# SURVEILLANCE AND RESISTANCE

## Police Use of Technology and Activist Mobilization in the San Francisco Bay Area

By Nadia Ghaffari

While a growing body of literature explores police technologies and their general implications, there is a gap in the literature around empirical study of what is actually happening on the ground and how resistance is mobilizing. By centering activists as a lens to investigate police practices, my research captures how police in the San Francisco Bay Area are utilizing surveillance technologies and how activists have mobilized to resist and challenge their use. I examine what the state publicly says that police should be doing with regard to technology usage, what media accounts say they are doing, what organizers reveal them to be doing in practice, and how organizers are responding. Through my empirical analysis, police and state rhetoric of "public safety" clashes with activist narratives of police abuse of power in an increasingly harmful and controlling surveillance state. Surveillance technologies are portrayed as "essential" for stopping crime when in reality, this framing is part of a utopian techno-solutionist orientation that obscures ongoing injustices exacerbated by dragnet surveillance, racial targeting, and public-private partnerships. There is a clear mismatch between state claims and practices. In response, activists are mobilizing through policy and legal channels to hold the police accountable, fight surveillance, and break down police power.

### I. Introduction

Police agencies use an abundance of surveillance technologies and tools to extend their control over cities. These technologies carry long histories of being racialized and classed both in their design and usage, despite being presented as "objective" tools. Thus, activists' resistance is critical to impeding the ever-expanding infiltration of technology into law enforcement and the normalization of disproportionately oppressive surveillance.

Previous literature has found consistently that surveillance and policing technologies – such as facial recognition – have serious consequences for perpetuating racial, gender, and class inequities (Browne 2015, Benjamin 2019). Overall, "neutrality" is a myth. Illustrating this, there have been numerous wrongful arrests made on the basis of flawed facial recognition – disproportionately affecting Black people (Hill 2020). Locally, a few City Councils, including Oakland and San Francisco, voted in 2019 to ban the use of facial recognition technology (FRT) by police, citing bias concerns; media outlets publicly covered this with bold headlines (Ravani

2019). Despite the ban, an article from April 2021 outlines how East Bay police have still been using FRT, and a council member demands an explanation for Alameda police ignoring the ban directive to partner with the private corporation Clearview AI – now facing lawsuits led by activist plaintiffs (Hegarty 2021). This demonstrates the complete lack of transparency and mismatch between state claims and practices. Examining the activism around these issues is important to grasp policy regulations that are being advocated for and demands of change that organizing groups would like to see, not only with facial recognition technology but with the host of surveillance technologies that police agencies operate at-large.

By studying police use of technology in the San Francisco Bay Area through the lens of activists, this project delves into how police surveillance intensifies power inequity, racial injustice, and social control. In line with the introduced tensions between city councils, county police, and civil liberties advocates, my findings illustrate a substantial difference between what the state publicly says that police should be doing and what organizers reveal them to be doing. This disparity informs how organizers are responding to the continued use of surveillance technology and is the main focus of my study.

## II. Literature Review

This work draws upon three fields of study: a) police adoption of new technology, b) critical technology studies, and c) resistance to surveillance. The literature broadly highlights that police are adopting new surveillance technologies, these technologies target marginalized groups and are inherently racist, and thus, there is resistance to them.

### *Policing Technologies*

The police have been adopting and utilizing technology ever since the police force was established in the United States in the early 1800s (Mason 2015). From nightsticks and batons to call and alarm boxes of the mid-1800s and the development of police transportation, these are all distinct examples of policing technologies (Mason 2015). Moving into the 1900s, fingerprinting and crime laboratories arose. The social movement period of the mid-1900s faced another escalation of police technology to more complex weaponry including assault rifles, rubber and plastic bullets, and tear gas as riot police instigated the race riots (Mason 2015). By the 1990s, most police departments were using computers for record-keeping and outlining patterns of crime (Mason 2015). Technological innovation amidst the rise of Big Tech has continued to furnish more tools specifically for surveillance – as is the focus of this study – at the disposal of law enforcement, such as smart cameras and predictive analytics which function as targeted weapons in their own way.

Surveillance technologies are not being used by police in a predetermined vacuum, rather their use is shaped by powerful actors and institutions. For example, surveillance capitalism and public-private partnerships directly influence the development and use of police technologies. Shoshana Zuboff (2019) contends that surveillance capitalism is the push from current global technology companies to give up our privacy and commodify our personal data, which is gathered by third parties, including police agencies, to predict behaviors and make law enforcement decisions. Other scholarship contends that the pervasiveness of police technologies is rooted in military purposes that develop and shape the logic of widespread technology usage.

Advanced technologies that were originally designed for military purposes are now often used in urban, public settings. Nunn details how technologies including photonics, thermal imaging, behavioral and facial recognition systems, remote monitoring by satellite, and biometric systems are fundamentally changing policing and the ways in which urban spaces are viewed by increasing the police's control (2001). Furthermore, Michael Rossler (2019) examines various technologies employed by police including body-worn cameras, aerial and visual surveillance, mapping and crime prediction, and less lethal force technology. He argues that some technologies such as body-worn cameras may strengthen police accountability, while other technologies such as aerial surveillance increase social control without clearly increasing police legitimacy – aligning with Nunn's argument in the latter case. Nunn and Rossler's work both show that police are adopting military-level technologies which increase social control and capacity for surveillance, while not having other clear justifications for these advancements.

In line with the lack of basis, Christopher Koper et al. (2014) analyze how contexts of policing influence the usage and efficacy of policing technology. They contend that technological advancements do not necessarily lead to increased productivity or communication among police. They also find that police often fail to intentionally use technology for diminishing crime and serving in the interest of the public. Thus, the technologies being adopted by police as a result of surveillance capitalism and military-informed logics fall under a techno-solutionist fantasy, where the technology usage is not actually serving a defensible or intentional purpose.

Following the notion of employing policing technologies as illusory "solutions," big data and predictive algorithms have been employed ubiquitously by police agencies – shaping a new wave of digital age policing that also lacks clear justification beyond increasing police control. As one of the few people looking at what police are actually doing in practice, Brayne utilizes interviews and ethnographic observations from two years of fieldwork at the Los Angeles Police Department (LAPD) to study the consequences of big data and algorithmic control. She argues that big data and predictive analytics exacerbate existing inequalities while threatening civil liberties. She contends that "dragnet" versus "direct" surveillance is increasingly common, distinguishing between analysis of information about *everyone* versus only those who are suspicious. The "dragnet" argument echoes Nunn and Rossler's analysis of pervasive surveillance with numerous data-collection points – the idea being that *all* data is necessary to respond to crime. Brayne highlights how police often resist federal mandates as they ruthlessly pursue massive data collection. Rushin (2014) echoes that there is a pattern of police misconduct not being addressed by the Department of Justice due to resource limitations, aligning with Brayne's position that the police can get away with wrongdoings and continue operating under the cover of employing technologies as "necessary solutions." While offering an inside look into the technologies used by LAPD, Brayne does not capture the effects of these technologies on policed populations nor prevailing mobilization patterns against them. To understand these effects, it is essential to turn to critical technology studies to grasp how the technologies used by police are biased and racist by design.

### *Critical Technology Studies*

In addition to literature on the police's general adoption of surveillance technologies, there is a growing body of literature on the racially-targetted nature of technology adoption and the problem with regard to various forms of systemic discrimination. We can categorize this literature as "critical technology studies." According to Leo Marx, policing functions as a complex sociotechnical system where a web of interconnected relations shape police's operations and the implications of the technologies they utilize (1997). With this reading and considering the total scene of actors, the notion that police technologies protect public safety becomes far more nuanced. Correspondingly, social scientists have emphasized that the "neutrality" and "inevitability" of technology are myths.

Scholars have identified serious consequences and implications of surveillance and facial recognition technology including racial and class biases, anti-Blackness, nonconsensual visibility, and targeted classification. Simone Browne (2015) draws parallels between current biometric technologies – being utilized by policing agencies – and slave branding, highlighting the importance of tracing the evolutionary history of these technologies amidst their unchanged functions: to catalogue and control Black bodies through racialized surveillance. Ruha Benjamin (2019) highlights how social structures, such as racism, are intertwined and inherently embedded in the technologies that we use – encapsulating complex sociotechnical systems. She argues that visibility or "coded exposure" often leads to racial surveillance or violence. There is a clear theme across Browne and Benjamin's research around how race and visibility directly influence policing through the carefully-targeted technologies and powerful tools used to classify and incarcerate people – disproportionately Black people and people of color.

Geoffrey Bowker and Susan Star (2000) further contribute to the arguments around classification, as they describe classification systems, such as facial recognition technology, as sites of political and social struggle. Since facial recognition technology algorithms are trained on existing unrepresentative data and predominantly trained on white skin tones, they perpetuate inequalities through codified poor accuracy on darker skin tones. Police have already misidentified and wrongfully arrested numerous Black men on the basis of bad face recognition matches (Hill 2020). These collective injustices have informed and sustained resistance efforts.

### *Resistance*

While there is extensive literature on the police's general adoption of new technologies and the associated critical impacts of these changes, the literature focused on resistance to policing technologies is limited compared to scholarship focusing on the problem itself. Kerrison et al. (2018) argue that Black youth challenge race-based surveillance practices for their clear structural injustices, but their paper mostly focuses on reasoning behind opposing surveillance rather than discussing tangible mobilization to challenge police surveillance. Adkins (2001) contributes to the scholarship covering the legal battles and mobilization through courtroom channels. He contends that in *Kyllo v. United States*, the Supreme Court had a critical opportunity to regulate the relationship between technology and personal privacy. While the Court's decision determined that using a thermal imaging device to detect heat in a private residence requires a warrant to enter, protected under the Fourth Amendment, they offered no further means of articulating when a technology has crossed the line. In other words, there has been some mobilization through legal channels; however, according to Adkins, the outcomes have not been fruitful in outlining concrete regulations.

A broader aspect of the resistance stems from police abolition and pro-abolitionist reforms that focus on demilitarizing the police. As scholars like Angela Davis, Mariame Kaba, and Ruth Wilson Gilmore have highlighted, police and prison abolition entail a vision of restructuring society and changing our current flawed model. Even when working on reform within the system of policing, literature has asserted that incremental reforms that break down power and keep abolition on the horizon are pro-abolitionist, moving toward a direction of care without violence (Kaba 2021). These aspects of resistance become relevant when looking at organizers' work specifically and their policy aims and visions.

Although many scholars have studied the general adoption of technology by police and the sociological implications of this, their contributions thus far have failed to adequately address and analyze empirical circumstances and activist resistance to technology adoption. This project contributes through a case study that directly engages the resistance and centers activists as a lens through which to study police practices. My research question specifically asks *how police in the San Francisco Bay Area are utilizing surveillance technologies and how activists have mobilized to challenge their use*. I have chosen to study the San Francisco Bay Area region as there has been increasing tension in this area around police surveillance technologies, and I seek to study how the resistance has materialized – with relevant applications to nationwide struggles. While the resistance is not showing up yet in the literature, this does not indicate that it is difficult to find. On the contrary, activism has been consistent and ongoing by numerous groups, mobilizing in various ways against unjust policing technologies, biased algorithms, and the surveillance state. My project's contribution rests on speaking directly with activist groups, learning about their work and how they are exposing police use of surveillance technologies.

## III. Methodology

My research data stems from document analysis as well as in-depth interviews. The document analysis covers the landscape of what police should be doing, as well as tensions with media reports, and in-depth interviewing reveals exactly how organizers are mobilizing and what they are challenging – extending beyond the purview of what is documented in public record.

I coded 5 text-based government documents – covering Berkeley, Oakland, and San Francisco's "Acquisition and Use of Surveillance Technology" public policies – with the following codes, based on prior knowledge: surveillance, facial recognition, regulation, policy, oversight, privacy, emerging technology, ban, bias, data, identification, and accountability. These 5 documents outlined policies, regulations, ordinances, and municipal codes about how police departments are *meant* to be utilizing surveillance technologies. In identifying these sources, I conducted searches online to find all mentions of surveillance in public record and public policy in Oakland, Berkeley, San Francisco, and Alameda County. These 5 met my selection criteria of being within the San Francisco Bay Area and having a publicly available use of surveillance technology policy.

I also analyzed 16 news and media reports as additional touchpoints beyond the government documents,

selecting pieces that are most widespread in addition to those that activist organizations share on their platforms. I chose media reports that encapsulate the issues local to the San Francisco Bay Area as well as prominent national news coverage, showing that this issue is pervasive.

Complementing the document analysis, I conducted 10 semi-structured in-depth interviews – from October 2021 to March 2022 – with members of 9 different advocacy organizations across the San Francisco Bay Area working to address police surveillance and advance justice. All interviews were conducted remotely through Zoom video-meetings; each lasted approximately 60 minutes. Interviewees were recruited through purposive sampling; I first identified the key activists and organizers to select based on their organization's website and then proceeded to reach out through email and social media, particularly leveraging Twitter. Through purposive sampling, I ensured that those I contacted would have the experience necessary to inform my research question. From there, I snowballed with 6 starting points by asking who they recommended for me to contact from their network – of those who have experience with mobilization.

To facilitate the interview process, I read a pre-written description of my study to each interviewee which included an introduction to who I am, the purpose of my research, how I plan to use the information, and a request to record the interview if they felt comfortable. All interviewees gave their consent, and I was able to record, completely transcribe, and code all 10 interviews. I coded deductively and inductively, both approaching my coding with prior knowledge from the literature as well as remaining open to new patterns that I observed in the data. Upon seeing patterns in codes and emerging themes, this guided my approach to the analysis which began with coding, then sorting interview data excerpts into categories, followed by local integration, and inclusive integration to cultivate a coherent analytical argument.

## IV. Findings and Data Analysis

### A. Technologies at Work and Policies for their Use

In terms of the concrete technologies being employed, there is significant overlap across the regions I examined: Oakland, San Francisco, and Berkeley. The surveillance technologies being used across all of these municipalities include cell site simulators (Stingrays), automatic license plate readers, gunshot detectors (ShotSpotter), facial recognition software, body cameras, social media monitoring, data mining tools (Dataminr), GPS tracking, gait analysis software, thermal imaging, and video cameras that record or can be remotely accessed.

Acknowledging the abundance of surveillance technologies in use, the technologies that my analysis focuses on are those that arose in the majority of my interview conversations with activists. Below are basic definitions of these technologies in addition to an examination of their use policies, which I will elaborate on further in my analysis.

- ShotSpotter is a gunfire locator service that is meant to identify where a gunshot was fired and send the location to law enforcement. The ShotSpotter use policy outlines that only police department personnel will have access to the system, and release of information requires a "need to know and right to know" written justification (City of Oakland, San Francisco Police Department).
- Automated License Plate Readers (ALPR) capture and analyze license plates that can be used for numerous applications including surveillance, toll collection, parking control, or stolen vehicles. The ALPR use policy outlines that its use "shall be restricted to legitimate law enforcement uses for the purpose of furthering legitimate law enforcement goals and enhancing public safety" (Alameda County, SFPD). The policy also highlights that all detections and queries are automatically recorded, and there is a required audit report including explanations for any data kept longer than 6 months (Alameda County). Further, it is only permissible to record license plates exposed to public view, and the policy states that ALPR data contains no Personally Identifiable Information (PII), although this can be obtained with "permissible purpose" (Alameda County).
- Cameras come in various forms, such as CCTV and smart home cameras, and are used for surveillance, tracking motion, and recording from various distances. The use policy for body cameras specifically prohibits "unauthorized use, duplication, editing, and/or distribution" of the

video files (City of Oakland, SFPD).

- Cell Site Simulators, also known as Stingrays, mimic cell phone towers and send signals to cell phones within a geographic area to trick them into conveying their location and other identifying information. The use policy for Cell Site Simulators explicitly prohibits the use of this technology at "crowd management events" and outlines that the technology may only be used "with a search warrant or for an identified exigency, with a concurrent application for a search warrant" (City of Oakland). Third party data-sharing requires a "need to know and right to know," and all data is to be *deleted* from the system once the phone tracking operation has been completed. An annual report is required, including all instances where the technology was requested, used, third-party sharing metrics, and demographics of who the technology located.
- Facial Recognition is a biometric technology that is meant to examine faces for identification, typically comparing with information in a large database of known faces. Alameda County and San Francisco banned the use of facial recognition by police as of 2019.

With the surveillance technologies defined, my analysis examines the juxtaposition of their purported versus actual uses.

**B. Regulation on Paper**

In addition to each individual technology's use policy, regulation on paper proclaims *a)* annual reporting requirements, *b)* data retention restrictions, and *c)* oversight stipulations. Firstly, each government document analyzed mentions that there is a **required annual report**; the city of Oakland names this the "Annual Surveillance Report," Berkeley refers to this as the "Surveillance Technology Report," and San Francisco names it the "Surveillance Impact Report." The report is meant to include a description of the technology, benefits, safeguards, costs, geographic parameters for its usage, a summary of complaints received, and information about efficacy. Despite the requirement of publishing this annual report, activist interviewees have elaborated numerous problems and shortcomings with this in practice. Reports are often significantly delayed in their publishing, sometimes entirely missing as in the case of ALPRs, or inconsistent with what is actually going on by leaving out certain technologies or associated data. One interviewee (Eden) elaborates,

> "We are currently looking at legal action and legal mechanisms for following up on annual reports and use policies. We've already filed lawsuits in 2 cities with extremely delayed reporting to put pressure on them to file their reports properly, accurately, and on time. When a city has published in the past, we've seen steps toward greater transparency since they know their practices will be publicized. This is why it's so important to make sure we have these reports and hold them accountable to it."

Another interviewee (Wynter) explains that despite the ALPR use policy that requires audit reports at least annually, "No such audits were produced in 2016, 2017, and 2018. When we brought this up to OPD in a Privacy Advisory Commission meeting in early 2021, OPD said no audits were undertaken."

Along with annual reporting requirements, regulation on paper outlines **data use and retention restrictions**. The police have also disregarded their own use policy data retention period of six months, as multiple interviewees discussed that they are holding data now for over two years – violating the Surveillance Ordinance. The data use policy violations do not just stop there, as Wynter emphasizes in our interview discussion that "OPD has given access to ALPR data to the FBI without following any of the standard data access protocols in the ALPR policy and without input from city council or the Privacy Advisory Commission." This points to another regulation on paper around **oversight and requirements for public comments**. Oversight as intended by Berkeley, Oakland, and San Francisco surveillance technology ordinance regulation requires technology proposals to undergo public discussion regarding the technology's use, costs, benefits, and concerns. Accountability and oversight are meant to be continued through annual reporting requirements.

In the face of regulation on paper, police departments' actions make it impossible for oversight to effectively take place. They are continuing to collect data ubiquitously without reporting properly and make decisions at their

own arbitrary discretion – neglecting established technology use policy requirements and surveillance ordinances.

### C. Police Use of Technologies in Practice

#### *Discourse of Public Safety*

In describing the police use of technologies in practice and tensions with regulation on paper, the narrative forwarded by the state upholding police practices is a discourse of public safety. The state's discursive strategy is to frame the problem as a lack of surveillance, emphasizing that surveillance footage is *necessary* for responding quickly to violence and crime. For example, San Francisco Mayor London Breed has proposed expanding the police's access to surveillance cameras around the city and allowing them to monitor the cameras in real-time (Johnson 2022). Many media outlets have covered this, and the San Francisco Chronicle reports that this is part of Mayor Breed's goal of "crack[ing] down on crime in the Tenderloin and citywide" (Cassidy 2022). Privacy advocates are heavily criticizing the plan for uplifting a dangerous surveillance state and leveraging anti-Asian hate crimes as opportunities to push for more surveillance as the so-called solution (Cassidy 2022).

Another example in the city of Berkeley exemplifies city officials identifying security cameras as the solution to gun violence in West Berkeley (Raguso 2021). Councilmember Taplin aligns with the public safety defense, explaining that residents "deserve the peace and security of knowing that our police department has the tools to focus… on violent crime" (Raguso 2021). This reasoning persists despite the estimated cost of installing the cameras in West Berkeley to be "$525,000-$1,050,000 up front, plus ongoing maintenance costs of $280,000" (Raguso 2021). While the police may enjoy this additional funding and discretion, activists in the media and in my interviews have highlighted that cameras have not proven to solve crimes and instead are exploited for other purposes. Police leverage the "surveillance is necessary" claims, despite evidence of bias and harm that this framework exacerbates without actually reducing crime in practice.

#### *The Dragnet of Data Collection: Disproportionate Outcomes*

Police use of technologies in practice is well-encapsulated by interviewee Lark's remark that "Investigation starts before the crime even takes place." The police begin investigating and collecting data and then proceed to selectively look for crime. This aligns with the notion that *all* footage is necessary to respond to crime and further aligns with the police's complete disregard for data retention limits, as seen with ALPR data. In practice, as emphasized in my interview with Orion, "The collection of personal data simultaneously from various technologies… creates a dangerous breeding ground for surveillance and abuse of information." Interviewee Raven described their observance of **ALPR** targeting as a widespread surveillance mechanism with no credible or useful information garnered.

> "The police with their ALPRs would go through the mosques and monitor local leaders, capturing not just the license plate itself but also for example the children of the leaders in their driveways at home next to the car… These privacy invasions create a lot of fear in a community where our visibility has already involved hazard in the past."

The sweeping, dragnet essence of ALPR usage shows how investigation begins before there is any crime or reason to warrant surveillance. Another interviewee Sun added that the "requirement of so-called 'legitimate law enforcement use' for ALPRs is far too vague of a standard and ALPRs are actually proven to racially profile and be highly ineffective in really combating crime." The vague use policy standard of "legitimate" use grants police departments discretion to surveil ubiquitously and target anyone for monitoring – with or without cause. While the intended use of ALPRs may outwardly seem to support safety, the policy's vagueness leaves room for effectively disregarding any benevolent intentions.

Police technology's scouring for crime before any crime has occurred also transpires with protest surveillance and First Amendment monitoring. With the use of **cell site simulators** in practice, interviewees once

again contrasted the narrative pushed by police and what actually occurs. Ray asserts, "The Stingray narrative by police is all focused on catching drug traffickers or investigating gang activity, but in reality Stingrays have been used to monitor protests and other First Amendment activity… the police have also been known and proven to collaborate with the FBI on this." This is firstly a violation of the use policy, which requires a "need to know and right to know" for third party data sharing. Furthermore, using cell site simulators to monitor protest activity is another example of premature investigating, collecting data, and targeting people acting lawfully within their protected right to assembly. As activists have outlined, the police blatantly ignore the intended purposes of technologies and breach their use policies to follow their own agendas. Lark explains, "The protests monitored most often are Black Lives Matter or protests against ICE … anything with a progressive agenda, the police see as a threat." With powerful data analytics and data-gathering tools at their disposal, including ALPRs and cell site simulators, the police's database of personal information about everyday citizens and community members is growing in sheer size and volume. Yet, not everyone is watched or dragged in equally; thus, the dragnet is disproportionate. Sun explains,

> "The police are watching all of us and gathering data points everywhere. But especially in some areas, they are over-policing, over-watching, and hyper-vigilant. They are literally searching for crime and sometimes, often, constructing it. Not only is over-policing a racist practice, but the algorithms are internally racist and biased as well since all they can operate off of is historical trends of who may seem suspicious or guilty – and all of this is disproportionately targeting immigrants, people of color, … those already who are marginalized. And so everywhere we go, we are scrutinized more, monitored more, and seen more by the police… Every time I go to a protest or crowded area, I have grown the natural habit to scan around all directions to be aware of where the cameras are and where I could be getting recorded. This has become second nature."

Blanche adds that as part of their additional organizing work for immigration rights, they "equip protestors [particularly those from marginalized backgrounds at progressive protests] with cover-up strategies such as always wearing physical masks at protests and informing protestors about using VPNs and alternative encrypted messaging apps like Signal to block the Stingrays."

The ALPR monitoring of mosque leaders and cell site simulator usage at protests convey the discretionary and racially-targeted surveillance that police carry out. The dragnet nature of the technology usage violates the ALPR use policy of "enhancing public safety" and the cell site simulator policy requirement of first obtaining a search warrant. The mass surveillance is fundamentally disconnected from any one particular investigation, and moreover, there is a range of completely undocumented technologies supporting the dragnet as well. While the policy on paper requires a review of all new adoptions of surveillance technology and documentation in the annual surveillance report, police departments have repeatedly failed to submit new technology policies for review. Wynter describes, "At the moment, there are at least 5 to 7 technologies OPD [Oakland Police Department] is using which they have not submitted for review and are just operating under the radar." The police's premature investigation and dragnet data collection violates the regulation on paper and allows them to make inequitable law enforcement decisions by piecing together their preferred narrative with past data.

### *Racially Targeted Law Enforcement*

Surveillance technologies in practice support the police in racially-targeted law enforcement. Interviewee Eden described two separate cases from her experience where technology wrongly identified and imprisoned a Black man after combing through previously collected data to piece together a story. The sole evidence in each case came from the technology **ShotSpotter**, meant to identify gunshot location. However, as the interviewee described, police are given authority to move the location of the gunshot by a block or two to align best with their preferred narrative of what happened at the scene. Sage clarifies, "Since the technology itself has a margin of error, police are given discretion to fill in the gaps." ShotSpotter has a track record of poor accuracy. This reliance on technology for retroactive law enforcement application and police discretion results in innocent people – in each

of these cases, Black men – serving time in prison. Justifications for this practice are directly in tension with the cautionary warnings from activists. Government documents and police organizations maintain that data collection and retention is necessary to "crack down on crime" and also anticipate future crime. Yet, crime continues, and instead we see wrongful arrests being made using questionable "evidence" from systems that cost significant amounts of money. Over four years, the San Francisco Police Department reported spending over 2.1 million dollars solely on ShotSpotter (SFPD). Despite this, as Orion emphasizes,

> "ShotSpotter's claims about reducing violence and being accurate are all a strategic marketing ploy for their business. It's very utopian and techno-solutionist, as if this is going to solve deeper-rooted problems… And crime is still on the rise across the board where ShotSpotter is used. This does not work, and it's only *creating* false arrests to be made where there shouldn't be… it is overall a very faulty technology."

Technologies such as ShotSpotter are being rolled out without careful consideration of the inaccuracies and flaws within the technology itself. Instead, it is blindly seen as an "objective" solution, and the consequences fall on those who are marginalized and targeted electively by the police – often using the technology as their exclusive evidence. Interviewees outlined how the money could be far better spent and would more directly address violence if invested back into community health, resources, and care rather than bolstering wrongful incarcerations. Orion's concern about ShotSpotter's marketing maneuvers concealing racial injustices stresses another critical aspect of the use of police technologies in practice: the technologies are often made by private, profit-seeking companies.

***Public and Private Partnerships***

Police partnerships with private corporations and entities are not a new phenomenon; however, emerging technologies are intensifying the nature of these connections and making them far more invasive. Looking at the police use of **cameras** in practice reveals a public-private partnership that, as Lark pointed out, "extends the surveillance arm of the police into people's homes and creates flows of technology from the home to the police and from the police back to the home." This control state that activists describe is advanced by private, consumer-based technologies such as the now ubiquitous Amazon Ring camera. Sage remarks,

> "People think of the camera as pointing outwards rather than pointing inwards… in reality, it's a total dragnet and the police have access to it all… once the camera is there, that's all they need since they can come up with any reason or subpoena demand to access all of the footage or even stream it live."

The police in Oakland, Berkeley, and San Francisco encourage people to register their cameras to "help solve crime," contributing to the familiar rhetoric that more cameras and more surveillance will help (City of Oakland). They are in actuality building up their arsenal and maximizing their control of cities, while at the same time mutually benefiting private technology companies' products. More than 600 – some sources report up to 1,800 – police departments nationwide have partnered with Ring, contributing to consumer-generated mass surveillance. Amazon has also thrown parties for the police and handed out free devices in their pursuit of befriending law enforcement as their esteemed customers (Haskins 2019). Blanche shared about the elaborate interconnections between the platform Nextdoor, Ring footage, and the police:

> "Nextdoor and neighborhood watch more generally have long histories that are both racialized and classed. In my activism, I've personally been targeted via Nextdoor; footage of me has been there posted for the police to come knocking on my door… This has happened to me multiple times. Police officers have also tried to ask my wife and kids questions about my anti-policing activism, stemming originally from online footage. I see people post their Ring camera videos on Nextdoor all the time, so the police basically have so many different data points and angles that they can monitor you with – from Ring to Nextdoor to anything else they get their hands on. It's hard to even find exact use policies or restrictions on this… it's like boundless power and control and data overcollection. And of course the prevalence of Ring cameras

> and these vigilante activities are only there to benefit and allegedly protect property and family in white urban neighborhoods… it's racialized, and this is undeniable."

In terms of use policies, as my interviewee also mentioned, it is very difficult to find any municipal codes on the regulation of Ring cameras; law enforcement can legally order access to the camera data and continue to promote the use of Ring in line with their rhetoric of promoting "public safety" despite any tangible crime-reducing evidence (Whittaker 2021).

**D. Mobilization Through Legal and Policy Channels**

Activists have addressed their objectives through *a)* policy channels, including by passing surveillance transparency ordinances and facial recognition bans, as well as through *b)* litigation and lawsuits such as in cases where police used a banned technology or did not publish their surveillance report. Their policy and litigation strategies are accompanied by coalition-building, community gatherings, research, public records requests, letter-writing, meeting requests, door-to-door campaigning, publishing op-eds, and widespread public education – from exposing how the police's artificial intelligence tools are biased to Blanche's work in informing protestors about cover-up techniques and how to block police Stingrays. Across their strategies, most activists that I interviewed also discussed a broader ultimate vision of reimagining the structure of our society and stripping the police of their power and tools.

***Policy Channels***

Activists' efforts through policy channels are concentrated on fighting local surveillance through surveillance transparency ordinances and facial recognition bans. In passing surveillance ordinances, which mandate use policy and screening process requirements for each policing technology, activists outlined a strategy of appealing to decision-makers' logic. Raven elaborates, "We compel them by saying like 'imagine if you found your license plate consistently somewhere, maybe a bar or church or place you visit frequently' and would you want this to be known about you?" By revealing the harmful patterns of information that stem from tracking the movements of innocent drivers, activists aim to establish clear unauthorized uses of the technology within the policy.

Appealing to decision-maker logic is not enough on its own for passing policy. Activists also use a strategy of building community power and collaborating across their organizations to meet with elected officials, post fact-sheets, share action alerts, monitor city council agendas, submit public records requests, share impacted people's stories, and show up for public hearings throughout the process of campaigning to pass a surveillance transparency ordinance. Activists highlighted that in their steps toward informing the public, one of their key objectives for this work is to hold meetings with decision-makers, legislators, and policy-makers directly where community members' voices are centered. In this light, public awareness is part of the policy arm of their mobilization. Ray explains,

> "We've found that bringing real people's experiences front and center for policymakers can be effective in making them see the issues and injustices. But in order to do this, we've had to do a lot of groundwork in meeting with community members and those who are being most impacted by police use of tech. We equip them with the right language that resonates with their experiences and that also captures the policy battles in stopping the spread of surveillance. We also inform them on exactly how these technologies are at work and the biases they contain, as a lot of this is purposefully obscured… We're empowering them with knowledge, and they combine this with their experiences to present to key policymakers and put pressure on them to put more safeguards in place and ban certain tech and get those transparency ordinances passed."

Activists put pressure on legislators directly by bringing informed community members and people most impacted

in conversation with decision-makers to achieve policies.

Although the policies are often overlooked by the police and fall within the realm of reforming an irreparable system, activists have noted in my interviews that policy can help make incremental positive change in the right direction. One of the primary goals of the surveillance ordinances is instituting transparency requirements. Eden emphasizes, "When they [the police] have to reveal what they are actually doing, they will be forced to do a better job. Transparency exposes their actions and the biases built into their tools, so we will not back down with public record requests and policy pushes and pushing for transparent and accurate reports, as they are *meant* to be doing." A few activists noted that they had seen significantly less instances of arbitrary usage of surveillance technology when police in those jurisdictions released their data in full. However, the struggle of adhering to transparency requirements still remains.

As activists highlighted in my interviews, many of the ordinance policies tend to ultimately be vague and "more watered down than intended" once they actually pass into effect. For this reason, police discretion is able to play a large role, and activists are constantly fighting for greater specificity and rigid boundaries in the language of policy regulation. Still, other policies outline ideal steps that are *not* taken in practice. For example, in the City of Oakland's existing policy, a series of steps are outlined for approving the use of surveillance technologies, including a necessary Privacy Advisory Commission meeting prior to moving forward. However, this evidently did not happen with the case of Clearview AI and Alameda County (Hegarty 2021). Alameda County police still went ahead with violating the facial recognition technology ban and worked with Clearview AI's technology; the police agencies' only "defense" was that they were offered a free trial (Leonida 2021). When annual reporting requirements, transparency codes, or technology bans as outlined in the policies are not followed, activists turn to a strategy of litigation and lawsuits. As Moon asserts, this is to "hold the police responsible for the bare minimum or in other words what is required and enforceable by policy." The policies give activists a basis for their litigation.

### *Strategy of Litigation*

Activists put pressure on police departments for transparency and accountability to the ordinances through litigation focused on suing for ordinance and policy violations; litigation has been central to activists' mobilization. Activists have led litigation efforts in suing San Francisco Bay Area cities for using facial recognition when it is banned, for missing or insufficient annual surveillance reports, and for stopping the unwarranted expansion of surveillance networks. When these lawsuits come to light, the public is also able to engage and be made aware of police abuses of power. Notably, San Francisco was sued in October 2020 by activists – Black and Latinx protestors – for the San Francisco Police Department's illegal surveilling of Black Lives Matter protesters through 400 privately-owned cameras, using facial recognition and other biometric systems that are included in the ban (Nash 2022). The police had disregarded the ban and proceeded with targeted surveillance. As Raven outlined in our conversation,

> "Despite our efforts in getting the surveillance technology ordinances passed, the police and the state continue to disregard the ordinances and abuse their power at the expense of marginalized folks and people of color… So we have to come at them with lawsuits and put pressure that way through legal channels… We cannot let them continue getting away with this."

This tension between the law and police abuse of power drives many ongoing injustices and fuels the targeted surveillance state that we are living in. Activists' lawsuits of municipalities for missing annual surveillance reports are striving to keep the police in check, and ultimately, they have seen success in getting some form of a report from the police after persistent litigation.

In the Clearview AI lawsuit, activists through litigation are challenging the invasive expansion of surveillance through biometric technologies – which inherently hold biases and perform poorly on darker skin tones. Interviewees highlighted how the use of Clearview AI as an object is inherently exclusionary. Investigations into Clearview AI have revealed connections to white supremacy and the far-right (Gilbert 2020). This speaks to the reality that many technologies are intrinsically political because their creation and maintenance requires

a certain social organization; furthermore, technologies encompass consciously political design (Winner 1980). Given the founder's ties to the far-right and the invasive nature of the algorithm itself that non-consensually scrapes billions of people's images online for law enforcement, historically marginalized people are targeted by the algorithm for identification – such as in protest settings or around immigration relief centers. Law enforcement and policing as an institution have never been "neutral" – which is abundantly evident with our current state of mass incarceration – and when granted powerful tools such as Clearview AI's algorithm, targeted biases are codified.

Activist plaintiffs – including four individual activists, alongside Mijente and NorCal Resist – have filed a lawsuit in the Alameda County Superior Court against Clearview AI for privacy violations (Hegarty 2021). The plaintiffs are challenging Clearview AI's "widespread collection of California residents' images and biometric information without notice or consent" (Bhuiyan 2021). The government may acknowledge the algorithm's bias performatively, but in practice, they are still calling for more surveillance and turning to Clearview AI. Clearview AI has made surveillance and over-policing far more accessible to law enforcement agencies. The algorithm claims to be the best tool for preventing crime, but a closer examination shows the dangerous politics and values of this object – which also align with law enforcement agencies' aims around social control. Through litigation channels, activists are resisting the police's illicit partnership with Clearview AI – given the facial recognition ban directive – and also denouncing the company's violation of privacy rights.

***Challenging the Role of Private Technology Companies***

Interviewees' shared serious concerns about the police working with private technology companies to acquire their technologies. Nine of ten interviewees explained that their mobilization demanded transparency of decision-making processes and were aimed to highlight conflicting interests behind private company contracts. Blanche explains,

> "There's a precedent for collected information to be misused, applied inappropriately… if you have a private company, gathering data, and handing it off, otherwise disseminating it, whether it's through contracts, breaches, to other agencies, there's again the potential for abuse and misuse and compromises…"

Blanche further described his involvement in a lawsuit against a private AI and FRT company in contract with the police department, and he emphasized that one of the main driving factors was this company's violations of privacy in pursuit of their own interests. He explained, "I believe that when a private company gathers this data, they don't really care about who or where the information goes to. They're concerned about making a profit." Similarly, Orion describes,

> "One of our [organization name's] key demands is breaking the partnership between private companies and the police. When you mix the ruthless pursuit of profit with law enforcement processes, this is a recipe for disaster. Why should we entrust these companies to collect our data with the carceral technologies that they make and make decisions about identifying criminals when they don't even have a place in the justice process?"

Moon additionally highlighted that in her push for abolition of the police, she is firmly against "giving the police more tools for surveillance and punishment and mass incarceration," especially when these tools are being made by "profit-hungry capitalists that are already exploiting the very people that these technologies would harm." Raven, Eden, and Lark expressed similar points and each brought up that facial recognition technology and any surveillance tools should be able to be "investigated" in terms of how these tools arrive at their biased classification decisions. When made by private companies who deem their work "proprietary," investigation and accountability become near impossible. Eden further elaborates,

> "Companies like [name] are in a way responsible for making life-altering decisions when their algorithms

> are used by the police like deciding parole or no parole, freedom or jail, deportation or not, whether someone is a risk or not… we are all just data points fed into their flawed algorithms and facial recognition systems. And the worst part is that we have no idea how their algorithm comes to their decision. [Organization name] has petitioned over and over again to have [company name] reveal their algorithm or at least what data their algorithm is trained on, but they refuse because they don't want their so-called precious 'innovation' to be taken or copied by another company. This is all in the name of *profit* and [company name] has made so much money off of working with the police and even working with ICE. They don't care that they are impacting real people's lives… they're just selling their product and perpetuating harm by doing so."

Eden is describing exactly the consequences of what Zuboff's (2019) literature describes as surveillance capitalism, or the commodification of our personal data for the use of third parties . The majority of my interviewees voiced deep concerns about the role of private technology companies in developing policing technologies, and their policy and litigation strategies have focused on breaking apart public-private collusion.

**E. Challenges to Mobilization**

Activists have been working diligently to demand transparency from the police, limit their technology tools, and hold them accountable. Yet, challenges have stood in the way around performative oversight mechanisms and public lack of awareness about the problem.

The Privacy Advisory Commission and emerging Oversight Boards across the San Francisco Bay Area are meant to be open for the informed public to comment and shape policy decisions. However, interviewees have revealed that **a)** the time allotted for public remarks is too limited to make any real impact on limiting surveillance or increasing accountability and **b)** the public is generally not adequately informed on the issues, which fuels activists' efforts to spread awareness. Oversight is more performative than practically effective.

Interviewees consistently remarked that there is not enough awareness for people to protest in the streets about this issue. They asserted that a lot of the injustices are occurring behind closed doors. Raven remarks,

> "The algorithms that police are using are essentially black boxes... the way they make decisions is invisible and most people, the average person, does not understand the injustices that these are inflicting, especially in the hands of police… More than that, the general public has no idea about how a specific technology can be biased in the first place."

In addition to the obscurity of the policing technologies themselves, many interviewees elaborated that unless we see an instance of misuse of policing technologies that "enrages the masses," we will not see mass protests, and harassment and abuse will continue "on an invisible individual level." Contributing to public lack of awareness, interviewees further remarked that the media and news reporting play a role in shaping people's awareness, or lack thereof. Lark concisely explains,

> "A lot of people, I feel, will kind of read that headline be like, 'Oh, that's awesome, these various governments... are denouncing this and they're not going to do it.' Well, it was just a simple denouncement. What the lawmakers do implement or don't implement, and even the backroom deals are completely different than the headline of an article that people read."

Thus, across my interviews, organizers suggested that part of the reason that there is not more public indignation around the issue of policing technologies is due to a general lack of awareness, and in some cases the media's masking of what is actually happening. Their mobilization entails a large component of public education through community gatherings, social media posts, and fact-sheets. This goes hand-in-hand with building a diverse coalition for change, as the push for public awareness coincides with activists' policy and litigation goals.

Mobilization through policy and litigation often require a certain level of public awareness and working diligently within institutional channels for meaningful change to occur. Recognizing the limits of this mobilization,

activists additionally noted that policing and law enforcement as a system work as they are *supposed* to – inherently flawed and unfixable. Raven explains,

> "The constant tension and conflicts between what police are supposed to do and what they actually do really makes me think that reforming a broken system will never be enough… It's not that the system is broken, but that it was built up to function in this way intentionally, all the way from police roots in slave patrols. I see our work around surveillance tech regulation and accountability as a stepping stone toward reimagining the role of police and looking toward police abolition as a more permanent solution to the corruption and power abuses."

The unchecked power of the police and their all-purpose, investigative surveillance technology tools provoke the imagination of alternate futures and means of providing safety.

## V. Conclusion

Police are using surveillance technologies to target, monitor, control, and collect data ubiquitously. My findings convey an absolute mismatch between state claims, regulation on paper, and the reality of policing. Police use of technology is bolstered by a discourse of public safety, while in reality reinforcing an unequal dragnet, supporting racially targeted law enforcement decisions, and helping to establish powerful private partnerships that further police control. To address this, activists have pursued a strategy of policy and litigation, campaigning to pass surveillance transparency ordinances and facial recognition ban policies accompanied by litigation efforts to hold police accountable for violations. Still, police departments continue to abuse their power, which leads activists to alternative imaginations of the future.

### *Vision for the Future*

Police technologies are fundamentally expressions of our current social arrangements and manifestations of the logic of policing. Innocent people are being surveilled and funneled into the carceral system, as policing technologies enforce a sense of "otherness" among those who are already marginalized. Activists are challenging the real consequences of police abuse of power and police surveillance through policy and litigation channels. While this regulation of surveillance technologies is incremental and crucial, the question of accountability still remains. Mobilization efforts fuel public awareness and work to restrict surveillance technology usage; however, a broader vision for the future of policing also arises. Many interviewees identified pro-abolitionist changes and see their work as a stepping stone to stripping the police of their technology tools, largely ineffective for public safety, with the ultimate goal of breaking down the police as an institution. The challenge lies in severing social reliance on police and countering misinformation rhetoric and law-enforcement-dominated narratives.

Given the evidence I have outlined, I see immense value in a future where the police are defunded. Specifically, given the police misuse of surveillance technologies and dangerously expansive private partnerships, I recommend policy that strips the police of their dragnet surveillance technologies, does not expand police budgets for any reason, ends data-sharing with third parties such as private corporations and ICE, repeals laws that hide police misconduct, mandates transparent reporting, and overall demilitarizes the police. Police use of surveillance technologies have shown disparate impacts against marginalized people, including people of color and immigrants. This affects people in acute ways, sparking daily fear among innocent community members. The concentration of police in certain areas further captures more crime – essentially *creating* crime with the aid of their technology tools and generating a vicious cycle of injustice. There are more effective ways to care for communities from the ground up, investing in housing, healthcare, and support services that will directly increase public safety as opposed to expanding the carceral dragnet by fueling a surveillance state.

**VI. Bibliography**

ACLU. 2018. "Stingray Tracking Devices: Who's Got Them?" (https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them)

Adkins, Douglas. 2001. "The Supreme Court Announces a Fourth Amendment General Public Use Standard for Emerging Technologies but Fails to Define It: *Kyllo v. United States*." *27 U. Dayton Law Review 245.*

Alameda Police Department. "Policy 462: Automated License Plate Readers (ALPRs)." (https://www.alamedaca.gov/files/assets/public/departments/alameda/police/hate-crime-stats/automated_license_plate_readers_alprs_.pdf)

Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. Oxford, England: Polity.

Bhuiyan, Johana. 2021. "Clearview AI uses your online photos to instantly ID you. That's a problem, lawsuit says." *Los Angeles Times.* (latimes.com/business/technology/story/2021-03-09/clearview-ai-lawsuit-privacy-violations)

Bowker, Geoffrey and Susan Star. 2000. *Sorting Things Out: Classification and Its Consequences*, Ch. 6 "The case of race classification and reclassification under apartheid" (pp. 195-225). The MIT Press.

Brayne, Sarah. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing.* Oxford University Press.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Duke University Press.

Cassidy, Megan. 2022. "Mayor Breed files ballot measure seeking to expand police access to surveillance cameras." *San Francisco Chronicle.* (https://www.sfchronicle.com/bayarea/article/Breed-files-ballot-measure-seeking-to-expand-16786369.php)

City of Berkeley. "Chapter 2.99 - ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY." Berkeley Municipal Code. (https://berkeley.municipal.codes/BMC/2.99.110)

City of Oakland. "Approved Impact Reports and Use Policies." (https://www.oaklandca.gov/topics/approved-impact-reports-and-use-policies)

City of Oakland. "Chapter 9.64 - REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY." Oakland Municipal Code. (library.municode.com/ca/oakland/codes/code_of_ordinances)

City of Oakland. "Oakland Privacy Advisory Commission Bylaws." (https://www.oaklandca.gov/documents/bylaws-and-establishing-ordinance)

City of Oakland. “Register Your Camera.” (https://www.oaklandca.gov/services/register-your-security-camera)

City of San Francisco. “CHAPTER 19B: ACQUISITION OF SURVEILLANCE TECHNOLOGY.” San Francisco Administrative Code. (https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320)

City of San Francisco. “19B Surveillance Technology Policies.” San Francisco Police. (www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies)

Electronic Frontiers Foundation. “Street Level Surveillance: Surveillance Cameras.” (https://www.eff.org/pages/surveillance-cameras)

Gilbert, Ben. 2020. “A controversial facial-recognition company working with police departments across the US is reportedly connected to white nationalism and the far-right.” *Business Insider.* (https://www.businessinsider.com/clearview-ai-far-right-white-nationalists-connections-report-2020-4)

Haskins, Caroline. 2019. “Inside Ring’s Quest to Become Law Enforcement’s Best Friend.” *VICE*. (https://www.vice.com/en/article/bjw9e8/inside-rings-quest-to-become-law-enforcements-best-friend)

Hegarty, Peter. 2021. “East Bay police used facial recognition technology despite ban.” *The Mercury News.* (mercurynews.com/2021/04/09/east-bay-police-used-facial-recognition-technology-despite-ban/)

Hill, Kashmir. 2020. “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match.” *New York Times.* (nytimes.com/2020/technology/facial-recognition-misidentify-jail)

Johnson, Cierra. 2022. “SF Mayor Proposes Expanded Police Access to Surveillance Cameras to Fight Crime.” *NBC Bay Area.* (https://www.nbcbayarea.com/news/local/sf-mayor-proposes-expanded-police-access-to-surveillance-cameras-to-fight-crime/2788375/)

Kaba, Mariame. 2021. *We Do This ‘Til We Free Us.* Haymarket Books.

Kerrison, Erin. 2018. “‘Your Pants Won’t Save You’: Why Black Youth Challenge Race-Based Police Surveillance and the Demands of Black Respectability Politics.” *Race and Justice, Vol. 8(1) 7-26.*

Koper, Christopher et al. 2014. “Optimizing the Use of Technology in Policing: Results and Implications from a Multi-Site Study of the Social, Organizational, and Behavioural Aspects of Implementing Police Technologies.” *Policing: A Journal of Policy and Practice, Volume 8, Issue 2.* Oxford University Press.

Leonida, Ellen et al. 2021. “Plaintiffs Steven Renderos, Valeria Thais Suárez Rojas, Reyna Maldonado, Lisa Knox, Mijente Support Committee, and NorCal Resist Fund v. Clearview AI, Inc.” *Superior Court of the State of California, County of Alameda.* (justfutureslaw.org/wp-content/uploads/2021-03-09-Complaint-vs-Clearview.pdf)

Manning, Peter K. 2008. *The technology of policing crime mapping, information technology, and the rationality of crime control*. New York: New York University Press.

Marx, Leo. 1997. "Technology: The Emergence of a Hazardous Concept." Technology and Culture, 51(3).

Mason, Alysia. 2015 "Continuity and change in the history of police technology: The case of contemporary crime analysis." Thesis. Rochester Institute of Technology.

Nash, Jim. 2022. "San Francisco faces hearing for summary judgment in protestor surveillance lawsuit." BiometricUpdate. (https://www.biometricupdate.com/202201/san-francisco-faces-hearing-for-summary-judgment-in-protestor-surveillance-lawsuit)

Nunn, Samuel. 2001. "Police technology in cities: changes and challenges." *Technology in Society Volume 23, Issue 1*.

Oakland Police Department. "Body Camera Policy." (https://www.aclu.org/other/oakland-police-department-body-camera-policy)

Oakland Privacy. "Toolkit: Fighting Surveillance." (https://oaklandprivacy.org/toolkit-fighting-local-surveillance/)

Raguso, Emilie. 2021. "Officials say security cameras could help curtail gun violence in West Berkeley." *Berkeleyside*. (https://www.berkeleyside.org/2021/10/15/west-berkeley-officials-security-cameras-gun-violence-city-council)

Ravani, Sarah. 2019. "Oakland bans use of facial recognition technology, citing bias concerns." *San Francisco Chronicle.*

Rossler, Michael. 2019. "The Impact of Police Technology Adoption on Social Control, Police Accountability, and Police Legitimacy." *Political Authority, Social Control and Public Policy.*

Rushin, Stephen. 2014. "Federal Enforcement of Police Reform." *Fordham Law Review, Volume 82, Issue 6, Article 20.*

Lamb, Jonah. 2017. "Courtroom testimony reveals accuracy of SF gunshot sensors a 'marketing' ploy." *San Francisco Examiner.* (https://www.sfexaminer.com/news/courtroom-testimony-reveals-accuracy-of-sf-gunshot-sensors-a-marketing-ploy/)

San Francisco Police Department. "Surveillance Impact Report. Audio Recorder - ShotSpotter, Inc. ("ShotSpotter")." (https://sf.gov/sites/default/files/2021-02/SFPD%20ShotSpotter%20Surveillance%20Impact%20Report.pdf)

San Francisco Police. "Surveillance Technology Policy. Automated License Plate Reader." (https://www.sanfranciscopolice.org/sites/default/files/2021-09/SFPDALPRPolicy20210903.pdf)

San Francisco Police Department. "Surveillance Technology Policy. Audio Recorder - ShotSpotter, Inc. ("ShotSpotter")." (https://www.sanfranciscopolice.org/sites/default/files/2021-09/SFPDApprovedGunshotDetectionTechnology20210910.pdf)

Sumagaysay, Levi. 2019. "Berkeley bans facial recognition." *The Mercury News.* (https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/)

Winner, Langdon. 1980. *Do Artifacts Have Politics?* Vol. 109, No. 1, Modern Technology: Problem or Opportunity? The MIT Press.

Whittaker, Zach. 2021. "Ring refuses to say how many users had video footage obtained by police." *TechCrunch*. (https://techcrunch.com/2021/06/08/ring-police-warrants-neighbors/)

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* PublicAffairs.

**Appendix**

**I. Interview Protocol**

[rapport]
[redacted]

[purpose]
I would like to ask you some questions regarding your experiences on this topic. There are no right or wrong answers; I am just interested in hearing what you have to say and learning from your background. *You are free to stop the interview at any time, take a break, or decline to answer any questions.*

[motivation]
I plan to use this information for an Honors Thesis research project that I am conducting as a student at [redacted]. There is value in bringing light to narratives that show the reality of police practices in our communities. Your responses will be important for us to understand this better.

[length, confidentiality, recording]
The interview will take approximately 1 hour. I will change your name and simple facts so that you are not identifiable and so that your information cannot be traced back to you – handling your information as confidentially as possible. With your permission, I will record the interview to keep an accurate record and to transcribe this interview. Is that okay with you? Do you have any questions? Can we begin?

*[introduction, thank the interviewee for meeting with me, establish confidentiality]*

1. What does your organization do?
2. With [organization name], can you tell me a bit about your role and what you do?
3. What got you interested in this type of advocacy? [policing technologies]

*[police technology usage in practice]*

4. What technologies are you aware of that the police use?
    a. How do you see FRT being used? Automated license plate readers (ALPR)? Body cameras? Shot-spotter? Cameras (CCTV vs. smart cameras which are called 'security cameras')? Cell site simulators (Stingrays)? Drones? Predictive algorithms? Social media screening? (dataminr, palantir, IBM, etc.)
5. Have you encountered instances where the police have misused a technology?
    a. If yes, could you please elaborate on this? What happened?
6. What do you know about the use of facial recognition technology by the police?

*[how organizations are **mobilizing** to confront local police use of technologies, such as FRT]*

7. What are the **actions** your organization has taken against policing technologies?
    a. Why did your organization choose these actions?
    b. How do you see your work relating to other orgs in the Bay Area who are doing this?
8. What are the obstacles to taking action, if any?
9. Are there examples of successes in taking action? What happened? Why do you think it succeeded?
    a. Failures of taking action? What happened? Why do you think it failed?
10. Has your organization put out any official statements, press releases, documents, or pledges regarding their demands around technology use by police?

*[conclusion]*

11. What policies or initiatives are of concern to your organization?
12. What policies or regulations would you like to see being enforced?
13. What are your visions and hopes for the future of how technology is used by police?
14. Is there anyone else I can talk to or anyone you recommend that I reach out to for interviewing? Community organizers? Allies?

**II. Consent Form**
**Consent to Participate in Research**

**Introduction and Purpose**
My name is [redacted]. I am an undergraduate student at the University of California, Berkeley working with faculty advisors in the Department of Sociology. I would like to invite you to take part in a research study for my Honors Thesis, which looks at police use of surveillance technologies, as well as how people are mobilizing to challenge police surveillance technologies.

**Procedures**
If you agree to participate in my research, I will conduct an interview with you at your convenience, with the default being a scheduled video-meeting. The interview will involve questions about your activism and advocacy experience. It should last about *60 minutes.* With your permission, I will audiotape and take notes during the interview. The recording is to accurately record the information you provide and will be used for transcription purposes only. If you choose not to be audiotaped, I will take notes instead. If you agree to being audiotaped but feel uncomfortable or change your mind for any reason during the interview, I can turn off the recorder at your request. Or if you don't wish to continue, you can stop the interview at any time.

**Benefits**
There is no direct benefit to you from taking part in this study. The hope of the research overall is to shed light on police use of technologies and mobilization against police surveillance.

**Risks/Discomforts**
You are free to decline to answer any questions you don't wish to, or to stop the interview at any time.

**Confidentiality**
Your study data will be handled as confidentially as possible. If results of this study are published or presented, individual names and other personally identifiable information will not be used.

To minimize the risks to confidentiality, I will destroy audiotapes after transcription, encrypt all study materials, and have extremely limited access to study records (limited to myself and my advisor).

I will transcribe the audio recordings as soon as possible after the interview, and then destroy the tapes. When the research is completed, I will save the transcriptions and other study data for reference. I will retain these records for up to 3 months after the study is over. The same measures described above will be taken to protect confidentiality of this study data.

Your information collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies.

**Compensation**
You will not be paid for taking part in this study.

**Rights**

***Participation in research is completely voluntary***. You are free to decline to take part in the project. You can decline to answer any questions and are free to stop taking part in the project at any time.

**Questions**

If you have any questions about this research, please feel free to contact me at [redacted].

**********

**CONSENT**

If you wish to participate in this study, please sign and date below. You will be given a copy of this consent form to keep for your own records.

_____

Participant's Name *(please print)*

_____ _____

Participant's Signature Date

**III. News, Media, and Reports for Analysis**

1. San Francisco Chronicle: “Oakland bans use of facial recognition technology, citing bias concerns”
2. San Francisco Chronicle: “Mayor Breed files ballot measure seeking to expand police access to surveillance cameras”
3. The Mercury News: “East Bay police used facial recognition technology despite ban”
4. Los Angeles Times: “Clearview AI uses your online photos to instantly ID you. That’s a problem, lawsuit says”
5. New York Times: “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match”
6. The Atlantic: “Defund Facial Recognition”
7. AP News: “How AI Powered Technology Landed Man in Jail with Scant Evidence”
8. Narratively: “He Was Shot in the Back By a Cop…Then Spent 18 Months in Jail”
9. NBC Bay Area: “SF Mayor Proposes Expanded Police Access to Surveillance Cameras to Fight Crime”
10. Berkeleyside: “Officials say security cameras could help curtail gun violence in West Berkeley”
11. Electronic Frontier Foundation: “EFF, ACLU, and 30+ Community Groups Oppose Weakening San Francisco’s Surveillance Ordinance”
12. Electronic Frontier Foundation: “Support for the Stop Secret Surveillance Ordinance”
13. Just Futures Law: “Renderos et al. v. Clearview AI et al.”
14. Media Justice: “Police Body Worn Cameras: A Policy Scorecard”
15. Media Justice: “Digital Discrimination: Big Data, Surveillance, & Racial Justice”
16. Algorithmic Justice League: “Facial Recognition Technologies: A Primer”