

SEEING THROUGH SURVEILLANCE

WHY POLICYMAKERS SHOULD
LOOK PAST THE HYPE

ACLU

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION

Northern
California

SEEING THROUGH SURVEILLANCE

WHY POLICYMAKERS SHOULD
LOOK PAST THE HYPE

Surveillance is not safety. Yet, too often, police and other government agencies deploy invasive surveillance — from license plate readers and cell phone trackers to face surveillance and drones — without policymakers asking the right questions to understand the dangers of these systems. Whenever surveillance might be at issue, there should be a robust public conversation about non-surveillance alternatives, careful consideration of the long-term costs of surveillance and its impact on people’s lives, and a clear understanding that surveillance systems often fail to live up to their promise. If these issues aren’t raised, community members pay the price.

The evidence is clear that while surveillance has increased exponentially, public safety has not. On the contrary, surveillance systems often make people less safe, especially for groups that have historically been in the government’s crosshairs. Modern surveillance technology makes it possible for the government to track who we are, where we go, what we do, and who we know. It fuels high-tech profiling and perpetuates systems of biased policing. It facilitates deportations, chills speech, and imperils the rights of activists, religious minorities, and people who need reproductive and gender-affirming care.

Policymakers who care about racial justice, immigrants’ rights, reproductive justice, LGBTQ rights, privacy and free speech, and civil rights must pay attention to how surveillance may affect different members of their community. You have a responsibility to not allow surveillance systems that invite harm and create more problems than they solve.

The community, not the police, must be the leader in any decision about the acquisition or use of surveillance technology. Those who may be most impacted need to know when and why surveillance is being considered, what it is intended to do, and what it will cost them — both in dollars, and in their rights. And they need to be empowered to limit or reject surveillance if the costs outweigh the benefits.

We released the first edition of this guide and its model surveillance oversight legislation in 2014. Since then, many communities in California and across the country have used this guide to enact laws that bring independent oversight to surveillance technology and ban dangerous systems such as facial recognition.

This guide revisits the lessons learned about the real impacts and failures of surveillance and provides a framework for scrutinizing and understanding surveillance proposals. Its checklist walks policymakers and community members through essential questions to ask and answer — including whether the surveillance system should be used at all. Throughout, case studies highlight lessons to remember and missteps to avoid.

We hope this document, along with additional resources available at www.aclunc.org/SeeThroughTheHype, will serve as a helpful guide for making informed decisions and focusing on real public safety in your community.

TABLE OF CONTENTS

Surveillance Technology Overview	1
Key Questions to Ask and Answer for Any Existing or Proposed Surveillance	2
Why It Matters: The Costs and Consequences of Surveillance	3
A. The Proven Harms and Unproven Benefits of Surveillance	4
1. Surveillance Systems Fuel Racial Injustice	4
2. Surveillance Threatens Reproductive Freedom and Justice	6
3. Surveillance Exposes LGBTQ People to Harm.....	7
4. Surveillance Endangers Immigrant Communities.....	8
5. Surveillance Harms Religious Communities	9
6. Surveillance Threatens Free Speech and Suppresses Social Activism	10
7. Surveillance Entrenches Economic Injustice.....	12
B. The Full Costs of Surveillance.....	13
1. Surveillance Is Frequently Ineffective and Leads to Life-Altering Mistakes	13
2. Surveillance Marketing Is Often Misleading.....	15
3. Surveillance Takes Resources Away from Other Health and Safety Programs	16
4. Surveillance Creates Financial Risks Including Litigation and Data Breaches.....	18
C. Surveillance Programs are on Increasingly Shaky Legal Footing.....	19
How to Address Existing and Proposed Surveillance Technology	22
A. Collectively Evaluate Community Needs, Costs, and Alternatives	23
1. Decide Together: Involve the Entire Community from the Start.....	23
B. Critically Assess Any Existing Surveillance Program or Surveillance Proposal	28
1. Ask Whether Surveillance Technology Actually Helps.....	31
2. Consider the Full Costs and Potential Legal Liability of Surveillance	32
C. Adopt Policies and Laws That Target Surveillance	35
Conclusion	36

PUBLISHED BY THE ACLU OF NORTHERN CALIFORNIA / THIRD EDITION / JULY 2024

Authors: Matt Cagle, Nicole Ozer, Brady Hirsch

Contributing Writers: Ellen Gunn, Nicolas Hidalgo, ACLU NorCal legal interns

Design and Layout: Ison Design / Printing: Madison Street Press

This publication was underwritten with support from the ACLU Foundation of Northern California and the ACLU's generous members and donors.

SURVEILLANCE TECHNOLOGY

OVERVIEW

ARTIFICIAL INTELLIGENCE (AI):

Algorithms and software models that are trained on large datasets and are often fine-tuned by humans. AI may be incorporated into other software and systems and deployed in a variety of contexts to attempt to predict outcomes or to automate decision making. AI may also be incorporated into other surveillance systems. When developed or used in ways that do not adequately consider existing inequities, built-in algorithmic bias can perpetuate and potentially exacerbate discrimination.

AUTOMATED LICENSE PLATE READERS (ALPR):

Camera and software-based systems, either stationary or mounted on police cars, that scan license plates that come into view. They record the time and place of every single vehicle that they capture, compiling a log of people's routines and movements. Many ALPR software systems allow customer agencies to share driver information with the click of a button.

BODY CAMERAS: Small cameras worn by police that record audio and video. The cameras can capture anything from public interactions with police to sounds and images at rallies. Some body cameras are always on; others are controlled by the wearer. Introduced as a tool of police accountability, but easily exploited for surveillance of the public.

DATA BROKERS AND DATA MINING:

Companies known as "data brokers" frequently offer sensitive information about people for sale and may be obtained without the knowledge of users from devices, apps, and other sources. These companies may claim the capability to sift through this information to discover statistical patterns, trends, and other information about individuals or groups.

DRONES: Unmanned aerial vehicles that may carry cameras, microphones, or other sensors or devices. Drones range from small "quadcopters" that can maneuver near ground level to high-altitude planes with extremely powerful cameras. Drones are cheaper and often quieter than traditional aircraft, making it possible to deploy them frequently for surreptitious surveillance.

FACIAL RECOGNITION: Software that identifies or tracks a person or group of persons in photos or videos based on various facial characteristics. May also include analytics software purporting to determine a person's emotional state. Facial recognition products may be built upon "matching databases" of mugshots, driver's license photos, or photos scraped from the internet. Facial recognition has been widely criticized for significant threats to civil liberties and civil rights and accuracy issues.

INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ("IMSI") CATCHERS:

Surveillance device that emulates a cell phone tower in order to interact with nearby cell phones and often operates in a dragnet matter, scooping up information about every phone in range. IMSI catchers, commonly known as Stingrays (the brand name of one such device), identify nearby cell phones and can also be configured to intercept and capture the contents of communications including calls, text messages, or internet activity.

LOCATION TRACKING: A range of surveillance techniques used to remotely track a person's location. This includes devices that often contain GPS technology, ranging from modern cell phones to trackers that can be attached to a car. Electronic communications devices, including phones, can also be tracked by identifying cell towers or wireless networks the device uses. These devices often obtain and record location every few seconds and with pinpoint accuracy.

SOCIAL MEDIA MONITORING: The monitoring of people and activity on social networks using either manual or software-assisted techniques. This may take multiple forms, including manual monitoring via undercover accounts or using software products that collect posts, analyze personal relationships and political views, and organize the information so its searchable or readable in dossier form.

VIDEO SURVEILLANCE: Camera systems that allow remote observation or recording of activity in public spaces. Video feeds may be actively monitored or passively recorded. Studies have repeatedly shown cameras are costly and of limited use in deterring criminal activity or solving serious crime.

KEY QUESTIONS

TO ASK AND ANSWER FOR ANY EXISTING OR PROPOSED SURVEILLANCE

IS THE ENTIRE COMMUNITY ENGAGED IN EVALUATING PUBLIC CONCERNS AND NEEDS?

- Have you initiated a process to engage community members in evaluating public concerns and needs, potential interventions, and costs? Have you made sure the diversity of the community is fully represented in these discussions?
- What specific problem does your community want to address?
- Have you conducted an evidence-based inquiry and identified the most effective interventions to address this specific problem?
- What interventions are supported by diverse members of the community?

DO YOU KNOW ALL OF THE COSTS AND RISKS OF SURVEILLANCE?

- What impact can surveillance have on privacy, free speech, and the rights and safety of community members?
- Who is most likely to be harmed by surveillance? How could surveillance undermine commitments to support racial justice, immigrants' rights, LGBTQ rights, reproductive access, and other community goals?
- What are the financial costs of surveillance, including initial costs, long-term training, operation and maintenance, increased incarceration, and potential liability risks?
- Have you completed a full surveillance impact assessment to identify costs and risks?

DO YOU HAVE ALL THE INFORMATION YOU NEED, INCLUDING ALTERNATIVES TO SURVEILLANCE?

- What surveillance systems already exist in your community? Who is operating those systems or proposing new surveillance?
- How have you convened the entire community to discuss and critique existing or proposed surveillance? Have you made sure diverse people in the community are involved in these discussions?
- Has the agency proposing or using surveillance provided all available information about the surveillance system before the public debate begins?
- What evidence is there that surveillance will be effective in addressing community concerns and needs?
- What alternatives to surveillance would be more effective, less expensive, or have less impact on the rights of community members?
- How do you ensure agencies cannot deploy or use surveillance in the absence of community approval?

WHY IT MATTERS

THE COSTS AND CONSEQUENCES OF SURVEILLANCE

Police departments often pitch surveillance technology as a guaranteed way to improve public safety. However, the reality is that all too often, the opposite is true. Surveillance often does not prevent crime or improve public safety; instead, it exposes people and city governments to a whole new set of dangers and risks.

Many discussions about surveillance ignore not only the financial costs of the technology but also how it impacts people's lives, infringes on civil rights, and can actually make people less safe. Time and time again, surveillance systems end up compounding biases in our policing and prison systems, with Black and Brown people most affected.

Surveillance can also jeopardize the safety and freedom of immigrant community members at risk of deportation, LGBTQ people seeking community and care, and poor and unhoused community members criminalized for their economic status. It can also undermine the safety of people exercising First Amendment rights, such as activists who rightly fear retaliation or people seeking to practice their faith.

It is critical to take deliberate steps to scrutinize surveillance proposals using an open, public process designed to identify and assess all the harms and costs of surveillance. This begins with understanding how surveillance impacts real people.

A. THE PROVEN HARMS AND UNPROVEN BENEFITS OF SURVEILLANCE

1. SURVEILLANCE SYSTEMS FUEL RACIAL INJUSTICE

In a nation where police interactions with the public all too frequently turn dangerous, surveillance systems can exacerbate and magnify these problems, increasing the risk of unnecessary government scrutiny, in-person encounters, and violence. Again and again, police have used surveillance systems to create inaccurate and discriminatory watchlists, engage in discriminatory stops and searches, and upend people's lives.

Surveillance technologies amplify the over-policing of Black and Brown communities.

- In Oakland, the police department has disproportionately used automated license plate readers (ALPR) in African American, Latino, and lower-income neighborhoods. Analyzing raw data on how Oakland police had operated ALPR systems, researchers concluded, "If you are driving through or parking your car in a neighborhood with a higher density of white families, you are less likely to be picked up by ALPR cameras." Additionally, the locations where Oakland used ALPR didn't "correlate very well with crime," and the ALPR was "clearly not being used to deter automobile-related crimes."⁴
- In Los Angeles, the police department used "predictive policing" surveillance software to decide where to send officers, as well as which areas and individuals to target. The results were highly discriminatory. Under the direction of the predictive policing program, the LAPD sent helicopters — which they dubbed "ghetto birds" — to fly over some neighborhoods 80 to 90 times per week.⁵ Over a six-month period, six Black and Latino men were shot by police in areas the police had targeted under this program.⁶ All the while, police mocked the system's lack of effectiveness, comparing it to a Ouija board and calling it "a civil liberties nightmare."⁷ In fact, 85% of all people flagged by the LAPD's predictive policing program were Black or Latinx, and similar patterns repeated in departments across the country.⁸



"It is an affront to our movement for equity and justice that the SFPD responded by secretly spying on us. We have the right to organize, speak out, and march without fear of police surveillance."

— Hope Williams, ACLU of Northern California client and plaintiff in *Williams v. San Francisco*, speaking about the SFPD's surveillance of Black Lives Matter protests in summer 2020¹

“Predictive policing software uses data from the criminal legal system, which means that this data is a reflection of who has been historically policed and arrested – it’s not a reflection of crime. So for Black and Brown communities, predictive policing software is nothing new, but rather a continuation of age-old discriminatory policing.”

— Myaisha Hayes, Campaign Strategies Director, MediaJustice²

Predictive Policing’s Racist Feedback Loop



→ In New York, the neighborhoods with the heaviest levels of face surveillance infrastructure are the same areas that have been historically targeted with discriminatory stop-and-frisk policies. A 2022 study found that “the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras.”⁹

“The pervasive use of facial recognition technology is effectively a digital stop-and-frisk.”

— Matthew Mahmoudi, Amnesty International⁹

2. SURVEILLANCE THREATENS REPRODUCTIVE FREEDOM AND JUSTICE

We are living in a time where abortion and gender-affirming care is being criminalized in some states, and there is a real threat that surveillance information collected in communities will be exploited to identify, track, and criminalize people who travel for care and the Californians who are helping those people obtain care.¹⁰

Surveillance systems enable the government to monitor the details of our personal lives to a level previously unimaginable. Deploying surveillance systems in your community may fill databases with information that place people at risk. Even if you try to limit the sharing of information on your end, once this information is collected, there is no foolproof way to immunize it from legal demands brought by out-of-state governments. Local surveillance systems like video cameras and license plate readers are now liabilities for communities that are considered safe havens for abortion rights and that want to ensure people in their community can safely seek the care they need.

Indeed, people protesting in support of reproductive rights may also get caught in the net: After the leak of the draft *Dobbs* decision, a surveillance company provided the U.S. Marshals Service with regular alerts detailing pro-abortion protests, including posts by organizers, participants, and bystanders.¹¹

For policymakers with a commitment to abortion rights, it is essential to take a critical look at surveillance systems and how they might be deployed against people seeking reproductive care. These dangers are not entirely new, but the Supreme Court's decision to eliminate the constitutional right to abortion in *Dobbs* and the wave of new restrictions that followed have raised the stakes.

"Government surveillance technologies place progressive values at risk."

— Lilly Irani, Associate Professor, UC San Diego¹²



SURVEILLANCE AND ABORTION RIGHTS

The dangers that surveillance poses to people seeking reproductive care are real. Surveillance technology has been used to target anti-abortion advertisements at people visiting abortion clinics,¹³ and data brokers have been selling location information of people visiting reproductive health offices.¹⁴ There has also been an exponential increase in recent years of local police demanding to know the identities of those who have searched for a particular word online (also known as keyword demands), and those whose phones have been in a particular location at a particular time (geofence demands).¹⁵ A series of text messages with a friend about getting an abortion were used to sentence a woman in Indiana to thirty years in prison.¹⁶ In another case, an online search for the abortion medication misoprostol was weaponized as evidence to charge a Black mother of three with second-degree murder.¹⁷ Soon after the *Dobbs* decision, a teenager in Nebraska was sentenced for having an abortion after prosecutors obtained a record of her Facebook messages.¹⁸ Policymakers must do everything possible to avoid creating a surveillance infrastructure that endangers people and their reproductive rights.



3. SURVEILLANCE EXPOSES LGBTQ PEOPLE TO HARM

Government surveillance has played a key role in the historical police discrimination and profiling of LGBTQ people, particularly those of color. Surveillance has long been used to out, blackmail, humiliate, and bully LGBTQ people and to undermine LGBTQ movements for equality.

The power of modern surveillance poses whole new dangers to LGBTQ people, especially considering the extreme resurgence of anti-LGBTQ legislation. In 2023 alone, 496 anti-LGBTQ laws were introduced across the country. These attacks included legislation to outlaw gender-affirming healthcare, ban LGBTQ books and representation in classrooms, weaken nondiscrimination laws, and prevent trans children from participating in school activities like sports.¹⁹

Within this environment, surveillance is like a spark in a powder keg. Today's surveillance systems can collect, target, and analyze the information of LGBTQ community members in ways previously unimaginable. These systems, even if employed locally for one reason, can easily be coopted to attack queer youth, trans people, and the wider LGBTQ community. They also contribute to the "ongoing and pervasive problem" of discrimination and harassment by law enforcement based on sexual orientation and gender identity.²⁰

The flaws inherent in many surveillance systems can also directly harm LGBTQ people. Facial recognition is notoriously error prone and often built on unproven science, and yet, some vendors have attempted to use it to classify people by gender. A 2019 academic study found that transgender men were wrongly identified as women up to 38% of the time. Additionally, those who identified as agender, genderqueer or nonbinary — indicating that they identify as neither male or female — were mischaracterized 100% of the time.²¹

These errors can be particularly dangerous, given the frequency of police violence against transgender people. A national study found that transgender people who have to interact with police are nearly four times as likely to experience police violence and seven times more likely to experience physical violence than cisgender people.²² We may see a rise in these dangerous interactions, as officials in states with anti-trans laws use surveillance systems to collect information and investigate trans people and identify people who have received gender-affirming care.²³

HISTORICAL SURVEILLANCE OF LGBTQ COMMUNITIES



There is a long history of the government using surveillance to target people for their sexual orientation, gender identity, and sexual behavior.

Even before computers were widespread, police spied on LGBTQ communities and the establishments where they sought refuge and support. Harassment was frequent and systematic, as police engaged in incessant undercover activity to identify, out, and intimidate LGBTQ people.²⁴ In one notorious example, FBI Director J. Edgar Hoover maintained files with information on the sexuality of prominent actors, columnists, activists, members of Congress, and even presidents.²⁵

In the 21st century, the NSA used its post-9/11 surveillance apparatus to spy on and track the porn-viewing habits of alleged "radicalizers" in order to discredit them.²⁶ In addition, police and intelligence agents have repeatedly been caught using surveillance databases to track romantic partners.²⁷

In recent years, police have used the emerging surveillance infrastructure in communities to spy on LGBTQ people and events. The San Francisco Police Department gained access to a network of street-level video cameras to spy on people marching in the Pride Parade.²⁸ Elsewhere in California, schools have monitored social media and student online activities to out queer young people and limit their access to sexual education resources and information.²⁹

4. SURVEILLANCE ENDANGERS IMMIGRANT COMMUNITIES

Across the United States, federal immigration agencies have eagerly exploited local databases rich with information collected by private data brokers, municipal agencies, and police departments. This information is fed into a deportation machine that tears apart immigrant communities.

In the two decades since its creation in 2003, Immigration and Customs Enforcement (ICE) has devoted its massive resources to build and fund a vast, interconnected surveillance infrastructure. Between 2008 and 2021, ICE spent approximately \$2.8 billion on new surveillance technology, data collection, data analysis, and information-sharing initiatives.³⁰ Shrouded in near-total secrecy and with minimal oversight, ICE regularly taps into the trove of personal information collected and stored by state and local governments.³¹

The true magnitude of ICE's surveillance dragnet infrastructure was revealed in a 2022 academic study that shed light on the agency's capacity to secretly "pull dossiers on nearly anyone, seemingly at any time," without a warrant.³² The investigation found that ICE could search through the driver's license data of 74% of adults in the United States and ran the driver license photographs of one-in-three (32%) adults through its facial recognition system. The report also found that ICE could track the driving patterns of 70% of adults, and could use gas, electricity, phone, and internet records to automatically identify people's new home addresses.³³

In recent years, ICE has further expanded its reach into communities by exploiting local surveillance systems and databases to track, identify, and target immigrant community members for detention and deportation. No local surveillance system is safe from ICE's demands.



LICENSE PLATE SURVEILLANCE TARGETS IMMIGRANTS FOR DEPORTATION

In 2019, an ACLU of Northern California lawsuit revealed that over 80 local law enforcement agencies in a dozen states, including California, had helped feed a database of more than a billion license plate reader records accessible to Immigration and Customs Enforcement. The federal government has used these records to target and locate immigrants across the United States.³⁴

In many communities, the impact of these license plate readers was in direct conflict with commitments by elected leaders to protect the safety of their immigrant community members. For example, in Marin County, California, at the same time its board of supervisors passed a formal resolution to protect undocumented immigrants,³⁵ the county sheriff was sharing a trove of driver locations with ICE and CBP. This failure to understand the danger posed by license plate surveillance threatened the safety of many immigrant community members and resulted in a successful lawsuit by residents under a state privacy law.³⁶



“[A]ll people have the right to live with dignity regardless of their immigration status, and... have the right to move freely without having their personal details shared with the federal government or saved in a database without their knowledge or permission.”

— Tara Evans, ACLU client in *Lagleva v. Doyle* (challenge to Marin County sheriff’s sharing of ALPR information with CBP and ICE)³⁷

5. SURVEILLANCE HARMS RELIGIOUS COMMUNITIES

Government agencies have often weaponized surveillance systems to spy on, target, and intimidate people based on their religion. Once people are caught in a surveillance net, it’s difficult to get out. The government may wrongly tag someone as suspicious, labels that are then used to justify further prying into their private lives, placing them on a watchlist, or even threatening them if they do not cooperate with additional surveillance efforts.³⁸

TARGETING AMERICAN MUSLIMS WITH SURVEILLANCE

In the years after the 9/11 attacks, the New York Police Department created a secretive intelligence wing that infiltrated Muslim neighborhoods with undercover officers. These officers compiled dossiers about Muslim Americans going about their daily lives, monitoring them as they engaged in constitutionally protected activities in cafes, bookstores, and private residences, despite no evidence of illegal activity.³⁹ This unconstitutional surveillance harmed New York City’s Muslim community and led to a multi-year lawsuit and a settlement barring the NYPD from conducting investigations based on race, religion, or ethnicity, among other reforms to prevent discriminatory and warrantless surveillance.

6. SURVEILLANCE THREATENS FREE SPEECH AND SUPPRESSES SOCIAL ACTIVISM

All too often, police turn surveillance systems against movements for justice, targeting those who push for social and political change. From the FBI's notorious surveillance of the civil rights movement to the more recent widespread use of surveillance systems to spy on and scare Black Lives Matter protesters, there is a long and troubled history of surveillance systems being used to track, control, and sabotage Black and Brown activists.

“One of the most alarming parts of [the history of social movements] has been the ways that surveillance has been misused against Black people who are advocating for justice. It's been used to discredit, abuse, and incarcerate.”

— Ayọ Tometi, Black Lives Matter co-founder⁴⁰



PHOTO: IVAN RADIC



THE SURVEILLANCE THREAT TO MOVEMENTS FOR JUSTICE

If you are committed to racial justice, you need to understand how time and again, surveillance is deployed against protesters.

- A year-long public records investigation by the ACLU of Northern California uncovered how the California Highway Patrol (CHP) had used aircraft and high-powered cameras to monitor the summer 2020 protests following the murder of George Floyd. In recordings made across the state, CHP fixated on community members exercising their First Amendment rights — including zooming in closely and lingering over people speaking at vigils, kneeling, participating in die-ins, making signs, and even handing out water and dancing.⁴¹ CHP even recorded a “vigil ... so quiet that the loudest sound was helicopters overhead.”⁴² Activists in another city described how “people got scared off by the police aggression and helicopters” and worried that the agency might use the footage as “social blackmail” at a later date.⁴³
- The San Francisco Police Department and the City of San Francisco were sued by three Black Lives Matter protesters after they activated a private network of surveillance cameras to spy on the peaceful protests winding through the city during summer 2020. By surveilling, the police took cameras purportedly intended to help address retail theft and property crime and turned them against people exercising their First Amendment rights.⁴⁴
- The Department of Homeland Security monitored the social media accounts of Black Lives Matter members and collected details about the locations of members and plans for peaceful protests in Ferguson, Mo., Baltimore, and New York City. Many questioned why DHS was surveilling members of a peaceful domestic social justice movement.⁴⁵
- Police across California secretly acquired and tested multiple social media surveillance products, including software that assigned individuals a “threat level” and encouraged surveillance of labor unions and hashtags like #BlackLivesMatter, #dontshoot, and #wewantjustice.⁴⁶ This led to nationwide negative press attention and new policies from Facebook and Twitter prohibiting surveillance of users.⁴⁷

Surveillance of social activists has lasting negative consequences: People who are afraid they will be monitored and retaliated against for their speech may hesitate to exercise their core constitutional rights. Too often, this fear is grounded in reality, as demonstrated by the federal government’s use of trumped-up charges against activists who participated in the 2020 mass demonstrations for Black Lives.⁴⁸

7. SURVEILLANCE ENTRENCHES

ECONOMIC INJUSTICE

Surveillance systems have an outsized impact on people living on the economic margins. Surveillance is frequently used to inflict excessive economic penalties, often with traumatizing effects that push people further into the cycle of poverty. Surveillance is also used to target the unhoused and enforce laws that make it illegal for people to sleep in vehicles or to sit, sleep, or eat in public places when they have no adequate alternatives.⁴⁹

Imposing invasive surveillance on people struggling economically takes an emotional, psychological, physical, and economic toll that can trigger life-changing consequences long after a person is initially tracked and recorded.⁵⁰ Surveilling and policing people based on economic status also feeds the creation of profiles that may be misused by other agencies to make consequential decisions, from child custody to access to benefits.⁵¹

Policymakers committed to treating everyone in their community with respect and dignity should be very wary of how surveillance can exacerbate economic injustice and the criminalization of poverty.

CASE STUDY Speeding Cameras Accelerate Racial Disparities in Ticketing

When Chicago installed speeding camera networks across the city, proponents claimed it would help increase pedestrian safety and eliminate racially biased police stops. However, in reality, the speed cameras actually accelerated racial disparities in ticketing. People in Black and Latinx neighborhoods were given tickets at twice the rate of households in white ZIP codes, and the tens of millions of dollars in penalties exacerbated economic disparities and proved disastrous for many low-income households.⁵² Red-light cameras produced similar disparities in the cities of Rochester, N.Y. and Miami, leading them to end their programs.⁵³

CRIMINALIZATION OF POVERTY AND SURVEILLANCE

- A number of cities have entered into predatory deals with private ALPR companies, using their “free” surveillance systems to collect outstanding court fines while giving away residents’ information for “nearly unlimited commercial use.” Under these arrangements, residents had to pay their original fine *and* an additional 25% processing fee (which went entirely to the private company) or be arrested.⁵⁴ In one Texas city, this practice resulted in 1,500 people, the vast majority of them Black, being put in jail in a single two-year period — simply because they could not afford to pay traffic fines.⁵⁵
- Residents in public housing have been subjected to invasive face surveillance in Detroit and New York City. Captured by cameras that gave police departments “round-the-clock video footage,” residents and their allies sounded the alarm bell about how they were being targeted solely because of their financial circumstances.⁵⁶

B. THE FULL COSTS OF SURVEILLANCE

Surveillance not only threatens people's rights and safety, but also wastes resources that could be spent on evidence-based alternatives. It is costly to deploy, operate, and maintain. It fuels needless arrests and contributes to the billions spent on incarceration. And when surveillance harms people, it leads to costly lawsuits and settlements. To calculate the full financial cost of surveillance technology, policymakers must look beyond the initial sticker price.

1. SURVEILLANCE IS FREQUENTLY INEFFECTIVE AND LEADS TO LIFE-ALTERING MISTAKES

STATISTICS: VOTERS OPPOSE INVASIVE SURVEILLANCE, SUPPORT RESTRICTIONS

A majority of Bay Area voters oppose invasive surveillance and support restrictions on police surveillance powers.

75% oppose the government's collection and storage of people's biometric information.

69% oppose live access to cameras at their homes and businesses.

66% oppose tracking of their social media posts.

Bay Area voters also strongly support community transparency, oversight, and auditing of police surveillance powers.

87% of Bay Area voters want mandated audits of how police use surveillance technology.

74% percent want the community to provide input before giving police any access to surveillance technology.

64% oppose giving police the authority to decide how and when to use surveillance without the oversight of elected officials.⁵⁷

There is very little evidence that surveillance improves public safety. Again and again, communities have adopted surveillance systems that can end up doing more harm than good.

CASE STUDY Oakland Spends \$2M on "Hardly Used" Police Technology

The cash-strapped city of Oakland learned through experience that surveillance technology can be an ineffective and expensive failure. An audit revealed that the city had squandered almost \$2 million on hardly used technology between 2006 and 2011. The auditor recommended steps to ensure that any technology purchased was intended to fulfill specific objectives and was regularly evaluated for effectiveness.⁵⁸ But Oakland's wasteful pattern continued — in 2023, the City of Oakland approved a proposal to massively expand driver surveillance.⁵⁹

CASE STUDY San Francisco Camera Program Fails to Meaningfully Improve Safety

In 2005, San Francisco installed government-owned video cameras in the city's high-crime, high-traffic areas, hoping it would deter and help solve crime. However, post-installation crime statistics published by mandate under a city ordinance revealed that the cameras "had no impact on violent crime" in neighborhoods with cameras and was not significantly successful as a tool for investigations and prosecutions.⁶⁰ Despite this history, in 2023 San Francisco's mayor proposed a ballot measure that would empower the police to unilaterally expand the program while eliminating oversight by the police commission.⁶¹

In addition to its operating costs, surveillance technology may malfunction in truly tragic ways. Operators cannot be relied upon to catch errors, and, in practice, they have not. Communities considering surveillance must grapple with the real possibility that a surveillance system will wrongly identify or label a person as a suspect, with possible irrevocable consequences.

CASE STUDY Falsely Accused Due to Facial Recognition Errors and Police Misuse

Robert Williams was arrested in front of his family for a theft he had nothing to do with.⁶² The arrest of Williams, a Black man from Michigan, is one of six known cases in which police in the United States have wrongly arrested Black people based on flawed facial recognition results.⁶³ A few months later, Michael Oliver, also a resident of Michigan, was arrested for a separate theft based on a bad facial recognition match, even though he did not resemble the person photographed at the scene of the crime.⁶⁴ In yet another tragic case, police relied on a facial recognition error to arrest Porcha Woodruff, a Black woman who was eight months pregnant, holding her in jail and causing immense pain and trauma in the final stages of her pregnancy.⁶⁵ In New Jersey, Nijeer Parks was wrongly accused of a hit-and-run and forced to spend ten days in jail and pay nearly \$5,000 to defend himself after a facial recognition system misidentified him.⁶⁶ In Georgia, police jailed Randal Reid for nearly a week because a facial recognition system falsely connected him to a theft of luxury purses in Louisiana, even though Reid had never been to Louisiana.⁶⁷ In Maryland, Alonzo Sawyer was jailed for nine days for allegedly assaulting a bus driver even though he was sleeping on his couch at the time of the crime.⁶⁸ In all of these cases, police misuse of facial recognition derailed people's lives, forcing them into jail and sometimes causing them to accrue costly legal bills. While these people were eventually cleared, we don't know how many other people have been wrongly accused by police and are currently imprisoned due to inaccurate facial surveillance.


HELD AT GUNPOINT DUE TO ALPR ERRORS

On the roads, police use of automated license plate readers is pouring fuel on the fire of violent police stops. San Francisco police blindly relied on a license plate reader scan that erroneously flagged a 47-year-old Black woman's red car as a stolen grey truck. She was improperly stopped, forced to exit her vehicle, handcuffed, and held at gunpoint by four officers.⁶⁹ In 2018, police held a privacy activist and his brother at gunpoint on their drive home on Thanksgiving after their rental car was wrongly flagged as stolen.⁷⁰ In 2020, Colorado police pulled their guns on a Black family and their four young children after a license plate reader once again made an error, misidentifying the family's car as stolen.⁷¹

2. SURVEILLANCE MARKETING IS OFTEN MISLEADING

Surveillance technology companies often inundate local agencies with flashy marketing materials, claiming their products are an almost magical solution to the exact issues communities are seeking to address, whether public safety, the administration of benefits, the delivery of health care, or other government services.

These companies don't necessarily have a community's best interests at heart — rather, surveillance vendors seek to make profits, and this can involve selling systems that you do not need or that might not even work. It is important to have a critical eye with surveillance marketing and not rely on company claims when making important policy decisions related to surveillance.



“Surveillance technology has a veneer of objectivity, but many of these systems do not work as advertised. High-tech tools can create a false justification for the broken status quo of policing and can end up exacerbating existing racial disparities. We needed to know whether this system actually does what it claims to do. It does not.”

— Jonathan Manes, attorney with the MacArthur Justice Center, discussing Chicago Police Department's use of ShotSpotter gunshot detection microphones⁷²

CASE STUDY Surveillance Marketing Meets Reality

Surveillance companies often make extraordinary and unsupported claims about their products. In 2015, the ACLU of Northern California discovered a surveillance software vendor claiming their product's algorithm could use online posts and other public information to assign to a person a "threat level" of red, yellow, or green. This claim ignores the lack of evidence showing that software can objectively rate a person's positive or negative attributes.⁷³ Indeed, when a Fresno city councilmember tested the system, they were wrongly flagged as a threat.⁷⁴

Surveillance vendors have also increasingly tried to peddle facial recognition to communities, claiming that it will help address crime. But the high-profile rollout of facial surveillance in New Orleans contradicted these claims: It did not lead to a single arrest in nine months and "failed to identify suspects a majority of time."⁷⁵ According to one city councilmember, use of the system was "pretty obviously racist" with all but one use against Black men and women.⁷⁶ The Eye on Surveillance community group, who opposed the use of facial recognition in New Orleans, noted, "This is a bittersweet moment because although it's rewarding to witness the validation of what we've stated for years about this surveillance technology's inefficacy, we're disappointed that neither our coalition nor the people of New Orleans ... were believed to begin with."⁷⁷

CASE STUDY The Risk of "AI" Snake Oil

The risks of blind reliance on unsupported software vendor claims has become so pressing that in 2022 the United States Federal Trade Commission (FTC) warned Congress to exercise "great caution" in relying on artificial intelligence programs as a policy solution.⁷⁸ The FTC's report outlined several problems related to the use of AI systems, including inherent design flaws and inaccuracy, bias and discrimination leading to potentially illegal outcomes, and invasive commercial surveillance and exploitation of the data collected by such systems. The FTC also created a new Office of Technology that will in part help assess whether products are "oozing with snake oil."⁷⁹

3. SURVEILLANCE TAKES RESOURCES AWAY FROM OTHER HEALTH AND SAFETY PROGRAMS

The full costs of surveillance — including infrastructure, training, staffing, operations, and maintenance — can lead to budget overrun and take money away from other interventions that improve community health and safety.

These costs can be unexpected and unsettling — for example, Philadelphia planned to spend \$651,672 on a video surveillance program featuring 216 cameras. Instead, it spent \$13.9 million on the project and wound up with only 102 functional cameras after a year, a result the city controller described as "exceedingly alarming, and outright excessive."⁸⁰

Any discussion or debate about surveillance should reckon with how those funds might be better served on tangible community needs and proven health and safety programs outside the purview of police.

CASE STUDY Federal COVID Recovery Funds Used For Surveillance Systems

Recently, many local lawmakers squandered an important opportunity to improve public safety and health by deciding to spend billions of federal American Rescue Plan recovery funds on even more policing and surveillance, rather than on proven community-based public safety and social programs.⁸¹

The American Rescue Plan made a whopping \$350 billion available to state and local governments.⁸² The Biden Administration called on communities to dedicate American Rescue Plan funding to “proven strategies that will make our communities safer,” including “expanding evidence-based community violence intervention programs and preventing crime by making our neighborhoods stronger with more educational and economic opportunities.” Yet agencies spent less than 1% of it on actual “community violence prevention” programs.⁸³ For example, the city of Syracuse budgeted \$499,740 in “community violence intervention” to repair surveillance cameras and \$171,200 to expand ShotSpotter.⁸⁴

Further research revealed that more than 70 local governments had allocated ARPA funding for surveillance technology, including automated license plate reader systems, drones, surveillance camera systems, social media surveillance, and setting up or expanding real time surveillance hubs.⁸⁵

Among these, Macon-Bibb County, Ga., spent nearly \$2 million in ARPA funds⁸⁶ and New Haven, Conn., spent \$1.2 million⁸⁷ on heavily criticized ShotSpotter microphone surveillance.⁸⁸

Such actions were directly contrary to the push by many community activists to fund public safety interventions that rely less on police and invest more resources in treating crime’s root causes, such as poverty, mental illness, and substance abuse.⁸⁹

The deployment of surveillance systems without the consent or knowledge of the community also triggers public backlash. Oakland was forced to scrap most of the planning for its Domain Awareness Center and scale the project back considerably after community members protested the misleading mission statement and lack of transparency for the project.⁹⁰ Secretive attempts to purchase surveillance systems by officials in Santa Clara County (a stingray surveillance system) and San Jose (drones) also blew up when the community finally became aware of the plans and raised deep concerns.⁹¹

STATISTICS: THE RISE OF POLICE BUDGETS HAS NOT REDUCED CRIME

Over the past twenty years, the amount of surveillance in our communities has skyrocketed. The number of cameras, sensors, and surveillance software systems operating in our communities is higher than ever. Yet, at the same time, public safety has not correspondingly increased. What has gone up: killings by police, incarceration, prosecution of protesters, prosecution of abortion seekers, and the surveillance of low-income and unhoused people.

Despite calls to end the over-reliance on police, police budgets have actually substantially increased in recent years.⁹² A budget analysis of more than 100 cities and counties found that **83%** of law enforcement agencies were spending more on police in 2022, compared to 2019.⁹³ In **49** of those cities and counties, police budgets increased by more than 10%.⁹⁴ Police budgets have similarly increased throughout California. This is true across some of the largest cities, with Sacramento increasing by \$17 million in 2022,⁹⁵ Los Angeles rising by \$8.7 million, and San Francisco ballooning by **\$50 million** (not including an additional \$26.8 million for police overtime hours in spring 2023).⁹⁶

However, as police departments reach record levels of funding, crime rates have not taken a commensurate dive. A 60-year review of spending on state and local police revealed no correlation nationally between spending and crime rates. Instead, a rise in police funding increases the chances of low-level, nonviolent arrests, over-policing Black and Brown communities, and disinvestment from other approaches to public safety.⁹⁷

4. SURVEILLANCE CREATES FINANCIAL RISKS INCLUDING LITIGATION AND DATA BREACHES

Surveillance programs can create significant financial risks for communities, including litigation and data breaches.

Surveillance exposes cities and counties to costly litigation. For example, Muslim residents in Orange County filed a discrimination lawsuit when a confidential informant revealed that he had been sent into mosques to collect information on the identities and activities of worshippers.⁹⁸ The NYPD paid \$1.6 million in attorney fees to plaintiffs challenging its surveillance of New York's Muslim communities.⁹⁹ In San Francisco and Alameda County, counties have had to pay settlements to motorists who police wrongly pulled over, handcuffed, and held at gunpoint due to license plate reader errors and misuse.¹⁰⁰

Surveillance also creates the risk of expensive data breaches that endanger residents' privacy and economic security. It is important to consider these heavy costs and that cyber-attacks against local police departments, including attacks on surveillance camera systems, are on the rise,¹⁰¹ including the possibility of an unauthorized breach of your community's information.¹⁰²

Following best practices (which itself can entail significant expense) is not enough to prevent every breach. California law requires that a local agency notify residents about a security breach,¹⁰³ yet even the largest law enforcement agency in the country, U.S. Customs and Border Protection, could "not adequately safeguard" its facial recognition data against a damaging breach.¹⁰⁴ The cost of a sensitive surveillance data breach could be very high: On average, a data breach by a government agency costs the entity \$2.07 million. In 2018, cyberattacks cost the U.S. government \$13.7 billion.¹⁰⁵ Similarly, a 2022 report found that companies spent an average of \$4.35 million to resolve a data security breach.¹⁰⁶ Simply put, the more information you collect and retain, the greater the risk and potential cost of a breach.¹⁰⁷

On average, a data breach by a government agency costs the entity

\$2.07 million.

In 2018, cyberattacks cost the U.S. government

\$13.7 billion.

Similarly, a 2022 report found that companies spent an average of

\$4.35 million to resolve a data security breach.



C. SURVEILLANCE PROGRAMS ARE ON INCREASINGLY SHAKY LEGAL FOOTING



As the true costs of surveillance technology have come into focus, the legal underpinnings of surveillance are seeing new scrutiny and action from legislatures and government agencies. Courts and policymakers at the state and federal level, driven by increased public concern about privacy, racial justice, immigrants' rights, gender, sexuality, and reproductive rights, are taking action. As a result, your community needs to consider both the existing laws and the potential for legal change when evaluating a surveillance proposal.

In recent years, courts have increasingly found tech-powered government surveillance legally suspect. The U.S. Supreme Court has held that the government cannot search a person's cell phone, track a phone's location over time, or attach a GPS tracker to a person's vehicle, without first obtaining a warrant.¹⁰⁸ Such cases have begun to look at how modern surveillance techniques raise constitutional concerns when they touch upon the "privacies of life" that the Fourth Amendment seeks to secure from "too permeating police surveillance."¹⁰⁹ Building on these concepts, courts have declared unconstitutional a citywide aerial surveillance program,¹¹⁰ the police's long-term use of a "pole camera" to monitor a home,¹¹¹ and prosecutors' use of "geofence warrants" that capture identifying information of all devices used in a particular area.¹¹² The law continues to evolve, but it's already evident that surveillance programs adopted today may be subject to legal challenge and adverse court rulings tomorrow.

Surveillance programs are also vulnerable to lawsuits under state constitutions. The California Constitution's robust right to privacy is a leading example. Passed by the California voters in November 1972, the Privacy Initiative specifically amended Article I, Section 1 of the California state constitution to include an inalienable right to privacy.¹¹³ It created a state constitutional right sweeping beyond the Fourth Amendment and protecting against privacy incursions by both the government and private parties. The "moving force" behind this new constitutional provision was to protect against the "modern threat" related to the "encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society."¹¹⁴ For decades, governments have been sued for allegedly violating Article I, Section 1. As the right turns 50 years old and surveillance further expands, this trend will likely not abate.

"The right to privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose."

— California Supreme Court in *White v. Davis* (quoting ballot materials)¹¹⁵

Californians also have a robust state constitutional right to free expression. Article I, Section 2 of the California Constitution guarantees that “every person may freely speak, write and publish his or her sentiments on all subjects” and that California laws “may not restrain or abridge liberty of speech.”¹¹⁶ Courts have held that safeguarding free speech is a paramount concern because speech is “a freedom which is the matrix, the indispensable condition, of nearly every other form of freedom.”¹¹⁷

“A person does not surrender all Fourth Amendment protection by venturing into the public sphere.”

— U.S. Supreme Court in *Carpenter v. U.S.*¹¹⁸

CASE STUDY FBI Removes GPS Trackers After Supreme Court Rules That Warrantless Tracking Implicates Fourth Amendment

Throughout the United States, the FBI had installed approximately 3,000 GPS trackers on cars without a warrant when the U.S. Supreme Court ruled in 2012 that their use implicated the Fourth Amendment. As a result, the FBI had to deactivate the warrantless trackers and its agents had to physically retrieve them. Obtaining warrants before using any GPS trackers would have ensured the constitutionality of obtained evidence and saved the FBI considerable time and effort.¹¹⁹

OUR RIGHT TO PRIVACY IN PUBLIC

Just because surveillance may be happening on public streets and sidewalks does not mean that policymakers do not need to consider its harms and how it may conflict with rights of community members.

The U.S. Supreme Court has made clear that surveillance carries privacy and free speech threats even if it is conducted solely in public places. People do not lose their rights to private thoughts and communications just by venturing into the public. For example, it has been the case for more than half a century that police must comply with wiretap laws even if a person uses a payphone on a public street.¹²⁰ More recently, the Supreme Court declared that “[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere.”¹²¹ This is particularly true when surveillance information is aggregated to build a robust data profile that can “reveal much more in combination than any isolated record.”¹²² As Justice Sonia Sotomayor observed, “a precise, comprehensive record of a person’s public movements ... reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” For regular people, an “[a]wareness that the Government may be watching chills associational and expressive freedoms.”¹²³

The California Supreme Court has also held numerous times that being in a public space does not eviscerate privacy rights. In *White v. Davis*, it held that covertly “infiltrating” and monitoring the activities of students and professors at classes and public meetings without any indication of criminal activity violated the California Constitution.¹²⁴ In *People v. Cook*, the California Supreme Court held that warrantless aerial surveillance of a resident’s backyard also was an improper infringement on privacy rights, even though it was visible from public airspace.¹²⁵

Californians’ right to free expression also extends outside of the home, even to privately owned areas like shopping centers.¹²⁶

There have also been recent bipartisan efforts to pass and enforce laws at both the state and federal levels to address surveillance technology. The California Electronic Communications Privacy Act (CalECPA) provides robust privacy protection and imposes strict limits on government surveillance related to electronic information.¹²⁷ California also requires public hearings, detailed usage policies, and governing board and public involvement whenever a local agency seeks to acquire or use automated license plate readers, cell phone surveillance technology, or any military equipment, including drones.¹²⁸ California law also prohibits local agencies from sharing of information collected by automated license plate readers with out-of-state entities.¹²⁹ Residents and community groups have used these laws to stop illegal surveillance practices.¹³⁰

CASE STUDY ACLU Sues Marin County Sheriff For Illegally Sharing Driver Locations Far and Wide

The ACLU of Northern California, ACLU of Southern California, and Electronic Frontier Foundation sued the Sheriff and the County of Marin, alleging that the sheriff's sharing of driver locations with hundreds of out-of-state and federal agencies violated a state law prohibiting such sharing. The sheriff collected these locations with ALPR systems and had shared them with Immigration and Customs Enforcement, an agency that has used this sensitive information to locate, target, and deport community members. After the filing of the suit, the County and sheriff quickly changed their practices to come into compliance with state law. In addition, the County was forced to pay attorneys' fees to the plaintiffs in the case.¹³¹

These state and federal protections are driven by a clear shift in public attitudes towards surveillance. Community members are concerned about surveillance and want lawmakers to rein it in. To that end, a number of local governing bodies have adopted laws requiring transparency and oversight of surveillance systems acquired or used by police and other departments.¹³²

Whether or not your community has adopted laws limiting or prohibiting surveillance, you will need to be able to critically assess surveillance programs that are proposed or that already exist. The next section describes a process for assessing technology as a community, underscoring why surveillance is often not the solution to the problems you and your community seek to solve.

HOW TO ADDRESS

EXISTING AND PROPOSED SURVEILLANCE TECHNOLOGY

As you learn about existing surveillance or see proposals for new programs, spotting issues and asking the right questions will be key to protecting people and building real community safety.

Throughout this process, you should not assume that surveillance is the right solution. If you are starting a community engagement process with a discussion about a specific surveillance proposal, you have already skipped several critical steps.

Before even considering surveillance, you should reach out to underrepresented community members to discuss the problems they face. Ask how evidence-based health and safety programs can address those problems. Consider the many ways that surveillance can be misused or cause harm, undermine public safety, and waste resources better suited for other community programs. For existing surveillance programs, interrogate whether they actually solve problems your community wants to address.

Decisions about surveillance should never be made by surveillance companies and police acting alone behind closed doors. Using this framework, we hope you and your community take control of these important decisions and ensure that diverse community members are central to the process.

A. COLLECTIVELY EVALUATE COMMUNITY NEEDS, COSTS, AND ALTERNATIVES

1. DECIDE TOGETHER: INVOLVE THE ENTIRE COMMUNITY FROM THE START

The first step is to make sure that you are involving the entire community to discuss what is happening in their neighborhoods, what specific problems they want to address, and what evidence based interventions they support. There should be thorough discussion about how resources could be allocated to address community concerns in ways that don't increase surveillance and policing. If surveillance systems already exist, they should be reevaluated and discussed holistically by the entire community. As a policymaker, you should make sure the right questions are being asked and answered about all existing and proposed surveillance.

How are you convening the community to discuss community issues and interventions?

Community members should be in control of decisions that might involve surveillance. As you assess a surveillance proposal, create opportunities for meaningful and timely community input at multiple public hearings. These conversations about surveillance can take place at regularly scheduled, public lawmaker meetings, or you can organize a series of specific public meetings.

The community must be given meaningful advance notice that these public discussions will take place. Making sure the public is engaged early on will help everyone understand community interests and identify considerations or concerns. You should contact a wide array of community groups, including those working with ethnic and religious communities, and make them aware of the proposal. This conversation should not be a one-off event. It is important to maximize public awareness early in the process and engage those who might be most impacted by surveillance.

Local agencies should not acquire or deploy new surveillance systems, or expand their surveillance programs, before this debate takes place.



“Technology can only serve democracy to the degree that it is democratized.”

— Malkia Devich-Cyril,
Senior Fellow and Founding
Director, MediaJustice¹³³

Doing so circumvents the local democratic process and cuts community members out of the process. Community meetings with various speakers representing different perspectives (if law enforcement is the only entity given dedicated speaking time, you are doing it wrong) can help the community understand and express their views about local issues and possible interventions.

“What’s the appropriate amount of time police should be allowed to violate our privacy and safety without accountability and oversight?... It seems insultingly simple that the answer should be no time ever.”

— Nathan Sheard, Managing Director, Advocacy, Electronic Frontier Foundation¹³⁴

“I feel like the problem with government adoption of database technologies is they’re adopted as the silver bullet solution and then it cuts off the conversation from looking at alternatives, many of which probably don’t need to involve data or technology. It limits the scope of what’s possible.”

— Rashida Richardson, Assistant Professor of Law and Political Science, Northeastern University School of Law & College of Social Sciences and Humanities¹³⁵

What specific problem does your community want to address?

Surveillance technology is often thrown at problems that it cannot solve. Once you have engaged the community, spark a discussion about the underlying issues that people want to address. Listen to the community and write down the specific problems and measurable outcomes that the community desires. Vague purposes such as “protecting our city from criminals” make it difficult to identify the right interventions. By contrast, a purpose such as “increase recovery of stolen vehicles by 50%” succinctly identifies an outcome desired by community members and helps frame public discussion. Of course, whether surveillance will address it is another question entirely.

CASE STUDY San Jose's Drone Grounded Due to Backlash

San Jose residents were outraged when they learned their police department had purchased a drone without any public debate. Amid critical media coverage and protests from community groups, civil-rights advocates, and local residents, police apologized and said they would ground the drone until they could conduct adequate public outreach.¹³⁶

Focusing on the problems you seek to solve can also help bring into focus the individuals or communities who are most impacted by both the issues. Throughout, you should seek to solicit and understand the thoughts and concerns of diverse community members. Once you do, you can start considering the potential interventions that would actually achieve shared community goals.

What are the best ways to address community issues? What are potential interventions?

Once you have engaged the community and identified the problems you seek to solve together, ask what the best ways are to address community issues and what non-surveillance interventions could help achieve your goals. There are likely many interventions not involving surveillance that can help your community address public safety and health issues and may be strongly supported by community members.

Are there better alternatives to surveillance?

Having a robust discussion about the scope of potential interventions may not be easy. Surveillance vendors often aggressively market their products to police and try to tout their products as the only solution. Government agencies may be desperate for what seems like an easy fix. But the reality is much more complicated, with surveillance systems frequently causing more harm and creating more costs than they prevent. These real-life impacts, combined with the ineffectiveness of surveillance technology at delivering real public safety outcomes, are compelling reasons to ensure that fact-based conversations actually happen. Thoughtful debate will enable your community to identify and utilize interventions that have the potential to be more effective, less expensive, and less likely to be misused or otherwise negatively impact your community members. You might find it leads to decisions to dismantle and reject surveillance systems altogether.

ALTERNATIVES TO SURVEILLANCE GET SIGNIFICANT PUBLIC SUPPORT

Too often, surveillance is a knee-jerk reaction proposed by the police or touted by politicians, even if there is little evidence that it will address crime, and even if alternatives to surveillance are more strongly supported by community members.

Community members can be suspicious when surveillance and incarceration are used as a catch-all, expressing support for non-surveillance alternatives instead. A 2022 poll of San Francisco voters found that only 34% supported an expanded camera surveillance program. A significant majority strongly supported alternatives to surveillance, including 89% supporting more lighting to deter criminal activity and 90% supporting more drug and mental health services.¹³⁷

“Oakland residents are heavily surveilled. It hasn’t made them any safer ... They shouldn’t have to bargain away their civil liberties, especially since there’s no evidence that OPD’s shiny gadgets have made life safer in a city grappling with violence.”

— Justin Phillips, *San Francisco Chronicle*¹³⁸

Consider alternatives and ask what non-surveillance tools you can use to address the problems you identify with the community. The real-life impacts, combined with the ineffectiveness of surveillance technology at delivering real public safety outcomes, are compelling reasons to utilize other approaches.

In San Diego, **60%** of officer dispatches to the scene of the gunshot microphone failed to uncover anything

In Chicago, the system generated **over 40,000** dead-end police deployments.

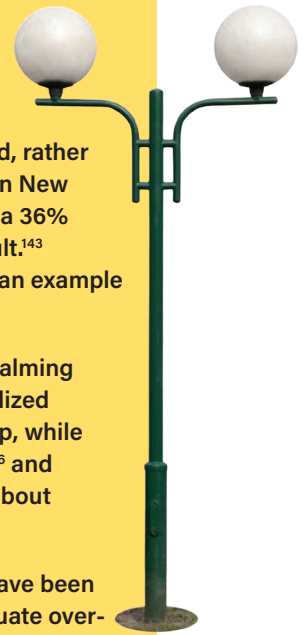
CASE STUDY Microphones “Not the Answer to Reducing Gun Violence”

Many cities have littered neighborhoods with gunshot detection microphones that experts have found to be ineffective, invasive, and inferior to community-supported violence reduction programs.

Studies of the systems in both San Diego and Chicago both found errors and that they often led to “dead-end” police deployments — in San Diego, 60% of officer dispatches to the scene of the gunshot microphone failed to uncover anything, and in Chicago, the system generated over 40,000 dead-end police deployments.¹³⁹ Not only do the dead-end deployments waste resources that could be used more effectively, but gunshot detection microphones also create a “false technological justification” for overpolicing and contribute to wrongful stop-and-frisks.¹⁴⁰ Rather than supporting public safety, they “increase the frequency of police interactions, which also increases the risk of Black Americans becoming the victims of police brutality or harassment.”¹⁴¹ Instead of throwing money at gunshot detection microphones, some experts point to properly designed violence reduction strategies as a much more effective public safety intervention.¹⁴²

ALTERNATIVES TO SURVEILLANCE THAT PRODUCE PUBLIC SAFETY RESULTS

Streetlights, not street cameras — Investing in the physical lighting of a neighborhood, rather than installing more cameras, can reap community-wide benefits. In a controlled study in New York City of streetlights in public housing developments, increased lighting levels led to a 36% reduction in nighttime outdoor crimes, including murder, robbery, and aggravated assault.¹⁴³ Community activists in California have also highlighted Oakland's lighting ordinance as an example that streetlights not only prevent crime but also make neighborhoods feel safer.¹⁴⁴



Speed bumps, not speeding cameras — Speed bumps and other traffic calming techniques have been shown to be effective for traffic safety,¹⁴⁵ can be utilized for a fraction of the cost of cameras (less than \$10,000 for a speed bump, while speeding and red-light cameras can cost \$80,000 per intersection),¹⁴⁶ and do not infringe on privacy by collecting and retaining information about community members.

Gun buybacks, not gunshot detection microphones — Gunshot detection systems have been found to be prone to error, are often ineffective in addressing any crime, and can perpetuate over-policing in communities of color. False alarms can lead to increased police presence in poor and marginalized neighborhoods, where gunshot detection systems are already disproportionately deployed.¹⁴⁷ Gun buyback programs focus on a core problem — the prevalence of guns — and have been extremely effective in taking guns off the street and in mobilizing communities to examine their stances on gun control.¹⁴⁸ For example, during a single-day gun buyback event in Santa Rosa, California, more than 400 firearms, including six assault weapons, were taken off the street.¹⁴⁹

Green chairs, not green lighting surveillance — Project Green Light Detroit is a mass surveillance network involving hundreds of cameras that transmit real-time footage to the police department — and the U.S. Department of Justice concluded it has been ineffective at reducing crime.¹⁵⁰ As an alternative, community members have applauded the Green Chairs, Not Green Lights program. Rather than increasing invasive surveillance, this community program uses funds to distribute chairs for people to “return to their front porches and see each other as neighbors.”¹⁵¹ It has fostered a “commitment to community safety and a willingness to get involved.”¹⁵²



Trees, not tracking devices — A growing body of research also suggests that greenery like grass and trees, not tracking devices and surveillance, may make cities safer. Research in Philadelphia in 2018 found that vacant lots that were “cleaned and greened” — for a cost of just \$5 per square meter — had statistically significant reductions in overall crime and burglaries over a 38-month period, including a 29% percent drop in gun violence in neighborhoods below the poverty line.¹⁵³ The researchers extrapolated that if the intervention was scaled across the entire city, it could translate to more than 350 fewer shootings each year. In Cincinnati, rapid tree loss due to plant disease was also associated with an uptick in property crimes, assaults, and violent crimes. Some say trees might signal that the area is well cared for or make an area inviting and can lead to more “eyes on the street” that can help prevent and reduce crime. Other theories point to the well-documented calming effect of vegetation,¹⁵⁴ or the idea that greenery promotes trust within a community.¹⁵⁵



B. CRITICALLY ASSESS ANY EXISTING SURVEILLANCE PROGRAM OR SURVEILLANCE PROPOSAL

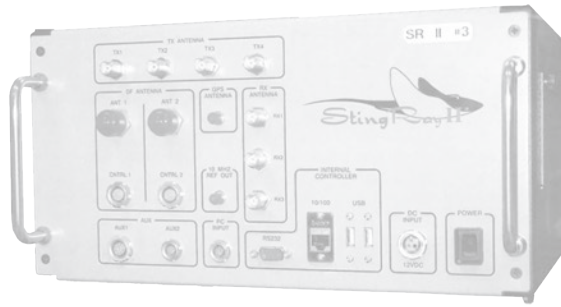
In addition to considering alternatives, your community needs to scrutinize any surveillance proposal and reconsider existing surveillance programs. Throughout the process of examining a proposal or program, continue to turn to your community and create opportunities and space for people to weigh in. Release as much information as possible; your community should understand any surveillance systems in operation and how they work. Together, center the problem the technology is supposed to solve and ask whether non-surveillance alternatives exist. With community partners, ask what impact the system has on civil rights and liberties and the full costs of the surveillance program.

If an agency in your community already possesses and uses surveillance technology, these programs might have started without any community involvement, democratic oversight, or consideration of how they harm civil rights and civil liberties. As a community leader, you have a responsibility to take a close and critical look at existing surveillance programs. Any existing surveillance technology should be reevaluated and publicly discussed. Departments should never expand or blindly continue a surveillance program — instead, take a close look at what surveillance is in use in your community.

As you examine things together, your community may decide to reject a proposal or dismantle or roll back a surveillance system. There are many reasons you may choose to cease an existing program: It may be too costly, ineffective, dangerous, or harmful to civil rights and liberties. There may also be a less costly and much less invasive non-surveillance alternative that you discover during the public debate. Ending a program might involve cancelling a contract, opting not to renew a contract, or simply directing the agency with the technology to cease using it. Whatever the decision, make sure it is done with full public transparency.

Have you been fully transparent about the surveillance proposal or program?

An informed debate can only take place if policymakers and the public are provided with full information about the surveillance being proposed or used. It requires that your community have access to a wide range of information in order to assess the potential impacts of surveillance and any alternatives that may address the same problems. The agency seeking surveillance technology must be required to prepare and release as much information as possible about the actual or potential uses of a surveillance technology to help everyone understand how a technology will work, its potential costs, and the safeguards that will prevent its misuse if the proposal was approved. This information should be released *far* in advance of any public meeting discussing the surveillance.



CASE STUDY Santa Clara County Cancels Stingray Buy Due to Transparency Concerns

In 2015, the Santa Clara County Executive rejected the Sheriff's Office proposal to purchase a Stingray after the board of supervisors questioned the expense and secrecy of the project. The board questioned how they could be asked to spend more than \$500,000 of taxpayer money to approve a purchase that was shrouded in secrecy even from the board itself. The County Executive ultimately vetoed the purchase because the company providing the Stingray refused to "agree to even the most basic criteria we have in terms of being responsive to public records requests ... We had to do what we thought was right."¹⁵⁶

CASE STUDY Oakland's "Domain Awareness Center" Forced To Scale Back After Keeping Community In The Dark

In 2013, the City of Oakland tried to expand its "Domain Awareness Center," which was originally focused on the Port of Oakland, into a citywide surveillance network linking together video cameras from local streets and schools, traffic cameras, and gunshot microphones. Instead of soliciting early public input about the expanded system, Oakland tried to move forward without any meaningful engagement with the community. Residents were outraged and the city council voted against expanding the system.¹⁵⁸

"I think issues or technologies like this and the secrecy just breaks all trust with our communities and for a democracy to work, there needs to be that trust with the government."

— Homayra Yusufi, Deputy Director, Partnership for the Advancement of New Americans¹⁵⁷

RECOMMENDATION:

EVALUATE A PROPOSAL WITH A SURVEILLANCE IMPACT REPORT

A surveillance impact report is an efficient way to conduct and summarize a critical analysis of how surveillance systems will affect the community's information and rights. The goal of a surveillance impact report is to explain, with evidence, how surveillance might function, any possible harms it may cause, and non-surveillance alternatives that would achieve the same or better result without the same impact on civil rights or liberties. With the support of city staff, and input from experts, a department proposing a surveillance system or expansion should release a report well before public hearings that includes at least the following:

- Information describing the technology, how it works, and the kinds of information it collects;
- The proposed purposes(s) for the surveillance technology;
- Evidence demonstrating the effectiveness of the proposed surveillance technology at directly addressing and solving for the stated purpose, including evidence of how it has been used in comparable communities;
- The location(s) it will be deployed and crime statistics for any location(s);
- An assessment identifying with specificity any potential adverse impact on civil liberties and civil rights, and discussing any plans to safeguard the rights of the public from such adverse impacts;
- The fiscal impact of the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding; and,
- What alternative community interventions would address the stated purpose and any information showing fiscal impact.

A worksheet to help your community prepare a Surveillance Impact Report is available at www.aclunc.org/SeeThroughTheHype.

1. ASK WHETHER SURVEILLANCE TECHNOLOGY ACTUALLY HELPS

What evidence exists that surveillance technology actually solves the problem?

There should be actual evidence that surveillance will improve public safety or address another specific problem the community has identified. Many surveillance systems are untested and do not prove to be effective. The primary goal of surveillance vendors is to sell their products and make a profit. Their claims should not be taken at face value and certainly not in isolation. Instead, focus on the facts. Has this surveillance technology solved the problem in any community like yours? The answers may surprise you.

THE FALSE PROMISE OF SURVEILLANCE TECHNOLOGY

Police departments and surveillance companies often boast of using surveillance to address crime, but there is little evidence of surveillance's actual efficacy.

- **Gunshot detection technology** — Multiple reports have shown that gunshot detection systems, such as ShotSpotter, are flawed in methodology and effectiveness.¹⁵⁹ The surveillance technology frequently fails to work, confusing gunshots with other noises, and its errors have put innocent people in jail.¹⁶⁰
- **Automated license plate readers** — Studies have found both a high error rate and low efficacy for “hits” connected to crime or wrongdoing. A study in Vallejo, California, found that 37% of ALPR “hits” from fixed readers, including readers attached to streetlights, were misreads.¹⁶¹ Another study found that fewer than 1% of ALPR scans result in “hits” connected to crime or wrongdoing.¹⁶²
- **Social media surveillance** — Leading technical experts have concluded that surveillance products designed to identify whether an individual “intends to commit” a crime based on social media are often flawed, biased, and likely to generate a large number of false positives.¹⁶³ The ACLU of Northern California even discovered a program used in Fresno, California, that purported to address crime by assigning residents “threat levels,” a practice whose flaws were on full display when the software algorithm flagged a city councilmember’s address as a likely threat.¹⁶⁴
- **Predictive policing** — An intensive investigation of 23,631 predictions made by prominent predictive software Geolitica found the software to be “terrible at predicting crimes,” finding a success rate of as low as 0.1% for some types of crimes.¹⁶⁵ Another investigation of 9 million crime predictions made by Predpol (predecessor to Geolitica) between 2018 and 2021 found outputs heavily skewed toward Black, Latinx, and poor neighborhoods, incessantly directing patrols to the same impoverished areas, while omitting wealthy, white communities.¹⁶⁶
- **Video surveillance** — Research from California and around the world on video surveillance has repeatedly shown that it has limited efficacy on crime.¹⁶⁷ A 2019 systemic review of 40 years of video surveillance showed that it has had “no significant effects” in combatting violent crime.¹⁶⁸ A comprehensive British government study looking at 13 jurisdictions found that cameras did not significantly reduce crime, especially violent crime in city centers, and they also did not reduce fear of crime. Surveys of individuals reported that they did not feel safer and were not more likely to go into city centers after camera placement.¹⁶⁹ In California, a thorough academic study by researchers at UC Berkeley of San Francisco’s Community Safety Camera (CSC) program also found that the surveillance failed to address violent crime.¹⁷⁰ And a year into a pilot program enabling San Francisco police to access private video cameras, it “remain[ed] unclear just how effective the strategy ... is in fighting crime” in the city, with data failing to show a meaningful connection between the cameras and public safety results.¹⁷¹

2. CONSIDER THE FULL COSTS AND POTENTIAL LEGAL LIABILITY OF SURVEILLANCE

In addition to questionable efficacy, there are often financial, legal, and practical concerns that weigh against deploying surveillance to address the problem your community has identified.

What are the impacts on civil rights and liberties?

A surveillance program cannot be effective if it risks harming the rights and lives of community members from varied and diverse backgrounds. During the public debate, make sure the public fully understands how the surveillance technology will be used, including its impacts. This means inviting people other than the police or vendors to explain the technology's impacts. Listen to community members' concerns with the technology. Ask for evidence about how it has been used in other communities. Alternatives to surveillance that are supported by the community should be fully considered and explored.



CASE STUDY Ring Surveillance Cameras Expose the Lives Of Community Members

Police departments have been encouraging and even incentivizing community members to purchase Ring cameras, touting them as a way to keep their community and homes safer.¹⁷² But community members have received several wake-up calls about the real impact of this surveillance technology on privacy and security. First, Ring suffered a data breach in 2019, and 3,600 owner account credentials were shared publicly, resulting in frightening consequences which included hackers spying into children's bedrooms.¹⁷³ Then Ring users realized that while the company promises that people have full control over who views their footage,¹⁷⁴ the reality is much messier. Ring now partners with nearly 2,100 police departments, allowing officers via Ring's "Neighbors" app to request video footage from users and send out alerts. This close relationship, coupled with the power dynamic between police and camera owners, invites coercive requests for footage that people may not feel they can turn down. Police have even circumvented the camera owners and demanded footage directly from Ring.¹⁷⁵ In 2021, the Los Angeles Police Department also requested access to Ring cameras to spy on Black Lives Matter protestors.¹⁷⁶

3,600 Ring owner account credentials were shared publicly through a data breach.

Ring partners with nearly **2,100** police departments allowing officers to request video footage from users and send out alerts.

Several cities considering surveillance proposals have found it useful to actively engage community members through either working groups or specialty committees to shape policy and provide oversight. Cities like Oakland and Vallejo have created standing committees of residents, experts, and advocates who can work together to analyze proposals and make recommendations.¹⁷⁷ The Redlands Police Department convened a Citizens' Privacy Council, open to any city resident, to provide advice on surveillance camera policies and oversee police use of the cameras.¹⁷⁸ Of course, the risk of a surveillance-focused committee risks prioritizing surveillance as a solution. Instead, you should keep the focus on real problems and non-surveillance interventions that actually work.

What are the financial and opportunity costs of this surveillance proposal or program?

Every dollar your community spends on surveillance technology is a dollar it cannot spend on some other community need. First, discuss the financial costs related to surveillance technology, which can include personnel time, training costs, maintenance, and upkeep, as well as any network and storage costs for the information your community may collect. There can also be potential lawsuit costs for violating rights, as well as costs for any data breaches of the information collected by your surveillance system.

CASE STUDY Redlands Deploys Insecure Camera Network

The surveillance camera network in the city of Redlands made the news for the wrong reasons when computer security experts demonstrated how easily they could take control of the cameras. Although the police department expressed concern about “people with criminal intent using the public camera feed to case homes or businesses or track the police force,” the network was deployed with no security at all. Even after the story broke, the network was secured with an outdated encryption protocol that a researcher described as “putting a diary lock on your front door.”¹⁷⁹

Questions about costs cannot be dismissed solely because an agency is seeking grant funding to pay for the technology. Grant money spent on surveillance may have been available to spend on other community interventions. Outside grants may also not cover the costs that follow a surveillance technology's adoption, particularly the long-term costs of operation, repairs, and personnel. Estimating these costs as accurately as possible — and making sure those estimates are shared with the community and made part of the debate about adopting surveillance — is key.

What are the legal risks of the surveillance proposal or program?

Surveillance technology can carry a number of significant legal risks and requirements, in part because of rapid changes to privacy and surveillance law. Under current law, misuse of surveillance systems or personal information or technical glitches outside of your control could subject your community to potential legal liability. And as courts and lawmakers continue to reassess how privacy and free speech rights should apply in the digital age, there is a risk that your community's investment in surveillance technology could leave it saddled with equipment that can no longer be legally used as intended. These factors need to be accounted for when assessing the true costs of any surveillance proposal.

What is the risk of errors, misuse, and mistakes?

Surveillance technology may be inaccurate or malfunction in truly tragic ways. Operators cannot be relied upon to catch errors, and in practice they have not. Communities considering surveillance must grapple with the real possibility that a surveillance system will wrongly identify or label a person a suspect, with possible irrevocable consequences.

C. ADOPT POLICIES AND LAWS THAT TARGET SURVEILLANCE

We hope you share a commitment to limiting the harms of surveillance and ensuring the community has power to influence and control key decisions about surveillance. So far, this document has described ways to analyze and limit harm of existing surveillance programs and proposals for new surveillance. You will encounter a number of different surveillance proposals as a policymaker, and so you should also consider policies and laws that formalize your community's approach to surveillance. Here is a sample of the decisions that California communities have adopted via law or policy:

- **A prohibition on the acquisition** and use of a particular surveillance technology;
- **Rejection of a proposed surveillance policy** after a robust public debate coupled with a resolution to scrutinize surveillance programs more broadly;
- **Amendments to an existing surveillance technology program** contract or use policy, including the imposition of new limitations on the program;
- **Closure or cancellation of a surveillance program** that is at odds with community values;
- **Creation of a surveillance advisory board** made up of local residents and that has the resources and authority to reject surveillance technology programs at odd with community values; and
- **A surveillance technology ordinance** that mandates transparency, accountability and oversight whenever surveillance technology is proposed or used. A number of governing bodies in California — including Santa Clara County, BART, Oakland, San Francisco, Berkeley, Davis, Palo Alto, and San Diego — have adopted versions of such laws.¹⁸⁰

CONCLUSION

Technology is at its best when it enriches our lives and empowers our communities. It should be something that expands our freedoms and capacity to create, connect, and overcome injustice.

But, too often, police and other government agencies turn to surveillance while keeping the community in the dark, secretly deploying invasive and ineffective systems. The result is that community members are increasingly surrounded by surveillance that pries into their private lives and quietly erodes their rights.

With abortion rights and LGBTQ people under increasing attack, and police violence at record highs, policymakers on the side of equal justice should take a critical look at all existing and future surveillance technologies. This begins with a clear-eyed look at the real-life impact of surveillance and requires centering the voices and desires of diverse community members throughout.

We hope that this guide helps you scrutinize surveillance programs and proposals, understand and discuss the real costs of surveillance, and carefully consider non-surveillance interventions that make your community healthier and safer.

If, after robust public debate and a full consideration of non-surveillance alternatives, your community continues to use surveillance systems, you can refer to our *Policy Brief: Important Limits on Surveillance* at www.aclunc.org/SeeThroughTheHype, a document that outlines some of the minimally necessary and enforceable limits that should be in place to prevent harm and abuse. You can also find additional resources on drafting and enacting a prohibition on the acquisition and use of a particular surveillance technology, developing a surveillance advisory board, and passing a surveillance oversight ordinance.

ENDNOTES

- 1 *Activists Sue San Francisco for Wide-Ranging Surveillance of Black-Led Protests Against Police Violence*, ACLU of Northern California, Oct. 7, 2020, available at <https://www.aclunc.org/news/activists-sue-san-francisco-wide-ranging-surveillance-black-led-protests-against-police>.
- 2 Myaisha Hayes, *What Safety Really Looks Like*, Medium.com/#NoDigitalPrisons, Jul. 9, 2018, available at <https://medium.com/nodigitalprisons/what-safety-really-looks-like-ced75304baeb>.
- 3 Amnesty International, *USA: Facial Recognition Technology Reinforcing Racist Stop-And-Frisk Policing in New York — New Research* (Feb. 15, 2022), <https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/>.
- 4 Jeremy Gillula & Dave Maass, *What You Can Learn from Oakland's Raw ALPR Data*, EFF: Deeplinks blog, Jan. 21, 2015, available at <https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>.
- 5 Mara Hvistendahl, *How the LAPD and Palantir Use Data to Justify Racist Policing*, The Intercept, Jan. 30, 2021, available at <https://theintercept.com/2021/01/30/lapd-palantir-data-driven-policing/>.
- 6 Johana Bhuiyan, *LAPD Ended Predictive Policing Programs amid Public Outcry, A New Effort Shares Many of Their Flaws*, The Guardian, Nov. 8, 2021, available at <https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform>.
- 7 Mara Hvistendahl, *How the LAPD and Palantir Use Data to Justify Racist Policing*, The Intercept, Jan. 30, 2021, available at <https://theintercept.com/2021/01/30/lapd-palantir-data-driven-policing/>.
- 8 Matt Wille, *LAPD's New Data-Driven Policing Is Just as Racist as Its Old Ways*, Input, Nov. 10, 2021, available at <https://www.inverse.com/input/culture/lapds-new-data-driven-policing-is-just-as-racist-as-its-old-ways>.
- 9 Amnesty International, *USA: Facial Recognition Technology Reinforcing Racist Stop-And-Frisk Policing in New York — New Research* (Feb. 15, 2022), <https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/>.
- 10 *Alabama's attorney general says the state can prosecute those who help women travel for abortions*, AP News, Aug. 31, 2023, available at <https://apnews.com/article/alabama-abortion-steve-marshall-2157a7d0bfad02aad1ca41e61fe4de33>.
- 11 Sam Biddle, *U.S. Marshals Spied on Abortion Protesters Using Dataminr*, The Intercept, May 15, 2023, available at <https://theintercept.com/2023/05/15/abortion-surveillance-dataminr/>.
- 12 Lilly Irani, *Opinion: Mayor's effort to weaken surveillance oversight threatens privacy and California values*, San Diego Union Tribune, Jan. 14, 2024, available at <https://www.sandiegouniontribune.com/opinion/commentary/story/2024-01-17/opinion-mayors-effort-to-weaken-surveillance-oversight-threatens-privacy-and-california-values>.
- 13 Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' during Clinic Visits*, Rewire News Group, May 25, 2016, available at <https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/>.
- 14 Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, Vice, May 3, 2022, available at <https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood>.
- 15 Hayley Tsukayama, *How California can protect anyone seeking an abortion or gender-affirming care*, S.F. Chronicle, Jun. 4, 2023, available at <https://www.sfchronicle.com/opinion/openforum/article/ab793-abortion-body-autonomy-18166066.php>; Cyrus Farivar, *Abortion Rights, Privacy Activists Push For California Ban On 'Digital Dragnet' Warrants*, a18.asmdc.org, May 2, 2023, available at <https://a18.asmdc.org/news/20230502-abortion-rights-privacy-activists-push-california-ban-digital-dragnet-warrants>.
- 16 Emily Bazelon, *Purvi Patel Could be Just the Beginning*, N.Y. Times, Apr. 1, 2015, available at <https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html>.
- 17 Lauren Rankin, *How an online search for abortion pills landed this woman in jail*, Fast Company, Feb. 26, 2020, available at <https://www.fastcompany.com/90468030/how-an-online-search-for-abortion-pills-landed-this-woman-in-jail>.

- 18 Michael Levenson, *Nebraska Teen Who Used Pills to End Pregnancy Gets 90 Days in Jail*, N.Y. Times, Jul. 20, 2023, available at <https://www.nytimes.com/2023/07/20/us/celeste-burgess-abortion-pill-nebraska.html#:~:text=A%20Nebraska%20teenager%20who%20used,to%20illegally%20concealing%20human%20remains>; Emily Baker-White & Sarah Emerson, *Facebook Gave Nebraska Cops a Teen's DMs. They Used Them to Prosecute Her for Having an Abortion*, Forbes, Aug. 8, 2022, available at <https://www.forbes.com/sites/emilybaker-white/2022/08/08/facebook-abortion-teen-dms/?sh=92edbf579c1>.
- 19 *Mapping Attacks on LGBTQ Rights in U.S. State Legislature*, Aclu.org, <https://www.aclu.org/legislative-attacks-on-lgbtq-rights> (last visited Jan. 9, 2024).
- 20 Amira Hasenbush, Christy Mallory, & Brad Sears, the Williams Institute, *Discrimination and Harassment by Law Enforcement Officers in the LGBT Community* (Mar. 2015), <https://williamsinstitute.law.ucla.edu/publications/lgbt-discrim-law-enforcement/>.
- 21 Lisa Marshall, *Facial recognition software has a gender problem*, CU Boulder Today, Oct. 8, 2019, available at <https://www.colorado.edu/today/2019/10/08/facial-recognition-software-has-gender-problem>.
- 22 National Coalition of Anti-Violence Programs, *Hate Violence Against Transgender Communities* (2017), https://avp.org/wp-content/uploads/2017/04/ncavp_transhvfactsheet.pdf.
- 23 René Kladzyk, *Policing Gender: How Surveillance Tech Aids Enforcement of Anti-Trans Laws*, POGO, Jun. 28, 2023, available at <https://www.pogo.org/investigation/2023/06/policing-gender-how-surveillance-tech-aids-enforcement-of-anti-trans-laws>; Mark Keierleber, *The risks of student surveillance amid abortion bans and LGBTQ restrictions*, The Guardian, Sep. 8, 2022, available at <https://www.theguardian.com/education/2022/sep/08/abortion-bans-school-surveillance-lgbtq-restrictions>.
- 24 J. Todd Ormsbee, *The Meaning of Gay: Interaction, Publicity, and Community Among Homosexual Men in 1960s San Francisco* (Lanham: Lexington Books, 2010); Christopher Agee, "Gayola: Police Professionalization and the Politics of San Francisco's Gay Bars, 1950–1968," *J. Hist. Sexuality* 15, no. 3 (2006): 462, 479. <https://www.jstor.org/stable/4629672>.
- 25 Ian Thompson, *Abusive Surveillance is an LGBTQ Rights Issue*, Slate: Outward, Jul. 10, 2014, available at <https://slate.com/human-interest/2014/07/fbi-monitoring-of-american-muslims-abusive-surveillance-is-a-gay-issue.html>.
- 26 Dan Goodin, *NSA spied on porn, online sexual habits to discredit "radicalizers"*, Ars Technica, Nov. 27, 2013, available at <https://arstechnica.com/tech-policy/2013/11/nsa-spied-on-porn-online-sexual-habits-to-discredit-radicalizers/>.
- 27 Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, Wash. Post: The Switch, Aug. 24, 2013, available at <https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/>.
- 28 Michael Barba, *SF police repeatedly secured access to camera network for live surveillance, emails show*, S.F. Examiner, Aug. 28, 2020, available at https://www.sfexaminer.com/archives/sf-police-repeatedly-secured-access-to-camera-network-for-live-surveillance-emails-show/article_cdd14807-cfcb-5e93-849e-5813et1c081da.html.
- 29 "Reports highlight concerns with increased monitoring of student activity online," *California School News* 27, no. 11 (Nov. 2021). <https://publications.csba.org/california-school-news/november-2021/reports-highlight-concerns-with-increased-monitoring-of-student-activity-online/>.
- 30 Georgetown Center on Privacy & Technology, *American Dragnet: Data-Driven Deportation in the 21st Century* (May 10, 2022), <https://americandragnet.org/>.
- 31 See, e.g., Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Database*, N.Y. Times, Jul. 8, 2019, available at <https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html>.
- 32 Georgetown Center on Privacy & Technology, *American Dragnet: Data-Driven Deportation in the 21st Century* (May 10, 2022), <https://americandragnet.org>.
- 33 Georgetown Center on Privacy & Technology, *American Dragnet: Data-Driven Deportation in the 21st Century* (May 10, 2022), <https://americandragnet.org>.
- 34 Vasudha Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU of Northern California blog, Mar. 13, 2019, available at <https://www.aclunc.org/blog/documents-reveal-ice-using-driver-location-data-local-police-deportations>.
- 35 Marin County Board of Supervisors, *Resolution No. 2020-97* (2020), https://marin.granicus.com/MetaViewer.php?view_id=33&clip_id=10252&meta_id=1079901.
- 36 *Lagleva v. Doyle* (License Plate Surveillance), ACLU of Northern California, Jun. 2, 2022, available at <https://www.aclunc.org/our-work/legal-docket/lagleva-v-doyle-license-plate-surveillance>.

- 37 Tara Evans, *21-10-12 Tara's Statement*, Electronic Frontier Foundation, Oct. 21, 2012, available at <https://www.eff.org/document/21-10-12-taras-statement>.
- 38 See *Tanvir v. Holder*, Case No. 13-CV-6951 (S.D. N.Y. Apr. 22, 2014) (First Amended Complaint), https://ccrjustice.org/sites/default/files/assets/Tanvir%20v%20Comey%2013-cv-6951%20First%20Amended%20Complaint%202014_04_22%20--%20AS%20FILED.pdf.
- 39 Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, Huff. Post, Feb. 25, 2012, available at http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html; Adam Goldman & Matt Apuzzo, *New York Drops Unit That Spied on Muslims*, N.Y. Times, Apr. 15, 2014, available at <http://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html>.
- 40 Jenna McLaughlin, *The FBI vs. Apple Debate Just Got Less White*, The Intercept, Mar. 8, 2016, available at <https://theintercept.com/2016/03/08/the-fbi-vs-apple-debate-just-got-less-white/>.
- 41 *Spies in the California Skies: New Records Expose State Police Aerial Surveillance of Racial Justice Protesters*, ACLU of Northern California blog, Nov. 16, 2021, available at <https://www.aclunc.org/article/spies-california-skies-new-records-expose-state-police-aerial-surveillance-racial-justice>.
- 42 Richard K. De Atley & Ryan Hagen, *Hundreds at Riverside's Fairmount Park hear speeches and march in protest of George Floyd's death*, The Press-Enterprise, Jun. 7, 2020, available at <https://www.pressenterprise.com/2020/06/07/hundreds-at-riversides-fairmount-park-to-hear-speeches-and-march-in-protest-of-george-floyd-death/>.
- 43 Matt Cagle & Jennifer Jones, *Recordings Show the California Highway Patrol's Aerial Surveillance of Racial Justice Protests*, ACLU of Northern California blog, Nov. 16, 2021, available at <https://www.aclunc.org/blog/recordings-show-california-highway-patrol-s-aerial-surveillance-racial-justice-protests>.
- 44 Joshua Sabatini, *Little-known surveillance helps nab thieves*, S.F. Examiner, Dec. 26, 2017, available at https://www.sfexaminer.com/news/little-known-surveillance-helps-nab-thieves/article_daa4aaf1-b2b5-5555-b70f-3c50ad472a3a.html; *Williams v. City and County of San Francisco (Illegal Surveillance)*, ACLU of Northern California, Oct. 7, 2020, available at <https://www.aclunc.org/our-work/legal-docket/williams-v-san-francisco>.
- 45 George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, The Intercept, Jul. 14, 2015, available at <https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/>.
- 46 Nicole Ozer, *Police Use of Social Media Surveillance Software is Escalating, and Activists are in the Digital Crosshairs*, ACLU of Northern California blog, Sep. 20, 2016, available at <https://www.aclunc.org/blog/police-use-social-media-surveillance-software-escalating-and-activists-are-digital-crosshairs>; Matt Cagle, *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU of Northern California blog, Dec. 15, 2015, available at <https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter>.
- 47 Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU of Northern California blog, Oct. 10, 2016 available at <https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target>; *Facebook and Instagram Publicly Prohibit Surveillance of Users Following Coalition Demands*, ACLU of Northern California blog, Mar. 10, 2017, available at <https://www.aclunc.org/news/facebook-and-instagram-publicly-prohibit-surveillance-users-following-coalition-demands>.
- 48 Movement for Black Lives, *Struggle for Power: The Ongoing Persecution of Black Movement by the U.S. Government* (2021), <https://m4bl.org/wp-content/uploads/2021/08/Struggle-For-Power-The-Ongoing-Persecution-of-Black-Movement-by-the-U.S.-Government.pdf>.
- 49 Eric Tars, National Homelessness Law Center, *Criminalization of Homelessness* (2021), https://nlihc.org/sites/default/files/AG-2021/06-08_Criminalization-of-Homelessness.pdf.
- 50 Virginia Eubanks, Seeta Pena Ganghadharan, Tamika Lewis, Mariella Saba, & Tawana Pety, *Our Data Bodies, Reclaiming Our Data* (Jun. 15, 2018), https://www.odbproject.org/wp-content/uploads/2016/12/ODB-InterimReport.FINAL_7.16.2018.pdf.
- 51 Virginia Eubanks, Seeta Pena Ganghadharan, Tamika Lewis, Mariella Saba, & Tawana Pety, *Our Data Bodies, Reclaiming Our Data* (Jun. 15, 2018), https://www.odbproject.org/wp-content/uploads/2016/12/ODB-InterimReport.FINAL_7.16.2018.pdf.

- 52 Emily Hopkins & Melissa Sanchez, Chicago's 'Race-Neutral' Traffic Cameras Ticket Black and Latino Drivers the Most, ProPublica, Jan. 11, 2022, available at <https://www.propublica.org/article/chicagos-race-neutral-traffic-cameras-ticket-black-and-latino-drivers-the-most>.
- 53 *Id.*
- 54 Dave Maass, "No Cost" License Plate Readers Are Turning Texas Police into Mobile Debt Collectors and Data Miners, EFF: Deeplinks blog, Jan. 26, 2016, available at <https://www.eff.org/deeplinks/2016/01/no-cost-license-plate-readers-are-turning-texas-police-mobile-debt-collectors-and>.
- 55 Alex Campbell & Kendall Taggart, *A Traffic Cop's Ticket Bonanza In A Poor Texas Town*, BuzzFeed News, Jan. 26, 2016, available at <https://www.buzzfeednews.com/article/alexcampbell/the-ticket-machine>.
- 56 Lola Fadulu, *Facial Recognition Technology in Public Housing Prompts Backlash*, N.Y. Times, Sep. 24, 2019, available at <https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html>.
- 57 ACLU of Northern California, *Tulchin Research: BAY AREA SURVEILLANCE (BASE)* (Apr. 2022), <https://www.aclunc.org/sites/default/files/ACLU-NC%20Bay%20Area%20Surveillance%20-%20%23225-AA%20-%20Base%20FQ%20-%20Final.pdf>.
- 58 Oakland City Auditor, *Police Technology Performance Audit: FY 2006–07 through 2010–11* (2012), https://www.oaklandauditor.com/wp-content/uploads/2018/06/20120801_Performance_OPDTech.pdf.
- 59 Kiley Russell, *Oakland Privacy Commission Backs Use of New ALPR System*, Piedmont Exedra, 2023, available at <https://piedmontexedra.com/2023/10/oakland-privacy-commission-backs-use-of-new-alpr-system>; Eli Wolfe, *Oakland's license plate readers have been off for months, so why does the city want more?*, The Oaklandside, Aug. 17, 2023, <https://oaklandside.org/2023/08/17/oaklands-license-plate-readers-have-been-off-for-months-so-why-does-the-city-want-more/>.
- 60 See Jennifer King, Deirdre K. Mulligan, & Steven P. Raphael, CITRIS, *CITRIS Report: The San Francisco Camera Safety Program* (Dec. 17, 2008), <https://citris-uc.org/wp-content/uploads/2023/01/citris-report-san-francisco-community-safety-camera-program-2008.pdf>.
- 61 J.D. Morris, *Mayor Breed wants S.F. voters to give police more power. Here are the details*, S.F. Chronicle, Oct. 17, 2023, available at <https://www.sfchronicle.com/sf/article/breed-police-2024-election-18428814.php>.
- 62 Robert Williams, *I Did Nothing Wrong. I was Arrested Anyway*, ACLU, Jul. 15, 2021, available at <https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway>; Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times, Jun. 24, 2020, available at <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>.
- 63 Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED, Mar. 7, 2022, available at <https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/>.
- 64 Elisha Anderson, *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*, Detroit Free Press, Jul. 10, 2020, available at <https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/>.
- 65 *After Third Wrongful Arrest, ACLU Slams Detroit Police Department for Continuing to Use Faulty Facial Recognition Technology*, ACLU, available at <https://www.aclu.org/press-releases/after-third-wrongful-arrest-aclu-slams-detroit-police-department-for-continuing-to-use-faulty-facial-recognition-technology>.
- 66 Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. Times, Dec. 29, 2020, available at <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.
- 67 Associated Press, *JPSO facial recognition tool led to mistaken arrest, lawyer says*, 4WWL, Jan. 2, 2023, available at <https://www.wwltv.com/article/news/crime/jpso-facial-recognition-tool-led-to-mistaken-arrest-lawyer-says/289-558cf26e-8652-41df-b81d-d69a9a1a2e3e>.
- 68 Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, WIRED, Feb. 28, 2023, available at <https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/>.
- 69 Matt Cagle, *San Francisco — Paying the Price for Surveillance Without Safeguards*, ACLU of Northern California blog, May 22, 2014, available at <https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards>. (Denise Green successfully sued San Francisco for violation of her civil rights).
- 70 Charlie Warzel, *When License-Plate Surveillance Goes Horribly Wrong*, N.Y. Times, Apr. 23, 2019, available at <https://www.nytimes.com/2019/04/23/opinion/when-license-plate-surveillance-goes-horribly-wrong.html>.

- 71 Matt Novak, *Cops Terrorize Black Family but Blame License Plate Reader for Misidentifying 'Stolen' Vehicle*, Gizmodo, Aug. 4, 2020, available at <https://gizmodo.com/cops-terrorize-black-family-but-blame-license-plate-rea-1844602731>.
- 72 Press Release, MacArthur Just. Ctr., *ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study*, May 3, 2021, available at <https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study/>.
- 73 Letter from coalition of experts opposed to the Extreme Vetting Initiative to Elaine C. Duke, Acting Secretary of Homeland Security, Department of Homeland Security (Nov. 16, 2017), <https://www.brennancenter.org/sites/default/files/Technology%20Experts%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%202011.15.17.pdf>.
- 74 Matt Cagle, *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU of Northern California blog, Dec. 15, 2015, available at <https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter>.
- 75 Alfred Ng, 'Wholly Ineffective and Pretty Obviously Racist': Inside New Orleans' Struggle with Facial-Recognition Policing, Politico, 2023, available at <https://www.politico.com/news/2023/10/31/new-orleans-police-facial-recognition-00121427>.
- 76 *Id.*; Sneha Singh, *New Orleans Police Face Recognition Efforts Fail to Yield Any Arrests in Nine Months*, Techstory, in, Jul. 30, 2023, available at <https://techstory.in/new-orleans-police-face-recognition-efforts-fail-to-yield-any-arrests-in-nine-months/>.
- 77 *Id.*
- 78 *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems*, FTC, Jun. 16, 2022, available at <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>.
- 79 Stephanie T. Nguyen, *A Century of Technological Evolution at the Federal Trade Commission*, FTC: Tech@FTC blog, Feb. 17, 2023, available at <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission>.
- 80 Alexandra Wigglesworth, *Alan Butkovitz: Cop cameras expose city tech 'missteps'*, Metro Philadelphia, Jun. 21, 2012, available at <https://metrophiladelphia.com/alan-butkovitz-cop-cameras-expose-city-tech-missteps/>.
- 81 Susie Cagle, Weihua Li, & Anastasia Valeeva, *Rifles, Tasers and Jails: How Cities and States Spent Billions of COVID-19 Relief*, The Marshall Project, Sep. 7, 2022, available at <https://www.themarshallproject.org/2022/09/07/how-federal-covid-relief-flows-to-the-criminal-justice-system>.
- 82 Susie Cagle, Weihua Li, & Anastasia Valeeva, *Rifles, Tasers and Jails: How Cities and States Spent Billions of COVID-19 Relief*, The Marshall Project, Sep. 7, 2022, available at <https://www.themarshallproject.org/2022/09/07/how-federal-covid-relief-flows-to-the-criminal-justice-system>.
- 83 The White House, *FACT SHEET: President Biden Issues Call for State and Local Leaders to Dedicate More American Rescue Plan Funding to Make Our Communities Safer — And Deploy These Dollars Quickly*, Statement posted under Briefing Room (May 13, 2022), <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/13/fact-sheet-president-biden-issues-call-for-state-and-local-leaders-to-dedicate-more-american-rescue-plan-funding-to-make-our-communities-safer-and-deploy-these-dollars-quickly/>.
- 84 Susie Cagle, Weihua Li, & Anastasia Valeeva, *Rifles, Tasers and Jails: How Cities and States Spent Billions of COVID-19 Relief*, The Marshall Project, Sep. 7, 2022, available at <https://www.themarshallproject.org/2022/09/07/how-federal-covid-relief-flows-to-the-criminal-justice-system>.
- 85 Electronic Privacy Information Center, *ARPA Surveillance Funding Table* (2023), <https://epic.org/wp-content/uploads/2023/03/EPIC-ARPA-Surveillance-Funding-Table.pdf>.
- 86 Edna Ruiz, *Commission approves gunshot detection system*, Macon-Bibb County, Sep. 17, 2021, available at <https://www.maconbibb.us/91721shotspotter/>.
- 87 Thomas Breen, *ShotSpotter Expansion Advances*, New Haven Independent, Feb. 15, 2022, available at https://www.newhavenindependent.org/article/shotspotter_expansion.
- 88 Garance Burke, Martha Mendoza, Juliet Linderman & Michael Tarm, *How AI-powered tech landed man in jail with scant evidence*, AP News, Mar. 5, 2022, available at <https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220>.

- 89 Jon Schuppe, *Police want a share of pandemic relief funds. Activists find that 'offensive.'*, NBC News, Jun. 5, 2021, available at <https://www.nbcnews.com/news/us-news/police-want-share-pandemic-relief-funds-activists-find-offensive-n1269494>; Ed Lazere, Center on Budget and Policy Priorities, *Using Federal Relief Funds to Invest in Non-Police Approaches to Public Safety* (Nov. 18, 2021), <https://www.cbpp.org/sites/default/files/Fed%20Funds%20for%20Policing%20Alternatives%20Sept%202021.pdf>.
- 90 Will Kane, *Oakland to limit surveillance center to port, airport*, S.F. Gate, Mar. 6, 2014, available at <https://www.sfgate.com/bayarea/article/Oakland-to-limit-surveillance-center-to-port-5290273.php>.
- 91 Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, available at <http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/>; *San Jose Police Apologizes for Secrecy Surrounding Purchase of Drone*, CBS News Bay Area, Aug. 15, 2014, available at <https://www.cbsnews.com/sanfrancisco/news/san-jose-police-apologizes-for-secrecy-surrounding-purchase-of-drone-crime-privacy-surveillance-drones-unmanned-aerial-vehicle/>.
- 92 Grace Manthey, *Law enforcement agency budgets in U.S. cities*, ABC7, available at <https://abcotvdata.github.io/police-budgets/police-budgets-graphs/index.html>.
- 93 Frank Esposito, Amanda Hernandez, & Grace Manthey, *Despite 'defunding' claims, police funding has increased in many U.S. cities*, ABC7, Oct. 19, 2022, available at <https://abc7.com/where-police-departments-defunded-how-does-funding-impact-crime-defund-the-budgets/12324846/#:~:text=The%20truth%20is%20his%20agency's,million%20%2D%20from%202019%20to%202022.>
- 94 *Id.*
- 95 Kristin Lam, *Sacramento City Council approves more police funding in \$1.4 billion budget*, CapRadio, Jun. 15, 2022, available at <https://www.caprado.org/articles/2022/06/15/sacramento-city-council-approves-more-police-funding-in-14-billion-budget/>.
- 96 Thomas K. Pendergast, *Board of Supes Approves \$26.8 Million Boost for SFPD*, Richmond Review/Sunset Beacon, Apr. 3, 2023, available at <https://sfrichmondreview.com/2023/04/03/board-of-supes-approves-26-8-million-boost-for-sfpd/>.
- 97 Philip Bump, *Over the past 60 years, more spending on police hasn't necessarily meant less crime*, Wash. Post, Jun. 7, 2020, available at <https://www.washingtonpost.com/politics/2020/06/07/over-past-60-years-more-spending-police-hasnt-necessarily-meant-less-crime/>.
- 98 See *Fazaga v. FBI*, 844 F.Supp.2d 1022 (C.D. Cal. 2012), <https://casetext.com/case/fazaga-v-fed-bureau-of-investigation-2>.
- 99 *NYC settles lawsuits over Muslim surveillance by police*, AP News, Jan. 17, 2016, available at <https://apnews.com/article/639c450ac2144dd39b849e4282e824d1>.
- 100 Matt Cagle, *San Francisco — Paying the Price for Surveillance Without Safeguards*, ACLU of Northern California blog, May 22, 2014, available at <https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards>; See Tim Cushing, *Another Bogus Hit from a License Plate Reader Results in Another Citizen Surrounded by Cops with Guns Out*, TechDirt, May 23, 2014, available at <https://www.techdirt.com/articles/20140513/07404127218/another-bogus-hit-license-plate-reader-results-another-citizen-surrounded-cops-with-guns-out.shtml>.
- 101 Peter Hermann, *Hack of D.C. police cameras was part of a ransomware scheme, prosecutors say*, Wash. Post, Jul. 28, 2019, available at https://www.washingtonpost.com/local/public-safety/attack-on-dc-police-security-cameras-had-broad-implications/2018/07/24/7ff01d78-8440-11e8-9e80-403a221946a7_story.html.
- 102 Jonathan Greig, *California town announces data breach involving police department, loan provider*, ZDNET, Jan. 10, 2022, available at <https://www.zdnet.com/article/california-town-announces-extensive-data-breach-involving-police-department-loan-provider/>.
- 103 See Cal. Civil Code § 1798.29.
- 104 Geneva Sands, *Border Agency Did "not Adequately Safeguard" Facial Recognition Data, Watchdog Finds*, CNN, 2020, available at <https://www.cnn.com/2020/09/23/politics/customs-border-protection-data-breach-watchdog-report/index.html>.
- 105 Security Intelligence, *The Cost of a Data Breach for Government Agencies* (Sep. 7, 2022), <https://securityintelligence.com/articles/cost-data-breach-government-agencies/>.
- 106 International Business Machines Corporation, *Cost of a data breach 2022* (2022), https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwv8qkBhAnEiwAkY-ahgoUM_r9ioky9UgDNIT7wtgz-H92b-0WzHUYVbNMRy62f-ADUEMUPBoC68EQAvD_BwE&gclsrc=aw.ds.
- 107 Symposium, *The Value of Privacy*, U. Cal.-Hastings School of L. Const. L. Q., Apr. 7, 2014 (oral remarks), available at <http://livestre.am/4P7Lk>.

- 108 *U.S. v. Jones*, 132 S.Ct. 945, 954 (2012) (Sotomayor, J., concurring), <https://casetext.com/case/united-states-v-jones-337>; *id.* at 957 (Alito, Ginsburg, Breyer, and Kagan, J., concurring in the judgment); *Riley v. California*, 134 S. Ct. 2473, 2489 (2014) (Roberts, C. J., Scalia, Kennedy, Thomas, Ginsburg, Breyer, Sotomayor, and Kagan, concurring), <https://supreme.justia.com/cases/federal/us/573/373/>; *id.* at 404 (Alito, J., concurring in part and concurring in the judgement); *Carpenter v. U.S.*, 138 S.Ct. 2206, 2223 (2018), https://www.law.cornell.edu/supremecourt/text/16-402#writing-16-402_OPINION_3.
- 109 *Carpenter v. U.S.*, 138 S.Ct. 2206, 2223 (2018), https://www.law.cornell.edu/supremecourt/text/16-402#writing-16-402_OPINION_3.
- 110 Press Release, *Federal Appeals Court Rules Baltimore Aerial Surveillance Program Is Unconstitutional*, American Civil Liberties Union, Jun. 24, 2021, available at <https://www.aclu.org/press-releases/federal-appeals-court-rules-baltimore-aerial-surveillance-program-unconstitutional>.
- 111 *Pole Cameras Require a Warrant in Massachusetts*, Simons Law Office blog, Sep. 19, 2020, available at <https://www.jbsimonslaw.com/pole-cameras-require-a-warrant-in-massachusetts-state-courts/>.
- 112 Jennifer Lynch, *First Appellate Court Finds Geofence Warrant Unconstitutional*, EFF: Deeplinks blog, Apr. 24, 2023, available at <https://www.eff.org/deeplinks/2023/04/first-us-appellate-court-decide-finds-geofence-warrant-unconstitutional>.
- 113 Ballot Pamphlet, Gen. Elec., *Proposed Amendments to Cal. Const. with Arguments to Voters* (Nov. 7, 1972), <https://www.aclunc.org/sites/default/files/Ballot%20Argument%20ACA%2051.pdf>.
- 114 *White v. Davis*, 13 Cal.3d 757, 774 (1975), <https://law.justia.com/cases/california/supreme-court/3d/13/757.html>.
- 115 *White v. Davis*, 13 Cal.3d 757, 774 (1975), <https://law.justia.com/cases/california/supreme-court/3d/13/757.html>.
- 116 Cal. Const. Art. I, Sec. 2.
- 117 *Palko v. Connecticut*, 7302 U.S. 319, 327 (1937), <https://supreme.justia.com/cases/federal/us/302/319/>.
- 118 585 U.S. 296 (2018)
- 119 Joann Pan, *FBI Turns Off 3000 GPS Devices After Ruling*, Mashable, Feb. 27, 2012, available at <http://mashable.com/2012/02/27/fbi-turns-off-3000-gps-devices/>.
- 120 See *Katz v. United States*, 389 U.S. 347 (1967), <https://supreme.justia.com/cases/federal/us/389/347/>.
- 121 *Carpenter v. United States*, 138 S.Ct. 2206, 2217 (2018), https://www.law.cornell.edu/supremecourt/text/16-402#writing-16-402_OPINION_.
- 122 *Riley v. California*, 134 S. Ct. 2473, 2489 (2014), <https://supreme.justia.com/cases/federal/us/573/373/>.
- 123 *United States v. Jones*, 132 S.Ct. 945, 955, 56 (2012), <https://casetext.com/case/united-states-v-jones-337>.
- 124 *White v. Davis*, 13 Cal.3d 757 (1975), <https://law.justia.com/cases/california/supreme-court/3d/13/757.html>.
- 125 *People v. Cook*, 41 Cal. 3d 373 (1985), <https://law.justia.com/cases/california/supreme-court/3d/41/373.html>.
- 126 *Robins v. Pruneyard Shopping Center*, 592 P.2d 899 (Cal. 1979) (holding that, under the California Constitution, members of the public have a legal right to pass out pamphlets and seek signatures in a privately-owned shopping center), *aff'd*, 447 U.S. 74 (1980), <https://casetext.com/case/robins-v-pruneyard-shopping-center>.
- 127 Cal. Penal Code §§ 1546-1546.4, https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1546.&lawCode=PEN; www.aclunc.org/calecpa.
- 128 Cal Civil Code § 1798.90.55 (ALPR), [https://law.justia.com/codes/california/2022/code-civ/division-3/part-4/title-1-81-23/section-1798-90-55/#:~:text=.55%20\(2022\)-,1798.90.,agency%20before%20implementing%20the%20program](https://law.justia.com/codes/california/2022/code-civ/division-3/part-4/title-1-81-23/section-1798-90-55/#:~:text=.55%20(2022)-,1798.90.,agency%20before%20implementing%20the%20program); Cal Govt Code §53166 (cell phone surveillance), <https://codes.findlaw.com/ca/government-code/gov-sect-53166/>; Cal Govt Code § 7070 et. seq. (military equipment), [https://casetext.com/statute/california-codes/california-government-code.title-1-general.division-7-miscellaneous.chapter-128-funding-acquisition-and-use-of-military-equipment.section-7070-definition#:~:text=\(c\)%20%22Military%20equipment%22,specifically%20excluded%20from%20this%20subdivision](https://casetext.com/statute/california-codes/california-government-code.title-1-general.division-7-miscellaneous.chapter-128-funding-acquisition-and-use-of-military-equipment.section-7070-definition#:~:text=(c)%20%22Military%20equipment%22,specifically%20excluded%20from%20this%20subdivision).
- 129 Cal Civil Code § 1798.90.55, [https://law.justia.com/codes/california/2022/code-civ/division-3/part-4/title-1-81-23/section-1798-90-55/#:~:text=.55%20\(2022\)-,1798.90.,agency%20before%20implementing%20the%20program](https://law.justia.com/codes/california/2022/code-civ/division-3/part-4/title-1-81-23/section-1798-90-55/#:~:text=.55%20(2022)-,1798.90.,agency%20before%20implementing%20the%20program).
- 130 See *Lagleva v. Doyle (License Plate Surveillance)*, ACLU of Northern California, Jun. 2, 2022, available at <https://www.aclunc.org/our-work/legal-docket/lagleva-v-doyle-license-plate-surveillance>; Matthew Guariglia, *Judge Upends Vallejo's Use of a Stingray*, Oct. 2, 2020, <https://www.eff.org/deeplinks/2020/10/judge-upends-vallejos-use-stingray>.

- 131 California Activists Sue Marin County Sheriff for Illegally Sharing Drivers' License Plate Data With ICE, CBP, and Other Out-of-State Agencies, ACLU of Northern California, Oct. 14, 2021, available at <https://www.aclunc.org/news/california-activists-sue-marin-county-sheriff-illegally-sharing-drivers-license-plate-data-ice>.
- 132 See, e.g., Nicole Ozer, *VICTORY! Santa Clara County Abandons Plans to Purchase a Stingray*, ACLU of Northern California, May 6, 2015, available at <https://www.aclunc.org/blog/victory-santa-clara-county-abandons-plans-purchase-stingray>; <https://www.aclunc.org/blog/californians-are-winning-fight-against-secret-surveillance>; Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, available at http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approves-ordinance-regulating-police-use; Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties, *Local Progress*, May 1, 2013, available at <http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/>.
- 133 Keynote address of Malkia Cyril, *Targeted Surveillance, Civil Rights, and the Fight for Democracy*, Center for Media Justice, Oct. 13, 2015, available at <https://mediajustice.org/news/targeted-surveillance-civil-rights-and-the-fight-for-democracy/>.
- 134 Aldo Toledo, *Critics attack Breed's billionaire-backed police ballot measure as dangerous to public*, SF Chronicle, Feb. 22, 2024, available at <https://www.sfchronicle.com/sf/article/breed-police-ballot-measure-18682557.php>.
- 135 Kim M. Reynolds, *Rashida Richardson: Oral Histories of Surveillance*, Our Data Bodies (Aug. 24, 2020), available at <https://www.odbproject.org/2020/08/26/rashida-richardson-oral-histories-of-surveillance/>.
- 136 John Salonga, *San Jose: Police Apologize for Drone Secrecy, Promise Transparency*, San Jose Mercury News, Aug. 5, 2014, available at <https://www.mercurynews.com/2014/08/05/san-jose-police-apologize-for-drone-secrecy-promise-transparency/>.
- 137 Matt Cagle & Jennifer Jones, *With Our Rights Under Attack, We Can't Let SFPD Exploit Private Surveillance Cameras*, ACLU of Northern California blog, Jul. 8, 2022, available at <https://www.aclunc.org/blog/with-our-rights-under-attack-we-cant-let-sfpd-exploit-private-surveillance-cameras>.
- 138 Justin Phillips, *Oakland residents are heavily surveilled. It hasn't made them any safer*, S.F. Chronicle, Oct. 20, 2022, available at <https://www.sfchronicle.com/bayarea/justinphillips/article/Oakland-surveillance-safety-17521104.php>.
- 139 Kara Grant, *ShotSpotter Sensors Send SDPD Officers to False Alarms More Often Than Advertised*, Voice of San Diego, Sep. 22, 2020, available at <http://voiceofsandiego.org/2020/09/22/shotspotter-sensors-send-sdpd-officers-to-false-alarms-more-often-than-advertised/>.
- 140 Press Release, MacArthur Just. Ctr., *ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study*, May 3, 2021, <https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study/>.
- 141 Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach, 55 U. Mich. J. L. Reform 767 (2022), <https://repository.law.umich.edu/mjlr/vol55/iss4/3>.
- 142 Press Release, MacArthur Just. Ctr., *ShotSpotter Generated Over 40,000 Dead-End Police Deployments in Chicago in 21 Months, According to New Study*, May 3, 2021, <https://www.macarthurjustice.org/shotspotter-generated-over-40000-dead-end-police-deployments-in-chicago-in-21-months-according-to-new-study/>; Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach, 55 U. Mich. J. L. Reform 767 (2022), <https://repository.law.umich.edu/mjlr/vol55/iss4/3>.
- 143 Aaron Chalfin, Benjamin Hansen, Jason Lerner & Luci Parker, "Reducing Crime Through Environmental Design: Evidence from a Randomized Experiment of Street Lighting in New York City," *Journal of Quantitative Criminology* 38 (2022): 127-157. <https://link.springer.com/article/10.1007/s10940-020-09490-6>.
- 144 Pacific Institute, *Streetlights and Community Safety* (2009), <https://pacinst.org/wp-content/uploads/2013/02/streetlights3.pdf>.
- 145 Iowa State University, *Temporary Speed Hump Impact Evaluation, Final Report* (Jul. 2022), https://nacto.org/docs/usdg/temporary_speed_humps_impact_evaluation_hallmark.pdf.
- 146 *Implementation costs for automated red light camera systems range from \$67,000 to \$80,000 per intersection*, Intelligent Transportation Systems Joint Program Office, Sep. 30, 2003, available at <https://www.itskrs.its.dot.gov/its/benecost.nsf/ID/2b209ad2c5ad2ab985256db10045892b>; Mark Lazzaretto, City Manager, *City of San Gabriel, Staff Report: City-Wide Speed Hump Policy Consideration* (Aug. 20, 2019), <https://www.sangabrielcity.com/DocumentCenter/View/11543/Item-6A--City-Wide-Speed-Hump-Policy>.

- 147 Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach, 55 U. Mich. J. L. Reform 767 (2022), <https://repository.law.umich.edu/mjlr/vol55/iss4/3>; Helen Webley-Brown, Anna Sipek, Katie Buoymaster, Juilee Shivalkar, Will Owen, & Eleni Manis, Surveillance Technology Oversight Project, *ShotSpotter and the Misfires of Gunshot Technology* (Jul. 14, 2022), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/62cc83c0118f7a1e018bf162/1657570241282/2022.7.7_ShotSpotter+Report_FINAL.pdf.
- 148 J.B. Wogan, *Cities Rethink Gun Buyback Programs*, *Governing*, Feb. 27, 2023, available at <https://www.governing.com/archive/gov-cities-rethink-gun-buyback-programs.html>; Helen Webley-Brown, Anna Sipek, Katie Buoymaster, Juilee Shivalkar, Will Owen, & Eleni Manis, Surveillance Technology Oversight Project, *ShotSpotter and the Misfires of Gunshot Technology* (Jul. 14, 2022), https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/62cc83c0118f7a1e018bf162/1657570241282/2022.7.7_ShotSpotter+Report_FINAL.pdf; Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach, 55 U. Mich. J. L. Reform 767 (2022), <https://repository.law.umich.edu/mjlr/vol55/iss4/3>.
- 149 Katy St. Clair, *Santa Rosa gun buyback program so successful that donations continue after incentives run out*, *Bay City News*, Nov. 2, 2022, available at <https://localnewsmatters.org/2022/11/02/santa-rosa-gun-buyback-is-so-successful-that-donations-continue-after-incentives-run-out/>.
- 150 Steve Neavling, *Detroit's Project Green Light Failed to Reduce Violent Crime*, *DOJ Finds*, *Detroit Metro Times*, Feb. 9, 2023, available at <https://www.metrotimes.com/news/detroits-project-green-light-failed-to-reduce-violent-crime-doj-finds-32332512>.
- 151 Green Chairs, Not Green Lights, <https://greenchairsnotgreenlights.org/> (last visited Mar. 28, 2023).
- 152 Myrtle Thompson-Curtis, *Green Chairs, Not Green Lights: Building Community from Our Front Porches*, *Riverwise Special Summer Edition*, 14 (2019), https://detroitcommunitytech.org/system/tdf/librarypdfs/2019-2206_Riverwise-Surveillance.pdf?file=1&type=node&id=80&force=.
- 153 Jackie Flynn Mogensen, *The Surprising Science of Fighting Crime With... Trees*, *Mother Jones*, 2019, available at <https://www.motherjones.com/environment/2019/04/trees-crime-cincinnati-philadelphia-ida-b-wells-chicago/>.
- 154 Bum-Jin Park, Yuko Tsunetsugu, Hideki Ishii, Suguru Furuashi, Hideki Hirano, Takahide Kagawa & Yoshifumi Miyazaki, "Physiological effects of Shinrin-yoku (taking in the atmosphere of the forest) in a mixed forest in Shinano Town, Japan", *Scandinavian Journal of Forest Research* 23, no. 3 (2008): 278–283. <https://www.tandfonline.com/doi/full/10.1080/02827580802055978>; Jonathan S. Kaplan, *Plants Make You Feel Better*, *Psychology Today*, Mar. 11, 2009, available at <https://www.psychologytoday.com/us/blog/urban-mindfulness/200903/plants-make-you-feel-better>.
- 155 Viniece Jennings & Omoshalewa Bamkole, "The Relationship between Social Cohesion and Urban Green Space: An Avenue for Health Promotion", *Int. J. Environ. Res. Public Health* 16, no. 3 (2019): 452, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6388234/>.
- 156 Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, *N.Y. Times*, Mar. 15, 2015, available at <https://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html>.
- 157 Lexi Spencer-Notabartolo, *Homayra Yusufi: Oral Histories Of Surveillance*, *Our Data Bodies* (Dec. 17, 2020), available at <https://www.odbproject.org/2020/12/17/homayra-yusufi-oral-histories-of-surveillance/>.
- 158 Ali Winston, *Oakland City Council Rolls Back the Domain Awareness Center*, *East Bay Express*, Mar. 5, 2014, available at <http://www.eastbayexpress.com/SevenDays/archives/2014/03/05/oakland-city-council-rolls-back-the-dac>.
- 159 Russell Contreras, *Critics say gunshot-detection technology often doesn't work*, *Axios*, Apr. 9, 2022, available at <https://www.axios.com/2022/04/07/campaign-zero-against-shotspotter-crime>.
- 160 Garance Burke, Martha Mendoza, Juliet Linderman, & Michael Tarm, *How AI-powered tech landed man in jail with scant evidence*, *AP News*, Mar. 5, 2022, available at <https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220>.
- 161 Jason Potts, *Research in Brief: Assessing the Effectiveness of Automatic License Plate Readers*, *Police Chief Magazine*, 14 (Mar. 2018), <https://www.theiacp.org/sites/default/files/2018-08/March%202018%20RIB.pdf>.
- 162 Ángel Díaz & Rachel Levinson-Waldman, Brennan Center for Justice, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use* (Sep. 10, 2020), https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations#footnote8_igdix3y/.

- 163 Letter from coalition of experts opposed to the Extreme Vetting Initiative to Elaine C. Duke, Acting Secretary of Homeland Security, Department of Homeland Security (Nov. 16, 2017), <https://www.brennancenter.org/sites/default/files/Technology%20Experts%20Letter%20to%20DHS%20Opposing%20the%20Extreme%20Vetting%20Initiative%20-%202011.15.17.pdf>.
- 164 Matt Cagle, *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU of Northern California blog, Dec. 15, 2015, available at <https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter>; Justin Jouvenal, *The new way police are surveilling you: Calculating your threat 'score'*, Wash. Post, Jan. 10, 2016, available at https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.
- 165 Aaron Sankin & Surya Mattu, *Predictive Policing Software Terrible At Predicting Crimes*, The Markup, Oct. 2, 2023, available at <https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes>.
- 166 Aaron Sankin, Dhruv Mehrotra, Surya Mattu, Dell Cameron, Annie Gilbertson, Daniel Lempres, & Josh Lash, *Crime Prediction Software Promised to Be Bias-Free. New Data Shows It Perpetuates It*, Gizmodo, Feb. 12, 2021, available at <https://gizmodo.com/crime-prediction-software-promised-to-be-free-of-biases-1848138977>.
- 167 Nicole Ozer, *Studies and Articles on Video Surveillance*, ACLU of Northern California blog, Jul. 31, 2007, available at <https://www.aclunc.org/blog/studies-and-articles-video-surveillance>.
- 168 Eric L. Piza, Brandon C. Welsh, David P. Farrington, & Amanda L. Thomas, "CCTV surveillance for crime prevention. A 40-year systematic with meta-analysis," *Criminology & Public Policy* 18, no. 1 (2019). https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1275&context=jj_pubs.
- 169 Martin Gill & Angela Spriggs, "Assessing the impact of CCTV," *Home Office Research Study* 292 (Feb. 2005). https://www.aclunc.org/sites/default/files/292_Assessing_the_Impact_of_CCTV_2005.pdf.
- 170 Jennifer King, Deirdre K. Mulligan, & Steven P. Raphael, CITRIS, *CITRIS Report: The San Francisco Camera Safety Program* (Dec. 17, 2008), <https://citris-uc.org/wp-content/uploads/2023/01/citris-report-san-francisco-community-safety-camera-program-2008.pdf>.
- 171 Aldo Toledo, *S.F. Police Are Using Cameras to Fight Crime More than Ever before. Is It Working?*, San Francisco Chronicle, Jan. 18, 2024, available at <https://www.sfchronicle.com/sf/article/breed-surveillance-camaras-18603519.php>.
- 172 Caroline Haskins, *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*, Vice: Motherboard blog, Aug. 2, 2019, available at <https://www.vice.com/en/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money>.
- 173 Neil Vigdor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, N.Y. Times, Dec. 15, 2019, available at <https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html>.
- 174 *Neighbors*, Ring.com, <https://ring.com/neighbors> (last visited on Mar. 28, 2023).
- 175 Alfred Ng, *Amazon gave Ring videos to police without owners' permission*, Politico, Jul. 13, 2022, available at <https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513>.
- 176 Matthew Guariglia & Dave Maas, *LAPD Requested Ring Footage of Black Lives Matter Protests*, EFF: Deeplinks blog, Feb. 16, 2021, available at <https://www.eff.org/deeplinks/2022/06/senator-declares-concern-about-amazon-rings-audio-surveillance-capabilities>.
- 177 *Privacy Advisory Commission*, OaklandCA.gov, <https://www.oaklandca.gov/boards-commissions/privacy-advisory-board> (last visited Apr. 13, 2023); Vallejo City Code, Chapter 2.27, https://library.municode.com/ca/vallejo/codes/municipal_code?nodeId=TIT2ADPE_CH2.27SUADBO56_2.27.010CRNA.
- 178 *Citizens Privacy Council*, CityofRedlands.org, <https://www.cityofredlands.org/post/citizens-privacy-council> (last visited Apr. 13, 2023).
- 179 Kashmir Hill, *Whoops, Anyone Could Watch California City's Police Surveillance Cameras*, Forbes, Aug. 21, 2014, available at <https://www.forbes.com/sites/kashmirhill/2014/08/11/surveillance-cameras-for-all/?sh=6878e0854131>.
- 180 *Fighting Local Surveillance: a Toolkit*, ACLU of Northern California, May 14, 2020, available at <https://www.aclunc.org/publications/fighting-local-surveillance-toolkit>.

SEEING THROUGH SURVEILLANCE:
Why Policymakers Should Look Past the Hype

[ACLUNC.ORG/SEETHROUGHTHEHYPE](https://aclunc.org/seethroughthehype)