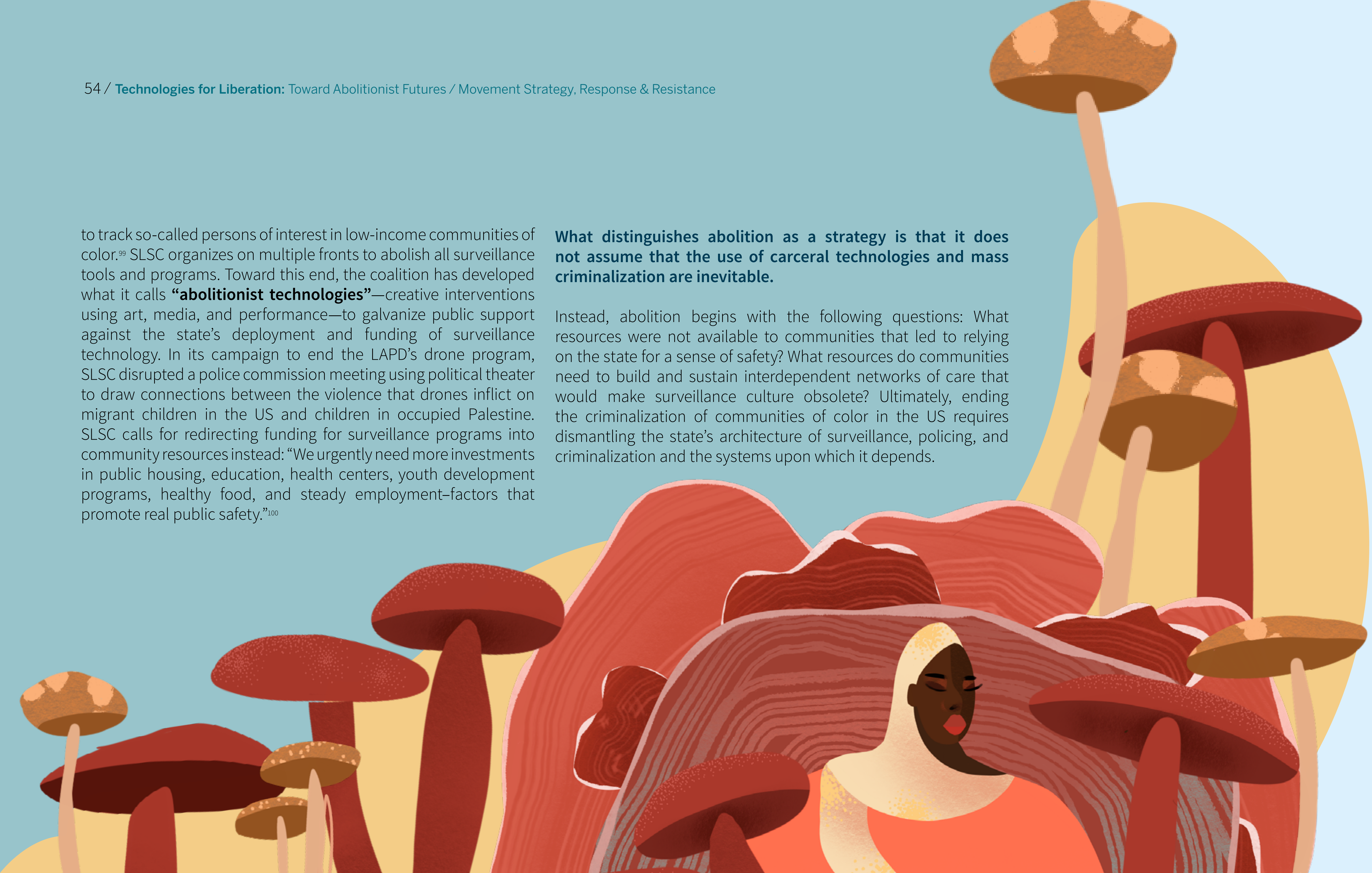
Abolition is the vision.

Abolition examines the root causes of systemic and interpersonal violence and how dominant narratives of policing have become internalized in our collective thinking. Abolition is an iterative practice that not only seeks to eliminate physical prisons, but also strives to transform the social conditions that lead to and feed oppressive, violent systems of policing, punishment, and incarceration.

Abolition is the antithesis of surveillance culture.

What distinguishes abolition as a strategy is that it does not assume that the use of carceral technologies and mass criminalization are inevitable. Drawing from historical lessons and legacies of resistance, an abolitionist approach calls for "a deep rethinking of our reliance on policing and surveillance to resolve all conflict, violence, and harms within our communities and society. It requires confronting our own sense of safety and the responsibilities of public safety, said a researcher and policy analyst interviewed for this research. If surveillance is, as one organizer put it, about "constant control of the body," then movements for abolition ask: How do we make structures of oppression and control irrelevant?

Organizations are creating successful abolitionist campaigns to fight tech and criminalization. In 2019, **The Stop LAPD Spying Coalition (SLSC)** won a hard-fought campaign to eradicate "Chronic Offender Bulletins" (COBs), which the LAPD had used



to track so-called persons of interest in low-income communities of color.[99] SLSC organizes on multiple fronts to abolish all surveillance tools and programs. Toward this end, the coalition has developed what it calls **"abolitionist technologies"**—creative interventions using art, media, and performance—to galvanize public support against the state's deployment and funding of surveillance technology. In its campaign to end the LAPD's drone program, SLSC disrupted a police commission meeting using political theater to draw connections between the violence that drones inflict on migrant children in the US and children in occupied Palestine. SLSC calls for redirecting funding for surveillance programs into community resources instead: "We urgently need more investments in public housing, education, health centers, youth development programs, healthy food, and steady employment–factors that promote real public safety."[100]

What distinguishes abolition as a strategy is that it does not assume that the use of carceral technologies and mass criminalization are inevitable.

Instead, abolition begins with the following questions: What resources were not available to communities that led to relying on the state for a sense of safety? What resources do communities need to build and sustain interdependent networks of care that would make surveillance culture obsolete? Ultimately, ending the criminalization of communities of color in the US requires dismantling the state's architecture of surveillance, policing, and criminalization and the systems upon which it depends.

Decarceration and Decriminalization

Decarceration and decriminalization are key goals in the abolitionist vision. A successful example is the nationwide **#BlackMamasBailOuts campaign, led by SONG and the National Bail Out Collective.** #BlackMamasBailOuts seeks to free Black mothers and caregivers so they can be with their loved ones for Mother's Day. In 2019, the campaign raised over $1 million and bailed out 123 Black mothers and caregivers in 37 cities.[101] As a decarceral strategy, #BlackMamasBailOuts offers a transformative model of investment in community support by directing funds not only for bail but also for childcare, sustainable housing, transportation, and legal services for Black mothers and caregivers. In doing so, the campaign recognizes that community support and services are necessary to keep people safe and well. It also celebrates Black trans mothers and caregivers who care for trans and gender non-conforming youth, along with Black queer families who defy heteronormative systems.

Along with decarceration, **broadscale decriminalization is needed to stop the expansion of mass criminalization enabled by surveillance technologies.** In Atlanta, **Solutions Not Punishment (SNaPCo)**, a Black trans-led collaborative, observed that the use of mounted cameras with enhanced surveillance capability on police vehicles led to more arrests of Black residents. In response, SNaPCo implemented a pre-arrest diversion initiative with the city so that those who were frequently stopped by police, particularly sex workers and people with neurodivergence, could avoid arrest and detention and access supportive services instead. A community organizer and advocate interviewed in 2019 reported that since 2017, 130 arrests have been diverted. This initiative was part of a broader campaign to decriminalize sex work across the state of Georgia. SNaPCo also partnered with **Women on the Rise**, a sister organization led by formerly incarcerated women, to close down the Atlanta City Detention Center. They are currently working to repurpose the former jail into a community space. SNaP4Freedom School, an organizer training program guided by a "Black trans futurist framework for practical abolition," organized a successful campaign to change a city ordinance that made marijuana possession a non-arrestable offense.[102] These strategic interventions have led to a larger push for decriminalization, as other municipalities have followed SNaPCo's model.

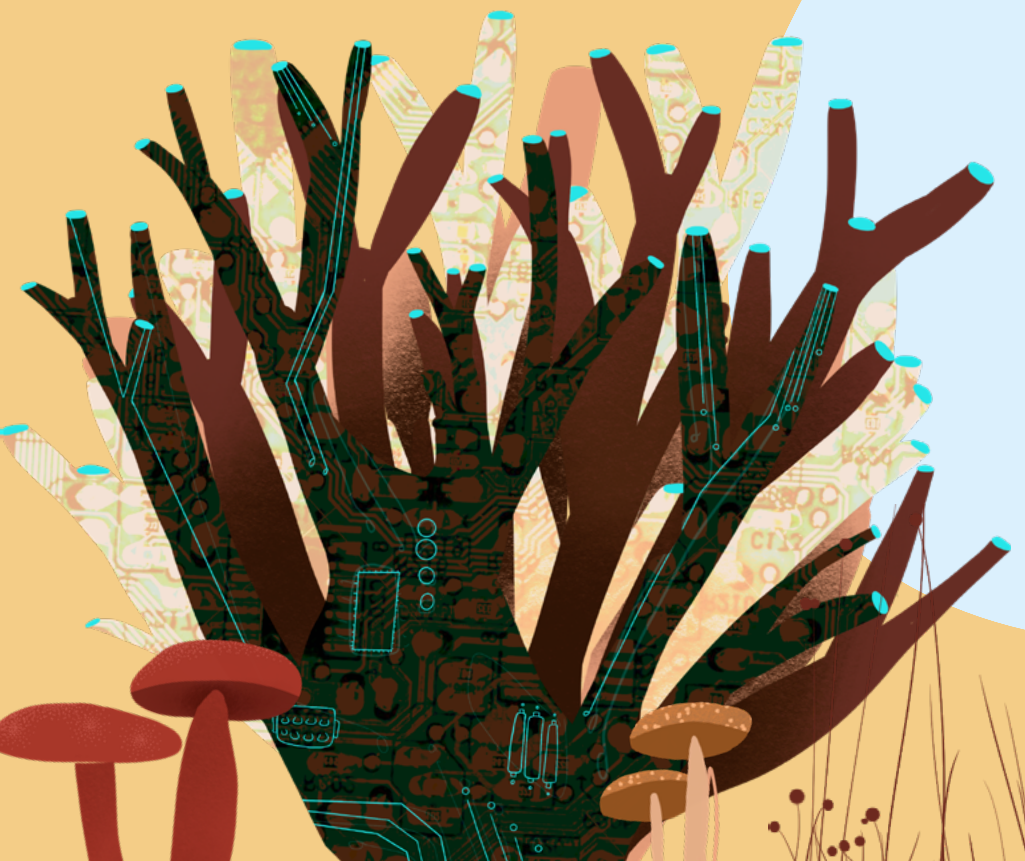
Resistance to profiling and 'Racist AI' has a long history leading to present-day battles against its use. In 2020, for example, partly in response to Black Lives Matters protests, the ACLU filed a case seeking to both ban the use of facial recognition technology by law enforcement and put in place a moratorium on the sale of facial recognition technologies to police forces by mainstream corporations.[103]

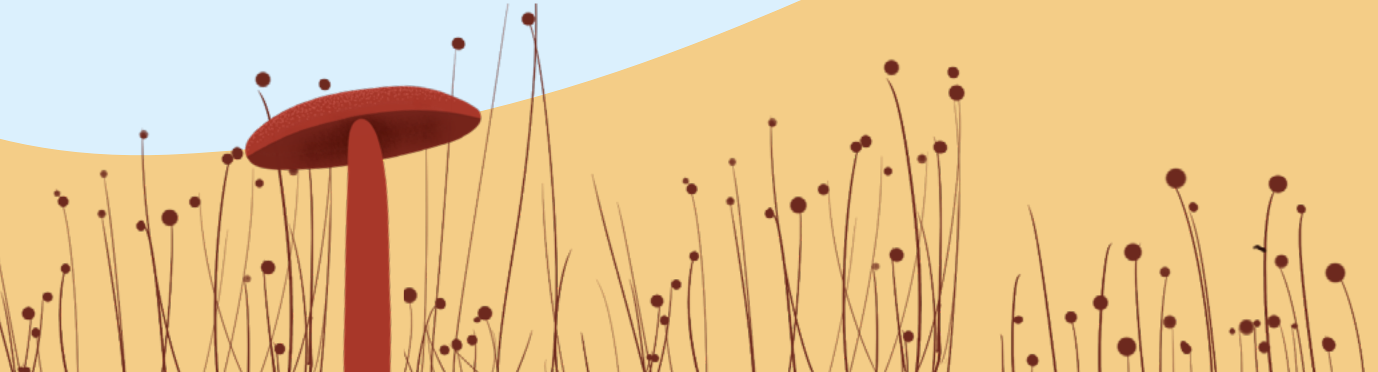
> “We’ve been doing immigration enforcement work for a while and technology is popping up in it and really changing the rules of the game. That means we have to be thinking about how we change culture, industry and economy in the US around deportations, in addition to just thinking of the federal policy that’s coming down from DC.”
>
> **campaign organizer**

Divesting from Surveillance Economies

Migrant justice organizations are calling for broad divestment from the surveillance economy that escalates arrests, detentions, and deportations in migrant communities.

Via the campaign #NoTechforICE (part of the larger #AbolishICE movement), organizations demand that tech corporations end their contracts with Immigration and Customs Enforcement (ICE) and stop building products that enable federal agencies to stalk and detain asylum seekers, refugees, and people of undocumented status. It also urges investors to divest from companies like Palantir that specialize in surveillance and data-sharing that have a direct hand in separating migrant families at the border.[104]





While many are skeptical about whether or not tech companies will be held accountable, spotlighting collaborations between private firms and ICE is a critical strategy for exposing the roles that tech companies play in the larger ecosystem.

In 2018, Mijente, a Latinx justice organization working at the intersection of immigration and tech, released “Who’s Behind ICE?” a report exposing the financial dealings between the US government and the tech industry.[105]

Mijente is organizing a geographically diverse, cross-sector network of migrant communities, tech workers, students, and social justice organizers to explore divestment strategies and intervene at the point of sale for surveillance products. For example, in 2019, migrant justice advocates championed California state bill “The Sanctuary State Contracting and Investment Act” (AB 1332), which would have barred local and state agencies from contracting with companies that provide data brokering services and data processing tools to ICE and CBP. Organizers hoped that AB 1332’s intervention model of creating economic consequences for cooperating with federal immigration authorities will shift the culture in Silicon Valley and push companies to adopt more ethical standards for conducting business.

> “This campaign is about exposing tech and data companies and getting people to understand how these companies are building the backbone of the deportation machine…and what it looks like to imagine possible strategies and tactics that we can engage with.”
>
> **campaign organizer**

Fighting Digital Prisons

Organizers are challenging electronic monitoring as an alternative to institutional imprisonment.

One example of these efforts is **MediaJustice's #NoDigitalPrisons** campaign. As political support mounts for decarceration (the reversal of decades of mass imprisonment in the US), MJ launched the #NoDigitalPrisons campaign to challenge the notion that electronic monitoring is a more humane replacement for traditional detention. Warning that electronic monitoring could become the new "technological" mass incarceration, MJ points out that the number of people shackled to electronic monitors has doubled in the past decade, and that more systems, including immigration and juvenile detention, are using these devices.[106] MediaJustice is **shifting the narrative to show that the experience of confinement and surveillance under "digital prisons" is a direct extension of physical incarceration.**

As part of #NoDigitalPrisons, MediaJustice initiated the **#ChallengingEcarceration** project to develop a set of guidelines for advocates and policymakers seeking to defend the rights of people under electronic supervision. These guidelines include provisions like credit for "time served under surveillance," since electronic monitoring is a type of state detention.[107] They also include restrictions on the kinds of personal data that can be collected by electronic monitors and how that data is shared. The guidelines also call for minimally invasive technology, with prohibitions on implants, biometric tracking, audio and video recording, and inflicting pain as punishment. Over 50 racial justice, criminal justice, and civil rights organizations have endorsed the guidelines.

> "I spent a year on an electronic monitor and I don't think electronic monitoring is an alternative to incarceration, I think it's another form of incarceration. The capacity of these devices, like cell phones, is going to greatly increase. Not only do they become devices of carceral control, they become devices of state surveillance. The data from them gets blended in with other databases. There's very little accountability for how the technology is used or what happens to the data that's gathered by electronic monitoring."
>
> **technologist & policy analyst**

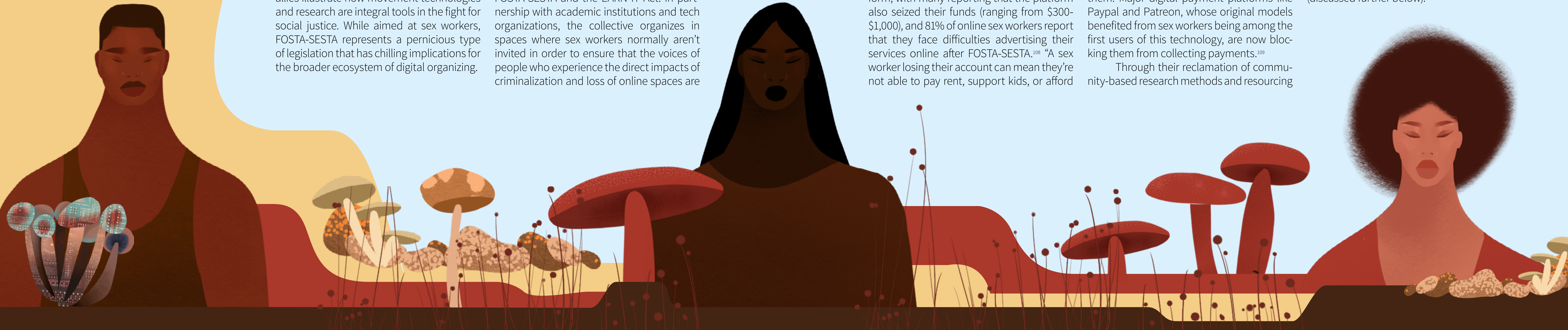
Research & Policy By Us, For Us

Securing work via digital platforms is a harm reduction strategy for many sex workers; online work is often safer than street-based work.

Documenting the direct negative impacts of FOSTA-SESTA on the safety, livelihoods and activism of sex-workers, organizers and allies illustrate how movement technologies and research are integral tools in the fight for social justice. While aimed at sex workers, FOSTA-SESTA represents a pernicious type of legislation that has chilling implications for the broader ecosystem of digital organizing.

Hacking//Hustling is a sex worker led collective working at the intersection of social justice and technology intentionally bridging gaps between the siloed communities of tech development, legal advocacy, academia, and grassroots movement organizing around the myriad ways that sex work is mediated by technology, including FOSTA-SESTA and the EARN IT Act. In partnership with academic institutions and tech organizations, the collective organizes in spaces where sex workers normally aren't invited in order to ensure that the voices of people who experience the direct impacts of criminalization and loss of online spaces are at the center of all policy conversations. They conduct community-based participatory research with fellow workers in the industry to learn how FOSTA-SESTA is harming economic self-determination and how sex workers are responding. According to their new study, approximately 33% of online sex workers experienced being kicked off a payment platform, with many reporting that the platform also seized their funds (ranging from $300-$1,000), and 81% of online sex workers report that they face difficulties advertising their services online after FOSTA-SESTA.[108] "A sex worker losing their account can mean they're not able to pay rent, support kids, or afford medicine or health care, and may also mean being disconnected from organizing efforts with friends who would help them," explained a sex worker activist. Many workers in the sex trades are experiencing economic instability and increasingly precarious working conditions as tech companies, fearful of federal and state prosecution, de-platform them. Major digital payment platforms like Paypal and Patreon, whose original models benefited from sex workers being among the first users of this technology, are now blocking them from collecting payments.[109]

Through their reclamation of community-based research methods and resourcing sex workers to share their lived experiences and expertise, groups like Hacking//Hustling remain at the forefront of movements by creating knowledge by *and* for sex workers impacted by surveillance. Hacking//Hustling also provides peer-led digital security *and* digital literacy trainings to strengthen the knowledge and security of their community (discussed further below).



Community-Centered Technologies

Community-centered technology is a powerful countervailing force in the fight against criminalization, equipping communities to use technology to resist surveillance culture.

Grounded in self-determination, organizers and movement technologists view their technology as a tool for liberation; they aim to shift the balance of power by actively supporting communities to have “access to the power to develop, control, and own technology.”[110]

> “How we approach the creation and use of technology has to be part of our vision of change. If we can create that, then new technology can actually unleash a bunch of power and not have it just be a way for corporations to monopolize and control people’s information.”
>
> **campaign organizer**

Organizers are using principles of design justice to re-envision who shapes technology, what it does and who has access to it in the first place. Organizers identified “design justice” as a theory and practice that centers engagement of communities in the design and development of technologies that impact them. Design justice is also “concerned with how the design of objects and systems influences the distribution of risks, harms, and benefits among various groups of people.”[111] As a framework, design justice considers: “Who gets to do design? Who we design for or with? What values do we encode in designed objects and systems?”[112] As a participatory model, design justice ensures that community members have a direct say over the goals, methods, and outcomes of creating and using technology infrastructure and tools.[113] This holistic approach to design proactively prioritizes what communities most desire and need from the design process.

Community technology and consentful technology are key conceptual prisms through which organizers are re-envisioning technology to support movement values.

As movement work increasingly relies on digital organizing, relationship building remains more critical than any tech tool. The Community Technology Network Gathering at the Allied Media Conference created guiding principles of community technology, which include access, empowerment, privacy, ownership, resource sharing, and collective expression.[114] Relatedly, the concept of consentful technology, developed by Allied Media, centers consent as a core value of empowering communities to access technology. Organizers emphasize strengthening community self-determination in accessing digital technologies by tea-

ching community members how to protect themselves and their data.[115] In this way, movement organizations help community members navigate their complex relationships with tech, both to reduce the harms of surveillance and to use tech for grassroots organizing and liberation.

Organizers are finding ways to adapt their digital organizing strategies to align with their values, ancestral knowledge, and traditional methods of convening people. For organizations whose approach hinges on digital organizing, the efficacy of their work continues to rely heavily on building interpersonal relationships in and across digital and physical spaces. A technologist, advocate & educator described this challenge: “Our work as online organizers and our big movement contribution is about figuring out how to create feelings of belonging at scale in ways that are honest and real.”

> “ I think one of the things that’s very challenging about being a smaller organization building software to solve complex problems is that it’s hard to resource. From a funding perspective, funders only want the sexy part, which is building software, and not the organizing part. It takes a lot to bring grassroots partners along on a process of developing and rolling out technology. ”
>
> **technologist, advocate, & educator**

Using these principles of design justice and community technology, communities are developing alternative technologies and solidarity platforms grounded in their politics.

Corporate infrastructure can expose organizers and community members to state surveillance, as many of these platforms permit government agencies and police to monitor social movements. In response, organizers are developing their own technologies that allow them to control their data and the security protocols needed to protect it.[116] To that end, some technologists are building community-owned infrastructure to provide internet service to their communities. By installing high speed internet antennas that share gigabit connections with people’s home computers and building their own local wireless mesh networks, they are able to cut out the corporate middlemen.

In Detroit, the **Equitable Internet Initiative (EII)**[117]—a collaboration between Allied Media Projects and the **Detroit Community Technology Project (DCTP)**—is building community wireless networks and bringing digital education and empowerment to a city where 40% of residents don’t have access to the internet.[118] Their solar-powered infrastructure can withstand flooding, storms, and utility shutoffs. Free, open Wi-Fi networks also help with emergency response, like when Superstorm Sandy destroyed the power grid in Red Hook, Brooklyn.[119] Despite the loss of cell service, residents and responders were able to communicate through their community Wi-Fi network. DCTP consists of community technologists—those with the desire to design, build, and facilitate a healthy integration of technology into people’s lives and communities, allowing them the fundamental human right to communicate. DCTP works to demystify technology and expand digital literacy in their communities through community technology programs. Through the EII, they support historically marginalized residents to build and maintain neighborhood-governed internet infrastructure that fosters accessibility, consent, safety, and resilience. EII trains residents as Digital Stewards and works to strengthen neighborhoods through community organizing, participation, collaboration, and resilient infrastructure.

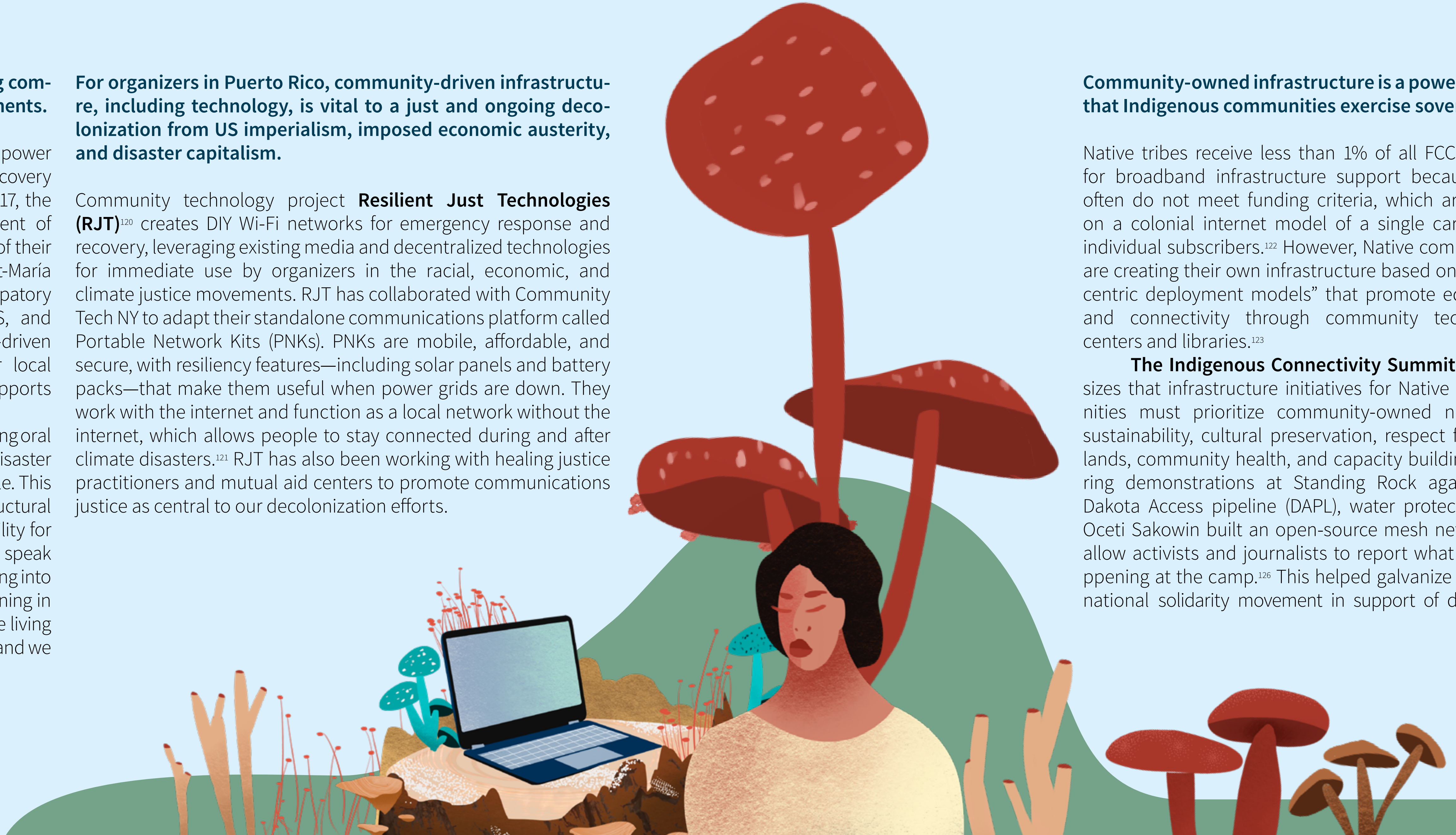
In a context of colonialism and climate disasters, building community resilience is critical for building power and movements.

Puerto Rico-based nonprofit **La Maraña** illustrates the power of design justice through its community participatory recovery model: "In the aftermath of hurricanes Irma and María in 2017, the failed government response sparked a collective movement of community-based initiatives that have come to the forefront of their communities' justice-based recovery." Its Imaginación Post-María initiative combines microfinancing, capacity-building, participatory budgeting, and design programs (such as Illustrator, GIS, and AutoCAD) to conduct mapping and planning for community-driven infrastructure projects. La Maraña has deep respect for local communities' relationship to the land, and the organization supports reclamation efforts as a central part of its methodology.

La Maraña begins each of its community maps by collecting oral histories, which are a powerful mapping tool when climate disaster has rendered the landscape of a neighborhood unrecognizable. This practice also records community members' desires for infrastructural changes. In this sense, La Maraña fashions a portal of possibility for a just future. One organizer described this process: "I tend to speak about the work that we're doing in communities as a way of going into a bubble. Sometimes I feel so overwhelmed by what's happening in Puerto Rico that when I go to the communities, I feel like we're living in a parallel universe, where we can dream, we can construct, and we can think of alternate lives."

For organizers in Puerto Rico, community-driven infrastructure, including technology, is vital to a just and ongoing decolonization from US imperialism, imposed economic austerity, and disaster capitalism.

Community technology project **Resilient Just Technologies (RJT)**[120] creates DIY Wi-Fi networks for emergency response and recovery, leveraging existing media and decentralized technologies for immediate use by organizers in the racial, economic, and climate justice movements. RJT has collaborated with Community Tech NY to adapt their standalone communications platform called Portable Network Kits (PNKs). PNKs are mobile, affordable, and secure, with resiliency features—including solar panels and battery packs—that make them useful when power grids are down. They work with the internet and function as a local network without the internet, which allows people to stay connected during and after climate disasters.[121] RJT has also been working with healing justice practitioners and mutual aid centers to promote communications justice as central to our decolonization efforts.



Community-owned infrastructure is a powerful way that Indigenous communities exercise sovereignty.

Native tribes receive less than 1% of all FCC funding for broadband infrastructure support because they often do not meet funding criteria, which are based on a colonial internet model of a single carrier and individual subscribers.[122] However, Native communities are creating their own infrastructure based on "tribally centric deployment models" that promote education and connectivity through community technology centers and libraries.[123]

The Indigenous Connectivity Summit emphasizes that infrastructure initiatives for Native communities must prioritize community-owned networks, sustainability, cultural preservation, respect for tribal lands, community health, and capacity building.[124] During demonstrations at Standing Rock against the Dakota Access pipeline (DAPL), water protectors[125] at Oceti Sakowin built an open-source mesh network to allow activists and journalists to report what was happening at the camp.[126] This helped galvanize an international solidarity movement in support of defending land and lives from extractive industries, even as private security firm Tigerswan launched cyber-attacks on activists and broke into fiber cable boxes on Standing Rock Sioux Tribe land.[127]

Other organizations forging solidarity platforms are **May First Movement Technology**, a nonprofit cooperative of movement organizations and activists across the US and Mexico that has created a solidarity platform that hosts over 10,000 email addresses and over 2,000 websites on collectively-owned, encrypted hardware.[128] **Palante Technology Cooperative** provides social justice-informed tech support, including data management and digital security, to movement organizations looking to use technology to advance their work.[129] **Riseup** is an autonomous tech collective that runs secure online communication tools, including its own email, chat servers, and VPN (virtual private network).[130] **VoterVox**, a project of **18MillionRising.org**, is a translation app that breaks down language barriers preventing limited English-proficient Asian American and Pacific Islander voters from participating in elections.[131]

> “We can’t create a magical policy to fix this. We can’t create one research project that’s going to unveil the entire thing. It is going to be a constant process where we have to be thinking about how to change the narrative and build power. And that can only happen with movement in communities that are directly impacted, involved and in the mix, and so funding has to be reflective.”
>
> campaign organizer

Movement technology is a resource-intensive investment because it is created by and for communities with a participatory design process that guarantees its accessibility and usefulness of the technology. Developing movement technology is critical for transforming the surveillance culture.

Developing solidarity platforms and tech tools for movement work is usually cost-prohibitive for small nonprofit organizations operating with limited budgets. Building platforms that aren’t just functional but also user-friendly is essential to moving from mainstream platforms to secure digital spaces. Creating successful movement technology requires long-term investment and support.

Data Defense and Stewardship

Organizers are creating healthier digital ecosystems that center data sovereignty and community-based training around digital security.[132]

The mainstream use of social media and search engine platforms is linked to increased surveillance; however, these same tools are necessary for effective organizing and community mobilization.

Because of the security risks posed by mainstream platforms, QT2SBIPOC organizers are increasingly switching to open source platforms that use E2E.

When they adopt encrypted technology, they shift the balance of power in the digital ecosystem because their data can no longer be captured and weaponized against them via social media intelligence (SOCMINT)[133]. But even those platforms marked as “progressive” aren’t always safe: the culture and economy of tech development continues to exclude QT2SBIPOC communities from the design process, resulting in products that may negatively impact these communities.

Holistic approaches to community capacity-building, education, and training around digital security are imperative to the larger abolitionist vision of social change and the fight against criminalization.

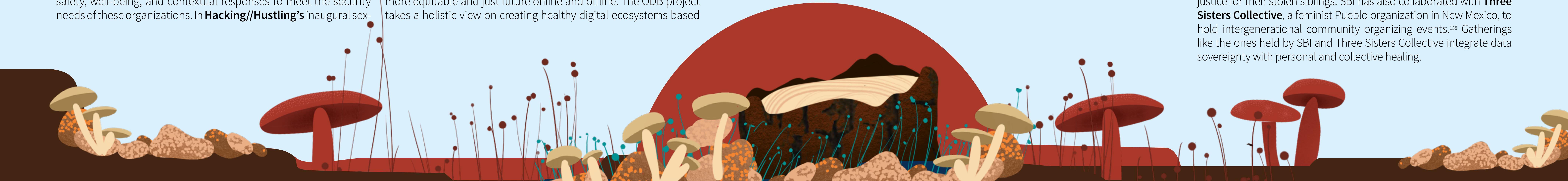
Most mainstream digital security resources and trainings focus on the security of an individual, which means they often fail to address systemic and community issues. Many grassroots organizations don't have IT staff or funding to update devices, which increases vulnerability to security breaches. For this reason, trainers adapt their approach to improving digital security protocol so it can be seamlessly integrated into an organization's existing infrastructure without placing burdensome and inaccessible demands on staff. Holistic safety addresses the technical risks that organizations encounter, and, equally as important, the somatic trauma that organizers and community members experience due to digital attacks and surveillance. Radical QT2SBIPOC digital security (digisec) and information security (infosec) trainers are bringing principles of holistic safety into their work, centering community safety, well-being, and contextual responses to meet the security needs of these organizations. In **Hacking//Hustling's** inaugural sex-worker led event in response to FOSTA-SESTA, they partnered with T4Tech, a trans and sex worker led organization, to lead the digital security trainings. Community members reported the importance of having trainers from their community lead the workshops and attributed it to why these trainings were more effective than previous efforts led by outside experts.

Organizers are designing tools and trainings for data defense and stewardship in response to how government agencies, tech companies, and corporations collect and weaponize data.

Organizations like the **Data Justice Program**[134] are actively fighting to end the conflation between surveillance/security and safety. They have been intricately involved in equitable census organizing and resistance to facial recognition and mass surveillance. Through the **Our Data Bodies' (ODB)** research, they determined that organizations who 'innovate' from a security or surveillance mindset, make already marginalized community members less safe. The program reshapes narratives and nurtures the existence of a more equitable and just future online and offline. The ODB project takes a holistic view on creating healthy digital ecosystems based on the principles of digital justice: access, participation, common ownership, and healthy communities.[135] Its recently created *Digital Defense Playbook* is a participatory training model that engages community members in learning about their data bodies, the ways their personal information is digitally collected, stored, and shared to surveil and criminalize them.[136] This work helps community members gain a more embodied understanding of the hidden flow of personal data between government and private agencies. One exercise, "What's In Your Wallet?," asks participants to examine the contents of their wallets (ID, credit cards, public benefits cards, etc.) and map the types of personal information that data-driven systems collect from them every day. They then learn how this data may be used to deny them access to public assistance, housing, employment, and other basic resources. ODB frames this analysis around how data-driven systems and technologies impede self-determination and chances for advancement in QT2SBIPOC communities. Participants are equipped to identify points of vulnerability and become informed stewards of their own data.

Organizations are fortifying their data sovereignty by conducting their own research, data collection, and data analysis for social justice, in addition to data stewardship.

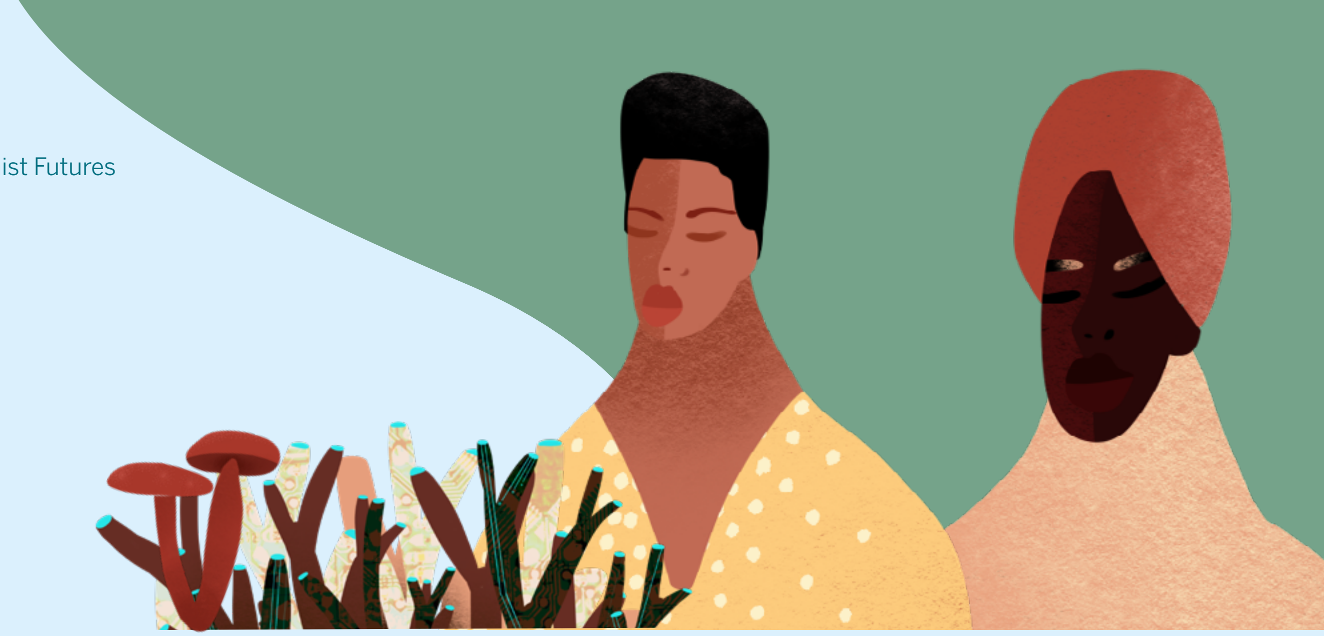
Indigenous feminist organizers are making critical connections between the importance of data ownership, land sovereignty, and gender justice with the **#MMIWGT2S (Missing and Murdered Indigenous Women and Girls, Trans, and Two Spirit People) campaign.** After noticing that official state reports grossly ignored or misrepresented the level of gender and sexual violence against Native communities, the **Sovereign Bodies Institute (SBI)** created its own comprehensive #MMIWGT2S database to honor the Indigenous women, girls, trans, and two-spirit people who have gone missing or been murdered.[137] Researchers from SBI centered Indigenous methodologies in gathering data about the identities of those in the database, including information left out of state reporting about whether these individuals ever returned to their tribal communities, received a traditional burial ceremony, or were targeted as sex workers. The database serves as a resource for activists and advocates to seek justice for their stolen siblings. SBI has also collaborated with **Three Sisters Collective**, a feminist Pueblo organization in New Mexico, to hold intergenerational community organizing events.[138] Gatherings like the ones held by SBI and Three Sisters Collective integrate data sovereignty with personal and collective healing.



Healing as an Abolitionist Technology

> “
>
> Healing justice is part of our abolition work. It is to equip folks with the memory of healing in us so that we don’t call the police to address a situation, but rather we take care of ourselves and each other. We’re not turning to the violent state...we’re actually resolving it ourselves. A lot of our work is intentionally to build the alternative as we’re trying to shut down or dismantle these systems. We will be much more powerful when we notice how much state violence impacts us and we’re able to end it within ourselves. Because if we’re well and we stop harming each other, I don’t see what else could stop us.
>
> ”

healing justice practitioner & organizer



Building movements that are powerful and sustainable enough to dismantle systems of oppression necessitates healing the personal, collective, and generational trauma that these systems cause.

In our previous report, *Healing Justice: Building Power, Transforming Movements*, we were excited to show how QT2SBIPOC organizers have long known and developed practices to support healing and resiliency as part of building community power—a framework known as healing justice.[139] Having become deeply skilled in conflict resolution, community accountability methods, and transformative justice[140] (which seeks solutions that do not use punishment, incarceration, or policing), movement organizations are creating interdependent networks of care within their communities as alternatives to reliance on the state. These organizations support addressing harm and resolving conflict without involving the systems that enact violence upon QT2SBIPOC communities.

These care networks provide communities with resources to develop their own protective practices from a place of healing the harms of internalized state violence. These holistic approaches integrate abolition, healing justice, and holistic safety into their organizing strategies.

For example, **Dignity and Power Now (DPN)** supports “communities most impacted by mass incarceration and state violence with tools to interrupt, respond to and mitigate the harms of violence by law enforcement agencies.”[141] They coordinate a rapid response network of organizers “who act as Healing Justice first responders following an act of police brutality” and who serve as listeners, police de-escalators, street medics, and healers. To transform systems of oppression, DPN believes in resourcing individual and collective healing and resilience with healing modalities that will “help lessen dependency on the state to respond to crisis in communities.”[142] More organizations are centering healing justice in their rapid response to digital and physical attacks, including working with movement funders to resource time for frontline organizers to recover from the toll of these attacks so that they can take care of themselves, prevent burnout, and continue to stay engaged in movement building.

> “People need resources to heal from emotional, psychological, and physical harm in order to keep doing the work. Our movement work as LGBTQI activists of color is made stronger when we lose fewer people.”
>
> community organizer

Healing Justice is a strategy that strengthens communities, an intentional and direct counterbalance to the ways in which tech surveillance and mass criminalization disaggregate and disrupt organizational power.

Community-based healing justice circles are another way in which organizers work toward abolition. Healing circles seek to heal generational trauma, they honor the ancestors whose work was the foundation of current resistance movements. These healing justice circles carry forward and draw upon indigenous practices of ceremony and medicine to foster healthy, sustainable movements for decades to come.

Southerners on New Ground (SONG), an LGBTQI liberation organization fostering a multi-issue justice movement in the South, hosts intergenerational circles where members listen together to audio recordings of SONG'S founders sharing stories about the organization's early resistance work, such as fighting the Ku Klux Klan in the 1990s.[143] This cross-generational passing of stories preserves SONG's history and connects members across different eras of movement building to strengthen SONG's base as it faces new and ongoing threats from surveillance technology.

CONCLUSION

In this report we explore the way that policing and criminalization are themselves technologies deeply rooted in white supremacy and how the high-tech interventions that are being deployed to police and surveil QT2SBIPOC communities are merely new extensions of the prison industrial complex that expand the control of the state. The stories shared in this report uplift the experiences of movement organizers and map often invisible and hidden processes of criminalization as they intersect with technologies of surveillance. We highlight the resilience and ingenuity of communities fighting back against carceral tech as they build networks of care and protection while simultaneously dexterously navigating and adapting to the rapid development of new carceral technologies.

We outlined key elements of these oppressive regimes, particularly as they impact communities of color and other groups oppressed by the US' neoliberal, white, capitalist, patriarchal, heteronormative system. Movement organizers continue to show the power of movement technology when developed by and for community. Moreover, their visions, values, and programming provide clear pathways forward in the struggle for justice in an increasingly digital world. With their lead, we conclude this report with a renewed call for long-term responsive funding initiatives that support organizations addressing the root causes of systemic inequality, challenge dominant narratives of criminalization and surveillance, and, ultimately, echo and affirm abolitionist organizing and self-determination.

GLOSSARY

Abolition: A vision and iterative practice that examines the root causes of systemic and interpersonal violence and how dominant narratives of policing have become internalized in our collective thinking so as to seem natural. It is the antithesis of surveillance culture.

Abolitionist technologies: As defined by the Stop LAPD Spying Coalition (SLSC), abolitionist technologies include creative interventions that use art, media, and performance to galvanize public support against state-backed surveillance technology. This is sometimes also referred to as anti-carceral technology.

Algorithmic suppression: A tool used by platforms that generates algorithms to censor content without transparency around how these censoring decisions are made.

Carceral technology: Carceral technologies are those that are bound up in the control, coercion, capture, and exile of entire categories of people. This term was coined by the carceral tech resistance network.

Community technology: This practice unites organizers and technologists to address the lack of equity in access to technology. It has six guiding principles, as articulated at the Community Technology Network Gathering at the Allied Media Conference: access, empowerment, privacy, ownership, resource sharing, and collective expression.

Community-owned infrastructure: The practice of communities sidestepping internet service providers and cable companies and building their own local wireless mesh networks to connect community members to the internet.

Consentful technology: Centers consent as a core value of empowering communities to access technology. This term was coined by the Allied Media Consentful Tech Project.

Data bodies: The ways personal information is digitally collected, stored, and shared to surveil and criminalize. This term was developed by Our Data Bodies.

Data sovereignty: The right to govern the collection, ownership, and application of a nation or community's own data. This definition was adapted from the 2017 Data Governance for Native Nation Rebuilding Report.

Decarceration: A process of reducing the rate of imprisonment, the number of persons in prison, and the institutions which facilitate incarceration and policing.

Decolonization: The process of gaining and claiming independence from colonial systems and powers through self-determination. According to "Decolonizing Technology" by Beatrice Martini, by linking that concept to the modern technology landscape, we are able to see the ways in which imperialist power dynamics and ideals exist within current technological networks and infrastructure, and how to address the harms they cause.

Deplatforming: A process of social media companies, financial technologies, and news platforms banning individuals from sharing content. Deplatforming is typically framed as a mechanism to stop the spread of alt-right 'high-risk' speech or 'controversial speech' on online platforms. However, it is often used to target sex workers.

Design justice: A theory and practice that centers engagement of communities in the design and development of technologies that impact them. It also focuses on how objects, technology, and systems create threats and advantages for different populations.

E-carceration: The use of wearable electronic monitors to deny the freedom of movement and self-determination of individuals on parole and probation.

Healing justice: This framework centers resiliency and survival practices that advance the collective safety and emotional, environmental, mental, physical, and spiritual well-being of communities with an eye toward long-term sustainability.

Holistic safety: A practice that addresses the technical risks that organizations encounter, and, equally as important, the somatic trauma that organizers and community members experience due to digital attacks and surveillance.

Internet autonomy: This refers to the right to access the internet without the threat of censorship or digital attack, especially by the government. We use this terminology instead of "internet freedom," which is politically linked to US imperialism.

Land sovereignty: This is the ability and right of Indigenous communities to decolonize and steward their ancestral lands. It is critical to Native people self-determining their future and healing from the destruction and genocide of settler colonialism.

Mass criminalization: A culture where aggressive policing and incarceration serve as the default tools for addressing social problems that should be solved by other strategies that eliminate the underlying inequities that disadvantage communities of color. It masquerades as a method of maintaining public safety and aggressively targets People of Color and people living below the poverty line.

GLOSSARY

Mass incarceration: A set of policies that has caused an enormous rise in the number of Black and brown people in prisons and immigration detention centers. It has also encouraged the hyper-policing of whole communities by law enforcement and government agencies.

Mass surveillance: Practices of monitoring and scrutinizing targeted communities using ever-improving technologies. Often, data gathered through these means are simultaneously used to extend and defend mass criminalization, while also rationalizing future surveillance projects as a 'preventative' measure.

Movement-based research: The use of surveys, focus groups, and other research methods in order to assess the risks, needs, impacts, goals, and visions of an issue. Designed by and for communities, it helps deepen organizers' understanding of issues and structures while also creating new forms of knowledge rooted in experience, context, and social justice.

Movement technology: Tools created and used by organizers to improve their capabilities to address their needs and those of their communities. These range from social media to apps, projects, and digital spaces adapted to support community and self-determination, resistance, and resilience.

Platform moderation: Set of tools and algorithms a platform uses to moderate the visibility of content on their platform. This is also known as content moderation. For example, shadowbanning is a type of content moderation.

Predictive policing: "Data-driven" surveillance practices that turn entire neighborhoods into vectors of criminal probability via the use of software that supposedly determines who is considered a "criminal" and where crime is "likely" to happen. It's one of the most dangerous forms of community-level algorithmic violence.

Prison industrial complex (PIC): Defined by Critical Resistance as "The overlapping interests of government and industry that use surveillance, policing, and imprisonment as solutions to economic, social, and political problems."

QT2SBIPOC: An abbreviation for Queer, Trans and Two-Spirit, Black, Indigenous, and People of Color.

Shadow banning: The covert blocking of a user's content such that they may not know they are being invisibilized. Shadowbanning is a type of content moderation.

Smart border: A surveillance network of artificial intelligence, drones, cameras, and infrared sensors, that is incorrectly touted as a more humane alternative to the Trump administration's draconian border wall project.

Social media intelligence (SOCMINT): The monitoring and gathering of information on social media platforms, whether the information is public or shared with a private group.

Somatics: This practice integrates the body, mind, and environment for personal healing with a collective social aim. It creates new, healthy ways of interacting with the world that can push movements forward.

Stalker state: A term coined by the Stop LAPD Spying Coalition to describe the network of overlapping data-sharing systems between social media corporations, private security firms, public service institutions, military departments, federal agencies, and local law enforcement.

Surveillance: Continuous observation of a place, person, group, or ongoing activity in order to gather information, often targeting disenfranchised populations (BIPOC, migrants) for the purpose of controlling them and limiting the impact of their actions.

Surveillance capitalism: A system of collaboration between the US government and private tech companies where corporations profit from making surveillance products.

Surveillance technology: Tools used by the state, other systems of policing, and individuals to complete and enhance social control, criminalization, and monitoring of communities. Expanded by capitalist and technological advances, these tools provide data for dominant narratives of governance and safety, expand the prison industrial complex, and increase the profit margin of participating companies across racialized, colonial, and patriarchal lines.

Transformative justice: An approach to addressing violence and harm that is rooted in community-based interventions and accountability. In seeking to break cycles of violence and manifest authentic social change, it turns away from the idea that punishment equates to justice and, instead, calls on practitioners to envision ways of acknowledging and repairing harm through self-determination, healing, and non-isolationist tactics.

Two-Spirit: Among Indigenous North American culture, Two-Spirit refers to individuals whose spirits are a blending of male and female spirit. Two-Spirit is essentially a third gender recognized in many Indigenous cultures.

ENDNOTES

[1] Stop LAPD Spying Coalition, “Before the Bullet Hits the Body,” (May 8, 2018), https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf.

[2] Malkia Devich Cyril, “Defund Facial Recognition,” The Atlantic (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/.

[3] Ariana Dongus, “Galton’s Utopia – Data Accumulation in Biometric Capitalism,” spheres: Journal for Digital Cultures (November 20, 2019), https://spheres-journal.org/contribution/galtons-utopia-data-accumulation-in-biometric-capitalism/

[4] Opal Tometi and Terence Courtney, “The State of Our Communities: Understanding Mass Incarceration and Migrant Detention.” BAJI: Black Alliance for Justice Immigration Resource Files (n.b.), https://www.racialequitytools.org/resourcefiles/BAJI_framingpaper.pdf .

[5] For more analysis on the history of surveillance and racism, see Simone Browne, Dark Matters: On the Surveillance of Blackness (Duke University Press, 2015), https://www.dukeupress.edu/dark-matters.

[6] Simone Browne, Dark Matters: On the Surveillance of Blackness (Duke University Press, 2015), https://www.dukeupress.edu/dark-matters.

[7] For an excellent resource on the history of mass incarceration and criminalization in the US, see Andrea J. Ritchie and Beth E. Richie, “The Crisis of Criminalization: A Call for a Comprehensive Philanthropic Response,” New Feminist Solutions (2017), http://bcrw.barnard.edu/wp-content/nfs/reports/NFS9-Challenging-Criminalization-Funding-Perspectives.pdf.

[8] Wendy Sawyer and Peter Wagner, “Mass Incarceration: The Whole Pie 2020,” Prison Policy Initiative (March 24, 2020), https://www.prisonpolicy.org/reports/pie2020.html.

[9] Alexia Ramirez, “ICE Records Confirm that Immigration Enforcement Agencies are Using Invasive Cell Phone Surveillance Devices,” ACLU (May 27, 2020), https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices/.

[10] Erin Taylor, “Sex Workers Are at the Forefront of the Fight Against Mass Surveillance and Big Tech,” Observer (November 12, 2019), https://observer.com/2019/11/sex-workers-mass-surveillance-big-tech/.

[11] Save Internet Freedom Tech, “Save Internet Freedom: Support the Open Technology Fund,” (August 24, 2020), https://saveinternetfreedom.tech/.

[12] Dr. Shoshana Zuboff, the author of The Age of Surveillance Capitalism, defines surveillance capitalism as “the unilateral claiming of private human experience as free raw material for translation into behavioral data” in a recent interview. https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

[13] Mike Giglio, “Would You Sacrifice Your Privacy to Get Out of Quarantine?,” The Atlantic (April 22, 2020), https://www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172/

[14] James Kilgore, “Big Tech Is Using the Pandemic to Push Dangerous New Forms of Surveillance,” TRUTHOUT, (June 22, 2020), https://truthout.org/articles/big-tech-is-using-the-pandemic-to-push-dangerous-new-forms-of-surveillance/.

[15] Human Rights Watch, “End Internet Shutdowns to Manage COVID-19,” (March 31, 2020), https://www.hrw.org/news/2020/03/31/end-internet-shutdowns-manage-covid-19.

[16] Tawana Petty, Defending Black Lives Means Banning Facial Recognition, Wired (July 10, 2020), https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/.

[17] Kade Crockford, “How is Face Recognition Surveillance Technology Racist?,” (June 16, 2020), https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/.

[18] This report defines abolition as a vision and iterative practice that examines the root causes of systemic and interpersonal violence and how dominant narratives of policing have become internalized in our collective thinking so as to seem natural. It is the antithesis of surveillance culture.

[19] Critical Resistance, “Reformist reforms vs. abolitionist steps in policing.” (n.d.), https://static1.squarespace.com/static/59ead8f9692ebee25b72f17f/t/5b65cd58758d46d34254f22c/1533398363539/CR_NoCops_reform_vs_abolition_CRside.pdf.

[20] Arguing that “security and safety aren’t the same,” Mariame Kaba develops a sharp analysis of holistic safety in a security state in this interview with The Next System Project: https://thenextsystem.org/learn/stories/towards-horizon-abolition-conversation-mariame-kaba

[21] For more information on Healing Justice, please see Healing Justice: Building Power, Transforming Movements report

[22] History.com Editors, “Jim Crow Laws,” (February 28, 2018), https://www.history.com/topics/early-20th-century-us/jim-crow-laws.

[23] Sarah Childress, “The Problem with “Broken Windows” Policing,” PBS (June 28, 2016), https://www.pbs.org/wgbh/frontline/article/the-problem-with-broken-windows-policing/.

[24] Three Strikes Project, “Three Strikes Basics,” (n.b.) Stanford Law School, https://law.stanford.edu/stanford-justice-advocacy-project/three-strikes-basics/.

[25] For more on California’s “architecture of surveillance,” see: Stop LAPD Spying Coalition, “The Architecture of LAPD Surveillance,” (n.d.), https://stoplapdspying.org/resources/architecture/.

[26] Michelle Alexander, The New Jim Crow: Mass Incarceration in the Age of Colorblindness (NY: The New Press, 2010).

[27] According to Mimi Onuoha and Diana Nucera, A People’s Guide to AI, artificial intelligence refers to the “theory and development of computer systems able to perform tasks that normally require human intelligence.” An algorithm is “a series of steps or set of rules [used by computer systems] for solving or performing a task.” https://alliedmedia.org/files/peoples-guide-ai.pdf.

[28] Joy Buolamwini, “InCoding—In The Beginning,” MIT Media Lab (May 16, 2016), https://medium.com/mit-media-lab/incoding-in-the-beginning-4e2a5c51a45d#.efx8zxith.

[29] Ruha Benjamin, Race after Technology (Polity Press, 2019).

[30] Rashida Richardson, Jason Schultz, and Kate Crawford, “Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice,” New York University Law Review Online, (February 13, 2019), https://papers.ssrn.com/abstract=3333423.

[31] Stop LAPD Spying Coalition, “Before the Bullet Hits the Body—Dismantling Predictive Policing in Los Angeles,” (2018), https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf.

[32] Joy Buolamwini, “InCoding — In The Beginning”

[33] Stop LAPD Spying Coalition, “Before the Bullet Hits the Body—Dismantling Predictive Policing in Los Angeles,” (2018), https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf.

[34] Ali Winston, “Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology,” The Verge (February 27, 2018), https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd.

[35] Stop LAPD Spying Coalition, “Before the Bullet Hits the Body—Dismantling Predictive Policing in Los Angeles,” (2018), https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf.

[36] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, “Machine Bias,” ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[37] James Kilgore, Emmett Sanders, and Myaisha Hayes, “No More Shackles: Why We Must End the Use of Electronic Monitors for People On Parole (2018),” MediaJustice, (September 16, 2018), https://centerformediajustice.org/wp-content/uploads/2018/10/NoMoreShackles_ParoleReport_UPDATED.pdf.

[38] Alexi Jones, “Correctional Control 2018: Incarceration and Supervision by State,” Prison Policy Initiative, (December 2018), https://www.prisonpolicy.org/reports/correctionalcontrol2018.html.

[39] James Kilgore and Myaisha Hayes, “#ChallengingEcarceration: Guidelines for Respecting the Rights of Individuals on Electronic Monitors,” The Center for Media Justice, (March 2018), https://mediajustice.org/wp-content/uploads/2019/03/electronic-monitoring-guidelines-final.pdf.

[40] Tommy Walters, “Critics Decry Surveillance App that Tracks Undocumented Immigrants,” Medium (October 22, 2019), https://medium.com/the-gotham-grind/critics-decry-surveillance-app-that-tracks-undocumented-immigrants-95ec30a2ed2c

[41] James Kilgore, “Big Tech Is Using the Pandemic to Push Dangerous New Forms of Surveillance,” Truthout.org, (June 22, 2020), https://truthout.org/articles/big-tech-is-using-the-pandemic-to-push-dangerous-new-forms-of-surveillance.

[42] James Kilgore, Sanders Emmett, and Myaisha Hayes, “The Center for Media Justice | No More Shackles Report,” accessed March 19, 2019, https://centerformediajustice.org/our-projects/challengingecarceration-electronic-monitoring/nomoreshackles/.
James Kilgore, Sanders Emmett, and Myaisha Hayes, “The Center for Media Justice | No More Shackles Report,” accessed March 19, 2019, https://centerformediajustice.org/our-projects/challengingecarceration-electronic-monitoring/nomoreshackles/.

[43] James Kilgore, Sanders Emmett, and Myaisha Hayes, “The Center for Media Justice | No More Shackles Report,” accessed March 19, 2019, https://centerformediajustice.org/our-projects/challengingecarceration-electronic-monitoring/nomoreshackles/.

[44] MediaJustice, “Racism, Transphobia, and Electronic Monitoring,” Medium, (September 27, 2019), https://medium.com/nodigitalprisons/racism-transphobia-and-electronic-monitoring-85ef4f1e6b84.

[45] James Kilgore, Sanders Emmett, and Myaisha Hayes, “The Center for Media Justice | No More Shackles Report,” accessed March 19, 2019, https://centerformediajustice.org/our-projects/challengingecarceration-electronic-monitoring/nomoreshackles/.

[46] Burcu Kilic with Scott Hulver, “Public Citizen Report: Workplace Privacy After COVID-19,” (August 13, 2020) https://www.citizen.org/article/workplace-privacy-after-covid-19/

[47] Jacob Demmitt, “85 Percent of Amazon’s Black US Workers Hold Unskilled Jobs,” Puget Sound Business Journal, (June 11, 2015), https://www.bizjournals.com/seattle/blog/techflash/2015/06/85-percent-of-amazon-s-black-u-s-workers-hold.html.

[48] James Kilgore, Emmett Sanders, and Myaisha Hayes, “No More Shackles: Why We Must End the Use of Electronic Monitors for People On Parole (2018),” MediaJustice, (September 16, 2018), https://centerformediajustice.org/wp-content/uploads/2018/10/NoMoreShackles_ParoleReport_UPDATED.pdf.

[49] Stingrays, also known as “cell site simulators” or “IMSI catchers,” are invasive cell phone surveillance devices that mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information. When used to track a suspect’s cell phone, they also gather information about the phones of countless bystanders who happen to be nearby. To learn more, read ACLU’s “Stingray Tracking Devices: Who’s Got Them?,” (November 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them

[50] Matt Binder, “Officials who say they’re ‘contact tracing’ protesters hurt the fight against COVID-19,” Mashable (June 5, 2020), https://mashable.com/article/contact-tracing-protesters/.

[51] Stop LAPD Spying Coalition, “The Architecture of LAPD Surveillance,” (n.d.), https://stoplapdspying.org/resources/architecture/.

[52] Marinus Analytics, “Traffic Jam,” (n.d.), https://www.thorn.org/spotlight/ and https://www.marinusanalytics.com/traffic-jam.

[53] Danielle Blunt, Emily Coombes, Shanelle Mullin, and Ariel Wolf , “Posting Into the Void: Studying the Impact of Shadowbanning on Sex Workers and Activists. A community report by Hacking//Hustling” https://hackinghustling.org/posting-into-the-void-content-moderation/

[54] The US government’s weaponization of data isn’t a new phenomenon. The Fugitive Slave Act of 1850 is an early documented instance where government and private mercenaries (slave catchers) used data collection and communications technology (print media) to criminalize and detain Black people who freed themselves from slavery via the Underground Railroad. Read more of this history by visiting Alvaro M. Bedoya’s article “What Happens When We Let Industry and Government Collect All the Data They Want,” Slate Magazine (November 7, 2014), https://slate.com/technology/2014/11/big-data-underground-railroad-history-says-unfettered-collection-of-data-is-a-bad-idea.html.

[55] Kim Zetter, “How Cops Can Secretly Track Your Phone,” The Intercept (July 31, 2020), https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/

[56] American Civil Liberties Union, “Stingray Tracking Devices: Who’s Got Them?,” (November 2018), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them

[57] George Joseph, “NYPD Officers Accessed Black Lives Matter Activists’ Texts, Documents Show,” The Guardian (April 4, 2017), https://www.theguardian.com/us-news/2017/apr/04/nypd-police-black-lives-matter-surveillance-undercover.

[58] Jana Winter and Sharon Weinberger, “The FBI’s New US Terrorist Threat: ‘Black Identity Extremists,’” Foreign Policy (2017), https://foreignpolicy.com/2017/10/06/the-fbi-has-identified-a-new-domestic-terrorist-threat-and-its-black-identity-extremists/.

[59] James Vincent, “NYPD used facial recognition to track down Black Lives Matter activist,” (August 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram. \

[60] Kate Cox, “Cops in Miami, NYC arrest protestors from facial recognition matches,” Arts Technica (August 19, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/

[61] Aaron Mackey, The PACT Act’s Attempt to Help Internet Users Hold Platforms Accountable Will End Up Hurting Online Speakers (July 21, 2020), https://www.eff.org/deeplinks/2020/07/pact-acts-attempt-help-internet-users-hold-platforms-accountable-will-end-hurting

[62] “End-to-end encryption (E2EE) is a method of secure communication that prevents third-parties from accessing data while it’s transferred from one end system or device to another. In E2EE, the data is encrypted on the sender’s system or device and only the recipient is able to decrypt it. Nobody in between, be they an internet service provider, application service provider, or hacker, can read it or tamper with it.” See: https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE.

[63] Malware gives the attacker access to anything and everything happening on the device affected, as well as record sounds and trigger cameras attached. The exact function and access depends on what the malware is, what devices it has infected and how it is used. Malware has been found within malicious ads, within PDFs sent over email, within ASUS software updates, within Google Play applications, and on the phones of slain journalists.

[64] American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), and National Association of Criminal Defense Lawyers (NACDL) 2017 “Challenging Government Hacking in Criminal Cases” Guide. https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf.

[65] Geolocation refers to tracking a person’s real-time geographic location through their cell phone signal or internet-connected device.

[66] Brandon E. Patterson, “Black Lives Matter Organizers Were Labeled as ‘Threat Actors’ by a Cybersecurity Firm,” Mother Jones, (2015), https://www.motherjones.com/politics/2015/08/zerofox-report-baltimore-black-lives-matter/.

[67] Benjamin Powers, “How Police Use Social Media to Track and Target Activists of Color,” Complex (November 17, 2016), https://www.complex.com/life/2016/11/police-surveillance-activists-people-of-color.

[68] Will Parrish, “The US Border Patrol and an Israeli Military Contractor Are Putting a Native American Reservation Under ‘Persistent Surveillance,’” The Intercept (August 25, 2019), https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance/.

[69] Adi Robertson, “Border agents are checking entrants’ Facebook and Twitter profiles — but we still don’t know how closely.” The Verge (August 31, 2019), https://www.theverge.com/2019/8/31/20837448/social-media-dhs-cbp-surveillance-us-border-ismail-ajjawi-harvard.

[70] McKenzie Funk, “How ICE Picks Its Targets in the Surveillance Age,” (October 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html.

[71] Mijente, National Immigration Project, and Immigration Defence Project, “Who’s Behind ICE? The Tech and Data Companies Fueling Deportations,” (October 23, 2018), https://www.nationalimmigrationproject.org/PDFs/community/2018_23Oct_whos-behind-ice.pdf.

[72] César Cuauhtémoc García Hernández, “Creating Crimmigration,” Brigham Young University Law Review no. 14-12 (2014): 1457-1516. https://ssrn.com/abstract=2393662.

[73] Stephen Rex Brown, “ICE Arrests of Undocumented Immigrants at NYC Courthouses Increase Again in 2018: Report,” NY Daily News (January 27, 2019), https://www.nydailynews.com/new-york/ny-metro-ice-arrests-nyc-courthouses-20190125-story.html.

[74] Mijente, National Immigration Project, and Immigration Defence Project, “Who’s Behind ICE? The Tech and Data Companies Fueling Deportations,” (October 23, 2018), https://www.nationalimmigrationproject.org/PDFs/community/2018_23Oct_whos-behind-ice.pdf

[75] Mijente, “Palantir Played Key Role in Arresting Families for Deportation, Document Shows,” (May 2, 2019), https://mijente.net/2019/05/02/palantir-arresting-families/.

[76] Angela Chen, “How Far Has Technology Come Since the Last ‘Smart Border’ Failed?,” The Verge (February 22, 2019), https://www.theverge.com/2019/2/22/18236515/smart-border-virutal-fence-surveillance-trump-borders-politics-policy.

[77] Will Parrish, “The US Border Patrol and an Israeli Military Contractor Are Putting a Native American Reservation Under ‘Persistent Surveillance,’” The Intercept (August 25, 2019), https://theintercept.com/2019/08/25/border-patrol-israel-elbit-surveillance/.

[78] Shoshana Wodinsky, “Palmer Luckey’s Border Control Tech Has Already Caught Dozens of People,” The Verge, (June 11, 2018), https://www.theverge.com/2018/6/11/17448552/border-control-tech-security-lattice-palmer-luckey.ky.

[79] Alex Leblang, “Continuous Immigration Vetting: The Labyrinth of Government Databases Continues to Grow,” Privacy SOS, (February 28, 2019), https://privacysos.org/blog/continuous-immigration-vetting-labyrinth-government-databases-continues-grow/.

[80] Cloud hosting refers to the availability of computing services, database storage, and, in the case of AWS, technologies like machine learning and data analytics, via a network of remote data centers. For more information, visit: https://aws.amazon.com/what-is-aws/.

[81] Mijente, National Immigration Project, and Immigration Defence Project, “Who’s Behind ICE? The Tech and Data Companies Fueling Deportations,” (October 23, 2018), https://www.nationalimmigrationproject.org/PDFs/community/2018_23Oct_whos-behind-ice.pdf.

[82] Mijente, National Immigration Project, and Immigration Defence Project, “Who’s Behind ICE? The Tech and Data Companies Fueling Deportations,” (October 23, 2018), https://www.nationalimmigrationproject.org/PDFs/community/2018_23Oct_whos-behind-ice.pdf.

[83] Vasudha Talla, “Documents Reveal ICE Using Driver Location Data From Local Police for Deportations,” ACLU of Northern California, (March 13, 2019), https://www.aclunc.org/blog/documents-reveal-ice-using-driver-location-data-local-police-deportations; see also Electronic Frontier Foundation, “Automated License Plate Readers (ALPRs),” (August 28, 2017), https://www.eff.org/pages/automated-license-plate-readers-alpr.

[84] Vasudha Talla, “Documents Reveal ICE Using Driver Location Data From Local Police for Deportations,” ACLU of Northern CA, March 13, 2019, https://www.aclunc.org/blog/documents-reveal-ice-using-driver-location-data-local-police-deportations; Electronic Frontier Foundation, “Automated License Plate Readers (ALPRs),” Electronic Frontier Foundation, August 28, 2017, https://www.eff.org/pages/automated-license-plate-readers-alpr.

[85] The Center for Sexual Pleasure and Health defines Whorephobia as, “Whorephobia is the fear or hatred of sex workers. The term was coined by sex worker activists to denote the explicit hateful and violent attitudes about sex workers. The word also stems from the belief that sex workers are a social problem, diseased, or unintelligent victims that need to be rescued.” http://www.thecsph.org/word-week-whorephobia/

[86] Danielle Blunt, Emily Coombes, Shanelle Mullin, and Ariel Wolf , “Posting Into the Void: Studying the Impact of Shadowbanning on Sex Workers and Activists. A community report by Hacking//Hustling” https://hackinghustling.org/posting-into-the-void-content-moderation/

87 Salty, “An Investigation into Algorithmic Bias in Content Policing of Marginalized Communities on Instagram and Facebook,” (October 22, 2019), https://www.saltyworld.net/wp-content/uploads/2019/10/Algorithmic_Bias_Salty_Oct222019-16.pdf.

88 Jillian C. York, “Facebook’s ‘Real Name’ Policy Can Cause Real-World Harm for the LGBTQ Community,” (September 16, 2014), https://www.eff.org/deeplinks/2014/09/facebooks-real-name-policy-can-cause-real-world-harm-lgbtq-community.

89 This report uses the terminology “internet autonomy” instead of “internet freedom” because the concept of internet freedom is politically linked to US imperialism. Internet autonomy refers to the right to access the internet without the threat of censorship or digital attack, especially by the government.

90 Ann Wagner, “H.R.1865 - 115th Congress (2017-2018): Allow States and Victims to Fight Online Sex Trafficking Act of 2017,” Congress.gov (April 11, 2018), https://www.congress.gov/bill/115th-congress/house-bill/1865.

91 Legal Information Institute, “47 US Code § 230. Protection for Private Blocking and Screening of Offensive Material,” (1996) https://www.law.cornell.edu/uscode/text/47/230.

92 Elliot Harmon and Jeremy Gillula, “Stop SESTA: Whose Voices Will SESTA Silence?,” Electronic Frontier Foundation (September 13, 2017) https://www.eff.org/deeplinks/2017/09/stop-sesta-whose-voices-will-sesta-silence.

93 A content moderation tactic also referred to as “reduced visibility.”

94 Removing an individual’s access to a public platform, typically through shutting down an account to limit ‘controversial speech’ on a platform.

95 Danielle Blunt, Emily Coombes, Shanelle Mullin, and Ariel Wolf , “Posting Into the Void: Studying the Impact of Shadowbanning on Sex Workers and Activists. A community report by Hacking//Hustling” https://hackinghustling.org/posting-into-the-void-content-moderation/

96 Aja Romano, “A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It,” Vox (July 2, 2018) https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.

97 Danielle Blunt, Emily Coombes, Shanelle Mullin, and Ariel Wolf , “Posting Into the Void: Studying the Impact of Shadowbanning on Sex Workers and Activists. A community report by Hacking//Hustling” https://hackinghustling.org/posting-into-the-void-content-moderation/

98 Critical Resistance, “What Is the PIC? What Is Abolition?,” (n.d.) http://criticalresistance.org/about/not-so-common-language/.

99 Mark Puente, “LAPD to Scrap Some Crime Data Programs after Criticism,” Latimes. Com, April 5, 2019, https://www.latimes.com/local/lanow/la-me-lapd-predictive-policing-big-data-20190405-story.html.

100 Stop LAPD Spying Coalition. 2018. “Before the Bullet Hits the Body – Dismantling Predictive Policing in Los Angeles.” https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf.

101 National Bail Out, “Black Mama’s Bail Out—National Bail Out,” (n.d.), https://nationalbailout.org/black-mamas-bail-out/.

102 Solutions Not Punishment Co, “SNAP4Freedom School,” (n.d.), https://www.snap4freedom.org/snap4freedom-school.

103 Rebecca Heilweil, “Big tech companies back away from selling facial recognition to police. That’s progress,” (June 11, 2020), https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police.

104 Mijente, “Palantir Played Key Role in Arresting Families for Deportation, Document Shows,” (May 2, 2019), https://mijente.net/2019/05/02/palantir-arresting-families/.

105 Mijente et al., “Who’s Behind Ice? The Tech and Data Companies Fueling Deportations,” October 23, 2018.

106 James Kilgore and Myaisha Hayes, “#ChallengingEcarceration: Guidelines for Respecting the Rights of Individuals on Electronic Monitors” (The Center for Media Justice, March 2018), https://mediajustice.org/wp-content/uploads/2019/03/electronic-monitoring-guidelines-final.pdf.

107 MediaJustice, “Guidelines for Respecting the Rights of Individuals on Electronic Monitors,” https://mediajustice.org/wp-content/uploads/2019/03/electronic-monitoring-guidelines-final.pdf.

108 Hacking//Hustling, “Erased: The Impact of FOSTA-SESTA,” (2020), https://hackinghustling.org/erased-the-impact-of-fosta-sesta-2020/.

109 Hacking//Hustling, “Erased: The Impact of FOSTA-SESTA,” (2020), https://hackinghustling.org/erased-the-impact-of-fosta-sesta-2020/.

110 May First Movement Technology, “Movement Technologist Statement,” (n.d.), https://outreach.mayfirst.org/techstatement.

111 Sasha Costanza-Chock, “Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice” Proceedings of the Design Research Society (June 3, 2018), . https://ssrn.com/abstract=3189696.

112 Sasha Costanza-Chock, “Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice” Proceedings of the Design Research Society (June 3, 2018), . https://ssrn.com/abstract=3189696

113 The Design Justice Network has created three zines: Principles for Design Justice, An Exhibit of Emerging Practices, and Design Justice for Action, deepening the principles defined in 2016. http://designjusticenetwork.org/zine.

114 Diana Nucera and Andy Gunn, “Building the Community Tech Movement at the 2015 Allied Media Conference,” Allied Media Projects (September 1, 2015), https://www.alliedmedia.org/news/2015/09/01/building-community-tech-movement-2015-allied-media-conference.

115 For more information, see the Consentful Tech Project: http://www.consentfultech.io/.

116 Sasha Costanza-Chock Maya Wagoner, Berhan Taye, Caroline Rivas, Chris Schweidler, Georgia Bullen, & the T4SJ Project, “#MoreThanCode: Practitioners Reimagine the Landscape of Technology for Justice and Equity,” MoreThanCode.cc (2018), https://morethancode.cc/T4SJ_fullreport_082018_AY_web.pdf.

117 Projects like the Equitable Internet Initiative prioritize building mesh networks for families on government assistance, elderly residents, and people living in areas vulnerable to climate disasters. For more on EII’s work, visit: https://detroitcommunitytech.org/eii.

118 Mozilla, “Connecting the Unconnected in Detroit,” Read, Write, Participate (February 20, 2018), https://medium.com/read-write-participate/connecting-the-unconnected-in-detroit-f56790bea8e0.

119 Angely Mercado, “How Community-Owned Wi-Fi Changes the Game for Poor Neighborhoods,” NationSwell (May 29, 2018), http://nationswell.com/wi-fi-connects-poor-neighborhoods/.

120 Allied Media, “Resilient Just Technologies follows the principles of the Detroit Digital Justice Coalition: Access, Participation, Common Ownership, and Healthy Communities,” (n.d.), https://www.alliedmedia.org/resilient-just-tech.

121 Fairness and Accuracy in Reporting, “Teresa Basilio on Puerto Rico Communication Failure, Amrah Salomon on Indigenous Peoples Day,” (October 12, 2018), https://fair.org/home/teresa-basilio-on-puerto-rico-communication-failure-amrah-salomon-on-indigenous-peoples-day/.

122 Mark Goldstein, “Tribal Broadband: FCC’s Data Overstate Access, and Tribes Face Barriers Accessing Funding,” United States Government Accountability Office (October 3, 2018) https://www.gao.gov/assets/700/694934.pdf.

123 Miriam Jorgensen, Traci Morris, and Susan Feller, “Digital Inclusion in Native Communities: The Role of Tribal Libraries.” Association of Tribal Archives, Libraries, and Museums (2014), https://www.atalm.org/sites/default/files/Report%20for%20Printing.pdf.

124 Natalie Campbell, “Indigenous Connectivity Summit Community Report,” Internet Society (2018), https://muninetworks.org/sites/www.muninetworks.org/files/2018-01-04-ICS-Report-final.pdf.

125 #NoDAPL Standing Rock Water Protectors, “#NoDAPL Archive: Standing Rock Water Protectors,” (2019), http://www.nodaplarchive.com/news-articles.html.

126 Lisha Sterling, “How We Brought the Internet to Standing Rock,” Opensource.com (June 1, 2017), https://opensource.com/article/17/6/internet-standing-rock.

127 C.S. Hagen, “IT Specialists Investigate Cyber Warfare Crimes at Standing Rock,” High Plains Reader (July 12, 2017), https://hpr1.com/index.php/feature/news/it-specialists-investigate-cyber-warfare-crimes-at-standing-rock.

128 For more on May First Movement, visit: https://mayfirst.coop/en/.

129 For more on Palante Technology Cooperative, visit: https://palantetech.coop/about.

130 Riseup’s VPN allows internet users to anonymize their location, prevent surveillance from internet service providers, and avoid malware attacks through Riseup.net’s encrypted connection. Visit: https://riseup.net/en/vpn.

131 For more on VoterVox, visit: https://www.votervox.org/about?locale=en.
132 Rainie, Rodriguez-Lonebear, and Martinez argue that “Indigenous data sovereignty is the right of Indigenous peoples and tribes to govern the collection, ownership, and application of their own data” in the 2017 Policy Brief: Data Governance for Native Nation Rebuilding, http://nni.arizona.edu/application/files/8415/0007/5708/Policy_Brief_Data_Governance_for_Native_Nation_Rebuilding_Version_2.pdf. “ (Rainie et al. 2017b)

133 This refers to the process of monitoring and gathering of information on social media platforms, whether the information is public or shared with a private group.

134 Detroit Community Technology Project, “Data Justice,” https://detroitcommunitytech.org/?q=datajustice

135 T. Lewis, S.P. Gangadharan, S. P., M. Saba, and T. Petty. “Digital Defense Playbook: Community Power Tools for Reclaiming Data,” Our Data Bodies (2018), https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Spreads.pdf.

136 In “Digital Defense Playbook: Community Power Tools for Reclaiming Data,” T. Lewis, S.P. Gangadharan, S. P., M. Saba, and T. Petty argue that “Our data bodies are discrete parts of our whole selves that are collected, stored in databases, the cloud, and other spaces of digitally networked flows, and used to make decisions or determinations about us. They are a manifestation of our relationships with our communities and institutions, including institutions of privilege, oppression, and domination.” https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Spreads.pdf.

137 For more on the Sovereign Bodies Institute’s database and research, visit: https://www.sovereign-bodies.org/mmiw-database.

138 For more on #MMIWGT2S organizing, visit Three Sisters Collective: https://threesisterscollective.org/.

139 An excerpt from the Healing Justice Report: “The healing justice framework lifts up resiliency and survival practices that center the collective safety and emotional, physical, spiritual, environmental, and mental well-being of communities. These practices address the impacts of violence and trauma, including interpersonal, systemic, and generational violence, and they promote our collective safety, sustainability, and well-being. When integrated into movement strategies, these practices support us, as organizers and communities, to prioritize our safety and to care for each other towards our long-term survival.”

140 Ejeris Dixon and Leah Lakshmi Piepzna-Samarasinha, Beyond Survival: Strategies and Stories from the Transformative Justice Movement (Little Rock: Ak Press, 2020), https://www.akpress.org/beyond-survival.html.

141 Patrisse Cullors, “How Healing Justice For Survivors Of State Violence Can Help Mend Our Communities And Sustain Our Movements,” (May 21 2019), https://blavity.com/how-healing-justice-for-survivors-of-state-violence-can-help-mend-our-communities-and-sustain-our-movements.

142 Dignity and Power Now (DPN), “Healing Justice toolkit,” (n.d.), http://dignityandpowernow.org/wp-content/uploads/2019/05/Healing-Justice-Toolkit_PRINT_March-1.pdf.

143 For more on SONG, see: https://southernersonnewground.org/.

ACKNOWLEDGEMENTS

Technologies for Liberation: Toward Abolitionist Futures,

Suggested Citation: Pascal Emmer, Caroline Rivas, Brenda Salas Neves, Chris Schweidler. 2020. Technologies for Liberation: Toward Abolitionist Futures. Astraea Lesbian Foundation for Justice and Research Action Design. Available online at astraeafoundation.org/FundAbolitionTech

RESEARCH TEAM

The Astraea Lesbian Foundation for Justice is the only philanthropic organization working exclusively to advance LGBTQI human rights around the globe. Astraea was founded in 1977 by a cross-class, multi-racial group of women activists looking to fund a burgeoning women's movement that centered the leadership of lesbians and women of color. Through grantmaking, capacity building, philanthropic advocacy, and media and communications, we support brilliant and brave grantee partners in the US and internationally who challenge oppression and seed change. We work for racial, economic, social, and gender justice, because we all deserve to live our lives freely, without fear, and with dignity. In 2013, we launched the LGBTQI Racial Justice Fund affirming our long-standing commitment to advancing racial and economic justice. In 2014, we launched our CommsLabs programming, becoming the first funder to make a major investment in media, communications, and technology for LGBTQI communities globally. In 2018, Astraea committed to centering Healing Justice as a critical strategy for supporting grantee partners. Astraea invests in, advocates for, and amplifies LBTQI, feminist, and People of Color-led movements to bolster their power and sustainability. In our 40+ year history, we are proud to have granted more than $44 million to 1,700+ LBTQI activists and artists.

Research Action Design (RAD) uses community-led research, collaborative design of technology and media, and secure digital strategies to build the power of grassroots social movements. We are a worker-owned collective. Our work is grounded in the needs and leadership of communities in the struggle for justice and liberation. More about RAD can be found here: https://rad.cat/

GRATITUDE

This report is dedicated to the powerful Queer, Trans, Two-Spirit, Black, Indigenous, and People of Color (QT2SBIPOC) movements and movement technologists who are visioning and building towards liberatory futures. It is rooted in the groundwork of visionary abolitionists who are fighting to end policing, criminalization, and carceral technologies in all their forms, and it holds central the idea that "abolition is both a vision and a political strategy." We have learned so much from all of you, and are deeply grateful for the path you are forging for us all.

Technologies for Liberation: Toward Abolitionist Futures was made possible thanks to the contributions of so many individuals, activists, and organizations. We would like to thank and honor the many people who so generously shared their experiences and stories during interviews and workshops. Your stories and vision are the foundation of this research and the work ahead. We are so grateful to all of the research partners for their time, for sharing their expertise, and for their ongoing dedication and commitment to bringing this project to life.

The primary author of this report is Pascal Emmer, with writing and editing by Brenda Salas Neves, Caroline Rivas, Chris Schweidler, and Mihika Srivastava. We thank all of our research team members, whose dedication made this project possible: Pascal Emmer, Sophie Kreitzberg, Kyla Massey, Maya Richman, Caroline Rivas, Celiany Rivera-Velázquez, Brenda Salas Neves, Chris Schweidler.

Thank you to J. Bob Alotta, whose vision helped plant the seeds for this work. We are grateful for her critical leadership and guidance as this project unfurled.

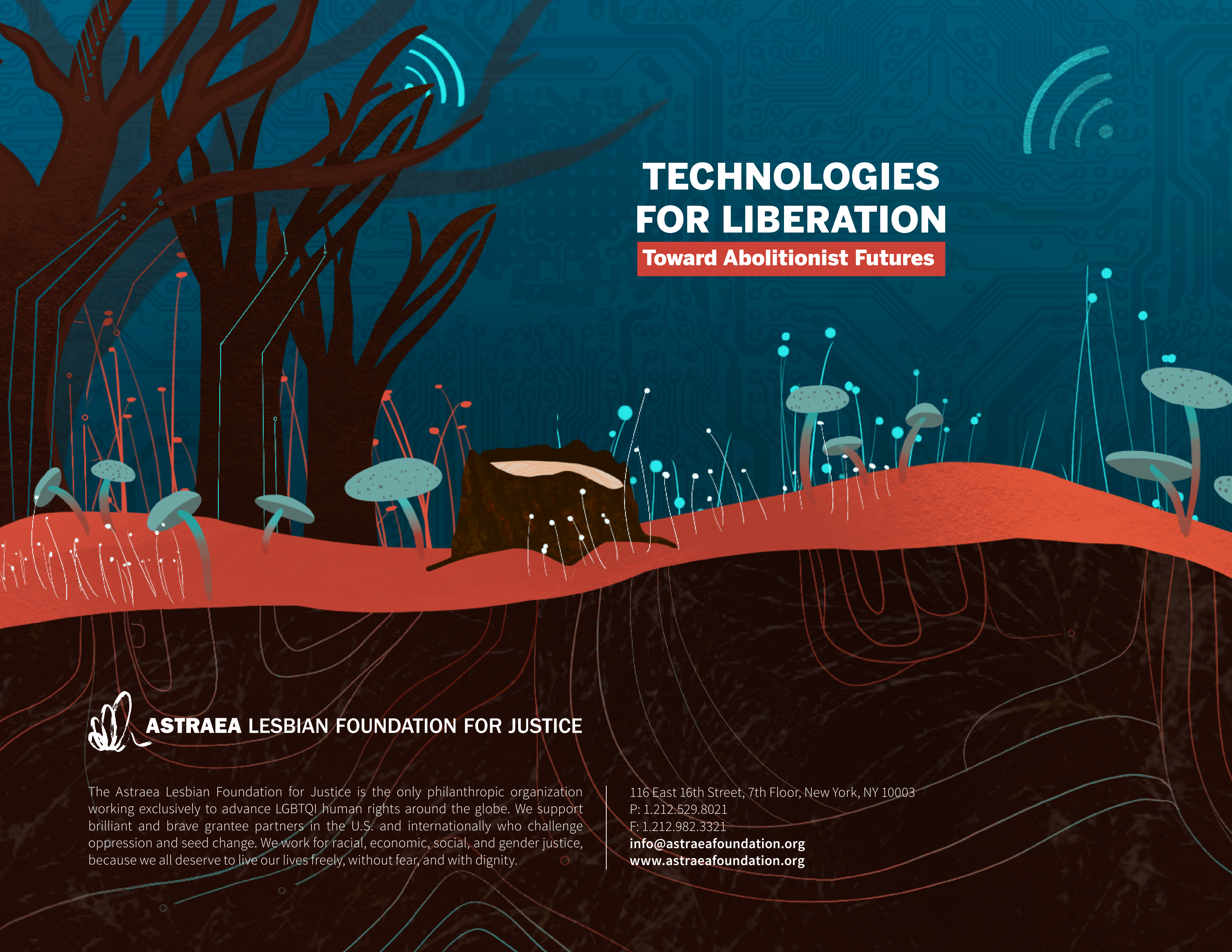
Thank you to the advisory committee for providing their knowledge, expertise, feedback, and invaluable insight throughout the research process, many of whom joined us for an in-person participatory data analysis session held in May 2019 including: Sarah Aoun, Teresa Basilio, Danielle Blunt, Helen Ceballos, Sasha Costanza-Chock, Jacinta Gonzalez, Hamid Khan, Tamika Lewis, Matt Mitchell, Cara Page, Tawana Petty, Heriberto Ramirez, Steven Renderos, Celiany Rivera-Velázquez, Loan Tran, Iman Young.

Thank you to members of Astraea's brilliant staff for their valuable review, feedback and contributions throughout: Bridget de Gersigny, Sarah Gunther, Raviva Hanser, Shaena Johnson, Kim Kaletsky, Courtney Okeke, Sabrina Rich, Celia Turner.

Special thanks for support in the review and editing of this report: Ayana Byrd, Kenrya Rankin, Chriss Sneed, Danielle Blunt.

Design: Feeling.
Illustration: Amir Khadar.

This report was made possible with generous support from the Ford Foundation and the Levi Strauss Foundation. Thank you to Michael Brennan, Brook Kelly-Green, Luna Yasui and Daniel Lee for believing in our vision for this report and helping it come to fruition.



TECHNOLOGIES FOR LIBERATION

Toward Abolitionist Futures

ASTRAEA LESBIAN FOUNDATION FOR JUSTICE

The Astraea Lesbian Foundation for Justice is the only philanthropic organization working exclusively to advance LGBTQI human rights around the globe. We support brilliant and brave grantee partners in the U.S. and internationally who challenge oppression and seed change. We work for racial, economic, social, and gender justice, because we all deserve to live our lives freely, without fear, and with dignity.

116 East 16th Street, 7th Floor, New York, NY 10003
P: 1.212.529.8021
F: 1.212.982.3321
info@astraeafoundation.org
www.astraeafoundation.org