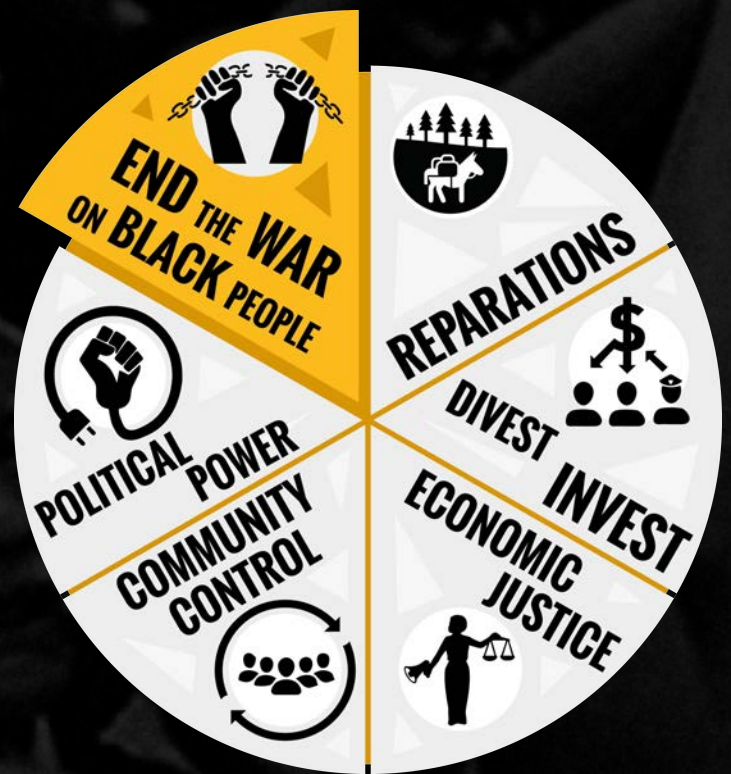


# A VISION FOR BLACK LIVES

POLICY DEMANDS FOR BLACK POWER, FREEDOM, & JUSTICE

AN **END** TO THE **MASS**  
**SURVEILLANCE** OF  
**BLACK** COMMUNITIES, AND  
THE USE OF TECHNOLOGIES  
THAT DISPROPORTIONATELY  
**MONITOR** AND  
**CRIMINALIZE** US

POLICY BRIEF 10 of 13



POLICY PLATFORM 1 OF 6

**M4BL**

THE MOVEMENT  
FOR BLACK LIVES

---

# AN END TO THE MASS SURVEILLANCE OF BLACK COMMUNITIES SUMMARY

---



**ACTION:** INCLUDING THE USE OF TECHNOLOGIES THAT DISPROPORTIONATELY MONITOR AND CRIMINALIZE US (INCLUDING GANG DATABASES, FACIAL RECOGNITION TOOLS, IMSI CATCHERS, DRONES, BODY CAMERAS, PREDICTIVE POLICING SOFTWARE, ELECTRONIC MONITORS, AND RISK ASSESSMENT ALGORITHMS)

## **THE ISSUE:**

While the vast and web of surveillance spreading throughout the U.S. impacts everyone, the harm to targeted groups, including Black, Latinx, Arab, Muslim, South Asian, Middle Eastern, and migrant communities, disabled people, low- and no-income, homeless or precariously housed people, and anyone receiving government benefits or using public services - including health care, housing, and schools - people involved in the sex trades and other criminalized economies, people who may be seeking self-managed abortion and other forms of health care, and activists who challenge state and corporate power is grossly disproportionate. Surveillance is increasingly being proposed as an alternative to incarceration, and corporations are increasingly profiting from our data.

## **THE DEMAND:**

- ❖ An end to the long-standing monitoring and criminalization of Black people.
- ❖ Diversion of public funds used for surveillance to meeting community needs.
- ❖ Elimination of gang databases and related information sharing, and provisions giving individuals placed on gang databases with notice and an opportunity to seek removal.
- ❖ Elimination of surveillance of targeted communities, including people accessing public benefits, hospitals, and services, disabled people, people in the sex trades, people seeking and providing information about self-managed abortion, political activists, Arab, Muslim, Middle Eastern, and South Asian people and communities, and people on probation or parole.

## **KEY FEDERAL LEGISLATION:**

- ❖ *Justice in Forensic Algorithms Act*, which would protect the rights of people accused of crimes.
- ❖ *Electronic Communications Privacy Act (ECPA)*, establishing digital due process.



# WHAT IS THE PROBLEM?

The Edward Snowden leaks in 2013 revealed a vast surveillance apparatus constructed by the FBI and NSA that collects information on everyone in the U.S. and abroad. These leaks confirmed that, in the 21st century, government surveillance has become a pervasive reality. While the web of surveillance impacts everyone, the harm to targeted groups, including Black, Latinx, Arab, Muslim and migrant communities, as well as poor, homeless or indigent individuals, disabled people, and anyone receiving government benefits or using public services, people involved in the sex trades and other criminalized economies, people who may be seeking self-managed abortion and other forms of health care, and activists who challenge state and corporate power is grossly disproportionate.

## WATCHING THE BLACK BODY

Though the violent birth of the U.S. produced racially-biased government monitoring from its very start, it wasn't until 1956 that the counterintelligence program of the Federal Bureau of Investigation (FBI) was created. Through that program, federal and local law enforcement used wiretaps and other methods to unlawfully harass, defame, detain, and even frame Black activists. While the FBI claimed to have ended the program in 1971, the extrajudicial targeting of Black activists by federal and local law enforcement continues to this day.

Despite the reemergence of violent white nationalism as the nation's number one threat to domestic security, federal and local government surveillance continues to target Black communities. Recent FBI leaks revealed that the FBI continues to target Black activists through the fabricated designation of "Black Identity Extremist," now renamed as "Violent Racial Extremism." Documents also showed that the Bureau implemented a program, dubbed "Iron Fist", to focus resources on spying, surveilling, and investigating Black activists, including through undercover agents. We understand this to be part of a larger set of federal countering violent extremism (CVE) programs that have largely focused on the Muslim community, including the almost 40% of American Muslims who are Black.



## DIGITAL POLICING AND PRISONS

Today, technology invades every aspect of Black life, in some cases improving it, but in most cases exacerbating existing inequalities. The ubiquitousness of digital technologies creates multiple points of entry into the criminal punishment system, and facilitates the speed, scale, and secrecy with which governments profile, police, and punish.

Policing has also evolved to use data, devices, and algorithms to create mechanisms for total information awareness for law enforcement at multiple levels of operation. Street cameras, license plate readers, domestic drones, Cell Site Simulators or “Stingray” devices, widespread face recognition, social media monitoring tools, and other technologies are used to unequally target Black people, without the knowledge or consent of local communities or of the people being monitored.

Over the past 10 years, social media monitoring has emerged as a major threat to Black activists and people organizing for racial justice, providing unprecedented power to law enforcement to monitor our movements and the people we represent.

Additionally, artificial intelligence and machine learning have evolved to power “predictive policing,” which uses search tools, scores, heat maps, and other methods that frequently draw on racially biased crime data to predict the occurrence and location of future crimes, replicating racial bias.

The data captured through these approaches—including location information, facial images, and browsing histories and cell phone data—are being centralized at digital fusion and real time crime centers, and held for indeterminate amounts of time.






Additionally, “gang databases” maintained by city, county, state, and federal law enforcement agencies collect extensive information on thousands of people, designating them as “known” or “suspected” gang members. Once designated a “gang member,” individuals are subject to increased profiling, surveillance, and restrictions on activities through civil gang injunctions. They are also often subject to greater use of force during police interactions, and are at risk of being subjected to increased penalties if convicted of an offense under “gang enhancements.”

Membership in any organization, whether formal or informal, including a group that may call itself or be described as a “gang,” is not itself illegal, and thus does not justify the maintenance of intelligence information, surveillance, or enhanced restrictions or punishment. Additionally, evidence cited by officers to justify inclusion in gang databases can be as little as wearing a particular color, or drawing a particular symbol in a school notebook, or being in a familial or other relationship with an actual or suspected gang member. As a result, gang databases can be wildly inaccurate and offer no mechanism to contest the designation.

For instance, in Cook County, IL, almost half of people listed in the gang database are there in part because they have a tattoo an officer believes is associated with gang membership. Over half are there because they frequent or live in an area associated with a particular gang, “affect their style of dress,” or “maintain an ongoing relationship with known criminal gang members.” As a result of profiling and targeted policing of Black communities, people listed in gang databases are disproportionately Black. In Chicago, for example, 75% of people whose information is contained in the city’s gang database are Black.

For immigrants, including Legal Permanent Residents, recipients of Temporary Protective Status (TPS) and Deferred Action for Childhood Arrivals (DACA), as well as undocumented immigrants, being listed as suspected gang members has led to being targeted by immigration enforcement for immigration raids, detention, and deportation.



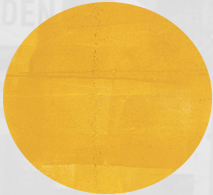


Black immigrants are three times more likely to be deported for a criminal offense; gang affiliation is often cited as a justification. Immigrants who are alleged to be involved with gangs are top immigration enforcement priorities for the Department of Homeland Security (DHS), even if they have no criminal convictions and DHS is targeting them based on allegations alone. Gang involvement is also one of the criteria used to deny appeals for stays of deportation through Deferred Action for Childhood Arrivals, a federal process that allows undocumented immigrants to remain in the United States. As a result, undocumented people designated as “gang members” can be deported even if they have no criminal history, and if they return to the U.S., they would be charged with a felony for unlawful re-entry.

Consequences of inclusion in a gang database also include increased police harassment, especially through traffic and other police stops. This can result in barriers to employment and housing, and can also affect bail decisions and result in sentencing enhancements and harsher conditions of probation and parole.

In addition to gang databases, the increasing use of biometric technologies such as smart doorbells and facial recognition at the top 20 US airports, in schools, and by U.S. Customs and Border Patrol (CBP) and local police departments alike create outsized danger and harm to Black lives. Facial recognition technology identifies people by matching facial features to existing photo and video databases. With the rise of machine learning and artificial intelligence, the threat to civil and human rights posed by facial recognition technology is expanding. Meanwhile, facial recognition tools remain inaccurate—particularly for darker-skinned, female, and young faces, for which the error rate is consistently higher—and continue to create an unreasonable investigative haystack in which to find a needle—obfuscating its original purpose.

The discriminatory collection and use of Black data isn't exclusive to law enforcement.



From applying for public health care and housing, or receiving other government social programs, Black people accessing public services are frequently required to provide their most intimate data, thereby furthering the criminalization of Black people in the 21st century.

Private tech companies contracted by the state and social media platforms are freely facilitating surveillance and data sharing used to target migrants and other criminalized populations.

## SUBSTITUTE PRIVATE SURVEILLANCE

Governments aren't the only ones targeting Black communities for surveillance—wealth is being created for the ruling class from the data and DNA of Black bodies. *Artificial intelligence in the form of algorithms increasingly powers decisions that are fundamental to our economic lives: decisions about who gets credit, a job, healthcare, or housing.* Incorrectly framed as a neutralizing tool, AI can perpetuate discriminatory outcomes through faulty inputs, faulty conclusions, testing failures, and proxy discrimination. These are primary contributors to the mounting cases of algorithmic injustice—instances where people are excluded from benefits and opportunities, or subjected to unfair pricing, where they would otherwise be protected from intentional discrimination. As disproportionate users of social media and mobile devices, Internet users of color are frequently required to turn over information to social media sites and mobile apps as a precondition of use. Sites and apps like Facebook and Twitter often capture a great deal of data about our location, contacts, messages, search histories, and more.

Though Black users represent one of their most engaged audiences, these data mining sites fail to protect Black users from censorship, hate speech and third party or law enforcement monitoring on the platform.



Social media companies, among others, store our personal data for commercial purposes and, increasingly, share this information with law enforcement agencies, biometric companies, and the companies responsible for electronic monitors, and the increasingly pervasive trove of surveillance equipment.



## **VIOLATING CONSTITUTIONAL PROTECTIONS AND HUMAN RIGHTS**

All of these surveillance practices disproportionately impact Black communities, including migrants. They violate the First, Fourth, and Fourteenth Amendment rights of Black, Latinx, Arab, and Muslim people and migrants in the U.S. Without guiding policies, practices, principles, or regulatory parameters that restrain, ban, or place a moratorium on their public and private use, these surveillance technologies supersize the potential for discriminatory policing and criminalization and further erode due process protections under the law. These practices expand the police state and facilitate big profits for a growing surveillance industry—and they use the Internet, potentially the most democratic communications platform the world has ever known, to do it. At the same time, the few technological tools available to protect an individual's information, like encryption, are under constant attack.







# THE DEMAND

## **WE DEMAND:**

- ❖ Transformation in the relationship between technology and the economy to prevent the expansion of surveillance capitalism.
- ❖ Moratoriums on the digital devices used to police race and poverty.
- ❖ Increased accountability of platform companies to Black communities.
- ❖ An end to the long-standing monitoring and criminalization of Black people.
- ❖ Diversion of public funds used for surveillance to meeting community needs.
- ❖ Elimination of gang databases and related information sharing, and opportunities for individuals placed on gang databases to receive notice and an opportunity to seek removal.
- ❖ Elimination of surveillance of targeted communities, including people accessing public benefits, hospitals, and services, disabled people, people in the sex trades, people seeking and providing information about self-managed abortion, political activists, Arab, Muslim, Middle Eastern, and South Asian people and communities, and people on probation or parole. Any policy solution should create the most room for abolition possible.

## **HOW DOES THIS SOLUTION ADDRESS THE SPECIFIC NEEDS OF SOME OF THE MOST MARGINALIZED BLACK PEOPLE?**

Migration, police profiling, stops and arrests, and accessing public benefits, health care, education, housing, and other government services, directly subject people to surveillance by the state, disproportionately impacting working class, low- and no-income, homeless, and disabled people, migrants, and criminalized populations. Additionally, the “war on terror” and rampant global Islamophobia subject Black Muslims to high levels of surveillance.



# FEDERAL ACTION:

## CONGRESSIONAL ACTION

- ❖ Pass legislation implementing a ban and/or moratorium on facial recognition technology. Regulation and oversight are insufficient to contain this dangerous technology.
- ❖ Pass legislation to rein in law enforcement's use of social media to monitor individuals and prohibit monitoring based on First Amendment protected activities. Legislation should also include a prohibition on undercover agents using social media to contact a minor without first contacting a parent.
- ❖ Pass legislation putting an end to dangerous and discriminatory surveillance programs that unjustly target communities on the basis of race, religion, or national origin/status. Specifically, Congress should defund and dismantle FBI and DHS surveillance programs that target people of color, youth, and religious communities like Black Identity Extremist (now called "Violent Racial Extremism"), Countering Violent Extremism, "Iron Fist," and Preventing Violent Extremism programs. Additionally, Congress should launch investigations on all "Countering Violent Extremism" Programs to expose potential civil and human rights violations.
- ❖ Pass legislation ending non-disclosure agreements between federal and local law enforcement agencies, and publicize the surveillance technologies that police have access to, along with their capabilities.
- ❖ Place a moratorium on all federal funding for the local purchase of surveillance technologies until adequate civil and human rights protections exist, and until contested technologies are banned outright.
- ❖ Prohibit trade secrets protections and allow people accused of crimes to access and challenge the evidence used against them, including algorithms developed by private vendors, like the *Justice in Forensic Algorithms Act*.



## FEDERAL ACTION:

- ❖ Update the **Electronic Communications Privacy Act (ECPA)** to demand and win federal law that establishes digital due process.
- ❖ Enact federal and state legislation that establishes rights over an individual's information, with mechanisms that allow an individual to know when their information has been tracked and limit the amount of time their data can be stored.
- ❖ Enact federal and state legislation to affirm the right to strong encryption.
- ❖ Affirm and defend the constitutional right of members of the public to record the activity of on-duty police officers in accordance with federal and state law.
- ❖ Enact legislation preventing companies from sharing or selling data with other government agencies and companies.
- ❖ Repeal **FOSTA/SESTA**, legislation that furthers online surveillance of people who are or are believed to be in the sex trades.

## AGENCY ACTION

- ❖ The Department of Homeland Security must defund and shut down all 78 fusion centers listed on the DHS website, and end the **Nationwide Suspicious Activity Reporting Initiative**, which doesn't meet legal standards for search or seizure under the Fourth Amendment.
- ❖ The Department of Homeland Security must disclose information about the number and substance of National Security Letters that have been served to media and tech companies. Media and tech companies should be encouraged to voluntarily do the same.
- ❖ Eliminate gang databases created, maintained, or consulted by federal agencies.





## STATE ACTION:

- ❖ **Immediately cease all funding for state surveillance programs and divert those resources to invest in the health and well-being of our communities.**
- ❖ **Prohibit information sharing with federal immigration or law enforcement authorities. Expand “sanctuary” policies by ending: (1) contracts that allow unfettered information sharing technologies and biometric collection to and from ICE; (2) contracts with private data brokers that work with ICE; and (3) predictive policing programs such as those developed by Palantir. Cities and states that have contracts with Palantir should immediately cancel those contracts. Stopping local law enforcement agencies from collecting, storing, and accessing data on Palantir systems is one important step toward ensuring the civil and human rights of local residents.**
- ❖ **Pass strong biometrics privacy protection laws that will allow people to decide how and if their intimate biometric scans should be used.**
- ❖ **Affirm the right to record the police in the commission of their duties, in every state, and repeal legislation in states that have explicitly revoked that right.**



## STATE ACTION:

- ❖ **Pass model state-based privacy acts that prevent government entities from searching our phones or online accounts without going to a judge, getting our informed and voluntary consent, or under conditions which create a clear emergency.**
- ❖ **Adopt policies that eliminate the use of electronic monitoring for individuals released on parole.**
- ❖ **Enact state laws eliminating gang databases and prohibiting state and local law enforcement from creating or contributing to other gang databases.**
- ❖ **Enact state laws strictly limiting the criteria under which an individual can be placed on a gang database and create mechanisms to give individuals prompt notice of placement on the database and an opportunity to seek removal.**



# LOCAL ACTION

- ❖ Enact a total prohibition on the acquisition of any new surveillance technology or development of surveillance programs by city councils, county boards, and other municipal bodies.
- ❖ Immediate abolition of any and all current use of surveillance technology and programs.
- ❖ Eliminate the use of risk assessment algorithms to set bail or determine pretrial detention.
- ❖ Abolish the use of predictive policing systems.
- ❖ Full disclosure on the use of existing surveillance technology and programs since their inception, including informing individuals and organizations who have been targeted by them.
- ❖ Full reparations for individuals and organizations whose civil and constitutional rights have been violated through the use of surveillance technology.
- ❖ Ban or place moratoriums on the purchase of any technology or software that will be used for local policing and joint “counter-terrorism” activities—including facial recognition technologies, body worn police cameras, licence plate readers, drones, cell site interceptors, and more.
- ❖ Mandate a fiscal impact assessment on the cost of purchase, maintenance, and storage of any policing technology and software.
- ❖ Enact local ordinances eliminating gang databases and prohibiting local law enforcement from contributing to other gang databases.
- ❖ Enact local ordinances strictly limiting the criteria under which an individual can be placed on a gang database and create mechanisms to give individuals prompt notice of placement on the database and an opportunity to seek removal.
- ❖ Prohibit establishment or enforcement of gang injunctions.



# MODEL LEGISLATION

## FEDERAL LEGISLATION

- ❖ A modernized *Federal Electronic Privacy Act* would protect equal digital due process under the law.
- ❖ *No Biometric Barriers to Housing Act* (HR 4008, 2019), which *bans* the use of facial recognition technology in public housing.
- ❖ *A set of legislative actions exist* to regulate Facial Recognition, but each one should be evaluated for whether or not they actually ban the technology or create a time-limited moratorium, whether they restrict spending on the technology or simply demand improvements to the technology.

## STATE LEGISLATION

- ❖ California Electronic Privacy Act, otherwise known as *CalECPA*
- ❖ Illinois Biometric Information Privacy Act (*740 ILCS/14*, 2008)
- ❖ California's Body Camera Accountability Act (*AB 1215*, 2019), which bans the use of biometric surveillance on police body cams.
- ❖ *SB178*—California Electronic Communications Policy Act
- ❖ *AB 90: Fixes to California's Gang Database*

# MODEL LEGISLATION

## LOCAL LEGISLATION

- ❖ **Surveillance Technology and Community Safety Ordinance**—this example, while effective in protecting Black communities by forcing law enforcement disclosure and mandating government transparency, fails to outright ban surveillance technologies, and would therefore require modification to align with our vision for Black lives to live free of surveillance.
- ❖ **Cook County ordinance eliminating regional gang database**
- ❖ **Chicago gang database ordinance**
- ❖ **Chicagoans to End the Gang Database lawsuit**
- ❖ **Community Safety Act, Providence, Rhode Island**

---

# RESOURCES

---

- ❖ **Watching the Black Body**, Malkia Devich Cyril
- ❖ **Facing Tomorrow's High Tech School Surveillance**
- ❖ **Dozens of Cities Have Secretly Experimented** With Predictive Policing Software
- ❖ **Statement of Civil Rights Concerns on Predictive Policing**
- ❖ **Police Body Worn Cameras Civil Rights Scorecard**
- ❖ **Civil Rights Principles for the Era of Big Data**
- ❖ **Body Camera Fact Sheet**—Body Cameras have not helped enforce accountability
- ❖ **Civil Right Principles on Body Worn Cameras**
- ❖ **The Benefits of Body Cameras are a Myth**
- ❖ **Who's Behind ICE?**
- ❖ Stop LAPD Spying Coalition—**The Architecture of Surveillance**
- ❖ **#NoDigitalPrisons**: Challenging E-Carceration
- ❖ **No More Shackles**: Why We Must End the Use of Electronic Monitors for People on Parole
- ❖ **Electronic Monitoring Guidelines**
- ❖ **The Perpetual Lineup**: Unregulated Police Face Recognition in America
- ❖ **America Under Watch**: Face Surveillance in the United States
- ❖ **Garbage In, Garbage Out**: Face Recognition on Flawed Data
- ❖ **Statement of Civil Rights Concerns About Monitoring of Social Media by Law Enforcement**
- ❖ **The Color of Surveillance**: What an infamous abuse of power teaches us about the modern spy era, by Alvaro Bedoya
- ❖ **Black America's State of Surveillance**, Progressive Magazine



---

# RESOURCES

---

- ❖ ***Surveillance of Black Lives Matter Movement Recalls COINTELPRO,*** [Huffington Post](#)
- ❖ ***Federal Appeals Court Says Lawsuit Over NYPD Surveillance of Muslims Can Proceed,*** [Washington Post](#)
- ❖ Inside the U.S. Border Industrial Complex: ***Spy Tech Meets Immigration Crackdown,*** [The Guardian](#)
- ❖ ***In Landmark Victory for Digital Privacy, Gov. Brown Signs California Electronic Communications Privacy Act into Law, ACLU of Northern California***
- ❖ ***California cops, want to use a Stingray? Get a warrant, governor says,*** [Ars Technica](#)
- ❖ ***Youth Justice Los Angeles, Tracked and Trapped:*** Youth of Color, Gang databases and Gang Injunctions
- ❖ Center for American Progress, Mistaken Identity: ***The Dangers of Sweeping Gang Labels for Black and Latino Youth***
- ❖ Brooklyn College Policing and Social Justice Project: ***Gang Takedowns in the deBlasio Era: The Dangers of 'Precision Policing.'***

---

# ORGANIZATIONS CURRENTLY WORKING ON POLICY

---

**ACLU**

**AI NOW**

**BYP100**

**BRENNAN CENTER**

**COLOR OF CHANGE**

**CENTER ON PRIVACY  
& TECHNOLOGY AT  
GEORGETOWN LAW**

**COUNCIL ON  
AMERICAN-ISLAMIC  
RELATIONS**

**DATA & SOCIETY**

**ELECTRONIC  
FRONTIER  
FOUNDATION**

**EQUALITY LABS**

**LUCY PARSONS LAB**

**LAWYERS  
COMMITTEE ON CIVIL  
RIGHTS**

**LEADERSHIP  
CONFERENCE ON  
CIVIL AND HUMAN  
RIGHTS**

**MEDIA JUSTICE,  
HOME OF THE MEDIA  
JUSTICE NETWORK**

**MIJENTE**

**MEDIA MOBILIZING  
PROJECT**

**MEDIA ALLIANCE**

**NAACP**

**OPEN TECHNOLOGY  
INSTITUTE**

**ORGANIZED  
COMMUNITIES  
AGAINST  
DEPORTATIONS**

**PROVIDENCE YOUTH  
STUDENT MOVEMENT  
(PRYSM)**

**UPTURN**

**STOP LAPD SPYING**

**WITNESS**

**YOUTH JUSTICE  
COALITION**



---

# AUTHORS & CONTRIBUTORS

---

- ❖ **Malkia Cyril, Media Justice**
  - With advice from **Nathan ‘Nash’ Sheard from Electronic Frontier Foundation**, **Alvaro Bedoya of the Center on Privacy and Technology at Georgetown Law**, and **Harlan Yu of Upturn**, among others.
- ❖ **Janae Bonsu, BYP100**
- ❖ **Tawana Petty, Our Data Bodies**
- ❖ **Makani Themba, Higher Ground Strategies**



JUSTICE!

---

# RELATED BRIEFS

---

**END THE WAR ON  
BLACK COMMUNITIES**

**END THE WAR ON  
BLACK YOUTH**

**END TO PRETRIAL  
DETENTION**

**END THE WAR ON  
BLACK HEALTH**

**END  
CRIMINALIZATION OF  
BLACK POLITICAL  
ACTIVITY**

**END JAILS, PRISONS,  
AND DETENTION  
CENTERS**

# A VISION FOR BLACK LIVES

POLICY DEMANDS FOR BLACK POWER, FREEDOM, & JUSTICE



**M4BL.ORG**

**M4BL**

**THE MOVEMENT  
FOR BLACK LIVES**