21st Century Policing:

The RISE and REACH of Surveillance Technology

ACRE ACTION CENTER ON RACE & THE ECONOMY

COMMUNITY RESOURCE HUB FOR SAFETY & ACCOUNTABILITY

About the Authors

Action Center on Race and the Economy (ACRE)

The Action Center on Race and the Economy (ACRE) is a campaign hub for organizations working at the intersection of racial justice and Wall Street accountability. We provide research and communications infrastructure and strategic support for organizations working on campaigns to win structural change by directly taking on the financial elite that are responsible for pillaging communities of color, devastating working-class communities, and harming our environment. We partner with local organizations from across the United States that are working on racial, economic, environmental, and education justice campaigns and help them connect the dots between their issues and Wall Street, so that each of the local efforts feeds into a broad national movement to hold the financial sector accountable.

The Community Resource Hub for Safety and Accountability

The Hub serves as a resource for local advocates and organizers working to address the harms of policing in the U.S. and seeking to cultivate community safety and accountability outside of the criminal legal system. The Hub is a conduit of information and assistance for local grassroots organizations across this nation and beyond.

This report was written by Jasson Perez, Alyxandra Goodwin, and Jessica Quiason of ACRE and Kelcey Duggan, Niaz Kasravi, and Philip McHarris of The Hub.

Special thanks to Kendra Bozarth, Tracey Corder and Carrie Sloan for your invaluable edits.

Acknowledgements

We want to thank the following people for taking time to speak with us about their work and law enforcement surveillance generally:

- **Albert Fox Cahn, Esq.** - Founder and Executive Director of the Surveillance Technology Oversight Project (STOP)
- **Andy Clarno** - Associate professor of Sociology and Black Studies & coordinator of the Policing in Chicago Research Group at the University of Illinois at Chicago
- **Clare Garvie** - Senior Associate with the Center on Privacy & Technology at Georgetown Law
- **Jacinta González** - Field Director & Senior Campaign Director at Mijente
- **Farhang Heydari** - Executive Director of the Policing Project at NYU Law
- **Brian Hofer** - Executive Director of Secure Justice & Chair of the City of Oakland Privacy Advisory Commission
- **Mike Katz-Lacabe** - Co-founder & Director of Research at The Center for Human Rights and Privacy
- **Beryl Lipton** - Senior Reporter & Projects Editor at MuckRock
- **Julie Mao** - Co-founder & Deputy Director at Just Futures Law
- **Rashida Richardson** - Director of Policy Research at the AI Now Institute at NYU
- **Alex Vitale** - Professor of Sociology and Coordinator of The Policing & Social Justice Project at Brooklyn College; author of The End of Policing

Executive Summary

Sitting at the intersection of criminalization and capitalism, the use of emerging surveillance technology has become increasingly popular among police departments in the United States over the last few decades. While public knowledge is still catching up to the full extent of the tools that police use, we are quickly understanding more about this technology each day. Adopted for use as police "reforms," sophisticated electronics and tech capabilities do not address the unchecked power and ballooning budgets of local police departments. Instead, they open the door for law enforcement to monitor communities while private companies profit from sales and contracts. As the movement to defund the police becomes impossible to ignore, replacing police officers with police cameras is called progress.

The fact that law enforcement has rapidly expanded the use of technologies, including facial recognition software, Stingray devices (transmitters which scan and collect data from cell phones), social media monitors, and other surveillance tools without much transparency or oversight is also greatly troubling. This development has major implications for the violation of civil liberties—especially for Black and Brown folks. Especially if police adoption of technology follows broader trends in data science, police will continue to utilize machine learning and artificial intelligence.[1] Neither of which are well regulated to protect the privacy, safety and health of **every day** people.

The rise of "big data"—huge amounts of data gathered into systems that can store, combine, and analyze them—and new systems of surveillance have assisted in expanding the arm of police and policing throughout the United States.[2] While our research finds disproportionate impacts on targeted communities and points to ways that public accountability and ownership can end profiteering, the only way to end these practices for good is by dismantling the system of policing and building one that is truly just and that shifts our paradigm from one of punishment to one of care.

The irony of the concept of so-called "proactive policing", which is purported to predict crime and stop it, is that it instead makes decisions about criminality for us—monitoring who is allowed to be in which neighborhoods and why as well as monitoring affiliations and social media, and predicting outcomes for people's futures. This irony dehumanizes those being surveilled and does not solve for the root causes of crime, while also lining the pockets of technology's creators and sellers—similar to the ways in which the prison industrial complex has operated.

Living in a "surveillance state," however, is not a foregone conclusion. Organizers across the country are pushing back against intrusive and problematic surveillance technologies by providing program models and model legislation to disrupt 21st Century Policing and ensure awareness and meaningful interventions. This report presents an overview of ongoing trends in police surveillance and the funding streams that have made and continue to make these trends possible. It also highlights ongoing advocacy efforts and provides recommendations for pushing back against the use of such technology by law enforcement.

Our five key recommendations are:

1. Defund the police and invest in community safety
2. End police surveillance data collection and sharing practices
3. End all federal funding for police surveillance technology
4. End all private funding of police departments
5. Incentivize public accountability and control of public safety

Technology is now integral to our everyday lives, but it does not have to be harmful. No matter how it's framed, surveillance technology is a threat to the safety and security of all people, but especially to communities of color. All forms of capitalism must go, including the surveillance capitalism that feeds racial capitalism.

Table of Contents

Introduction

Over the past year, the world has been overtaken by the COVID-19 pandemic. Yet as shutdowns were enacted across America, police violence against Black people continued. Still, COVID-19 could not stop the fight for racial injustice sparked by the murders of George Floyd and Breonna Taylor; people wore their masks into the street to participate in mass protests. However, rather than address police brutality, governments in the United States and across the globe have chosen to pursue new investments in and development of surveillance technology—all under the guise of public safety and health.

Long before COVID-19, the rise of "big data"[3] in the 21st century fueled the militarization of police in the US.[4] From facial recognition software to night vision equipment, American police departments have increased their use of surveillance technologies over the last 40 years. Through algorithmic-based policing practices such as focused deterrence and predictive policing,[5] law enforcement continues to gain access to technologies that enhance its capacity to surveil residents. Emerging surveillance technology has not only spread the reach and scope of policing; it has also expanded this reach within communities of color.[6] Furthermore, as witnessed by the white supremacist insurrection at the U.S. Capitol in early January of 2021 and the federal government's inept response, white people are less likely to be targeted and harassed by police.[7]

Further troubling is the fact that surveillance technologies, including Stingray devices[8] (used to capture large swaths of data from cell phones) and other tools used to surveil social media, have proliferated across the country without much transparency or oversight, a reality that carries significant implications for civil liberties.[9] In fact, police have been equipped with the resources necessary to conduct social network analysis (SNA), a method used to track and analyze social relationships within geographic systems. They maintain a large degree of discretionary control over these findings, including how they are used.[10]

Though the rise in surveillance technology is a direct response to demands for reforming or abolishing more physical, hands-on forms of policing—as explored in Section 1—it has not delivered on the promise of making policing fairer or more effective. In fact, it has instead served to exacerbate the negative impact on communities who already suffer disproportionately at the hands of law enforcement.

Police surveillance—which negatively impacts Black, Brown, and other marginalized communities and groups—both has the ability to exacerbate violations of civil liberties and to define how these communities view the US government and its role in civil society.[11] Recent research reveals that any contact with the criminal justice system can cause individuals to avoid engagement with parts of the social welfare system that document or surveil for other purposes, such as medical, financial, employment, and educational assistance. Further research has shown a growing connection between the welfare and criminal justice systems, as the administration of welfare benefits becomes increasingly digitized. For example, between 1997 and 2006, more than 10,000 food stamp recipients with outstanding warrants were lured into food stamp offices under false pretenses and arrested as part of "Operation Talon," in which various law enforcement agencies coordinated with benefits administrators in a sting operation.[12]

Various advocacy organizations are working through the lens of racial justice and privacy protections to expose and push back against any and all types of surveillance technology. As surveillance tools continue to emerge, however, privacy protections have become more complicated and the need to constantly track and challenge these tools increases.

Section 1.

The Rise and Reach of Technology

Background: Tech's Rise

Technology is not inherently bad. As with all tools and systems, policy and political choices determine who benefits from technology and who is left behind—or harmed. The rise and reach of technology have enhanced society in many ways, but technology has also been used (intentionally, though framed as coincidentally) to hurt Black and Brown people.

After a decade-long string of high-profile police killings and sustained social movements against police violence—including the Movement for Black Lives (M4BL)—police accountability has become central to the already growing demand for criminal justice reform. In December 2014, then-President Barack Obama initiated the President's Task Force on 21st Century Policing, which outlined six areas of improvement (Building Trust and Legitimacy; Policy and Oversight; Technology and Social Media; Community Policing and Crime Reduction; Training and Education; and Officer Safety and Wellness),[13] all with the implied goal of curbing violent policing and potentially improving law enforcement's presence in communities of color. Many of these reforms, specifically around data science, data collection, and visual surveillance tech (e.g., body cameras), promised the public the ability to hold police accountable, identify "bad apple" police officers, prevent racial profiling, and end the hyper-policing of communities. These reforms were intended to create a smarter, more accountable and racially just form of policing in response to the era of broken windows and stop-and-frisk style policing, which often targeted and victimized communities of color.[14]

What this task force could not address, however, was the inherently violent, racist, and classist nature and history of law enforcement. Instead, this practice in criminal justice reform paved the way for cities to become surveillance states.

Reform Is Hijacked by the Private Sector's Profit Motive

As police brutality remained (and remains) a constant, the violent legacy of racialized capitalism was upheld and entrenched, and "reform" efforts became a lucrative opportunity—for the tech sector to make a profit and for the finance industry to further extract wealth from over-policed communities whose residents remained starved of public resources.

In this way, reform efforts ultimately advanced the false idea borne from neoliberalism[15] that the private sector is more effective at systems change than public, government-backed avenues. More often than not, so-called reform is less about solving for systemic inequality, and more about solving problems in ways that allegedly help everyone "win." This method of faux inclusion does not, and cannot, lead to transformative change. At all times, we must ask: "Who is paying, and who is profiting?"

Moreover, reform initiatives led by finance and other private sectors deflect from the democratic demands of community organizations and advocates. They overshadow radical demands for police and prison abolition such as divestment from policing, the establishment of publicly controlled and democratically elected police accountability boards, and bans on surveillance technology that violate civil rights and liberties. These kinds of demands are increasing in volume and bypassing reformist demands, such as racial bias and de-escalation training.

A shift in the mid-to-late 2000s, when criminal justice reform increasingly became a bipartisan issue as states adopted reform legislation through the Justice Reinvestment Initiative (JRI), made way for surveillance technology to command influence in the reform debate.[16] Conservatives were intrigued by the possibility of profit, and many organizations on the right that had historically supported the growth of mass incarceration (directly or indirectly) changed their positions given the onset of progressive activism aimed at the criminal justice system.

Some of the reforms to improve the criminal justice system that resulted from bipartisan efforts have served to improve individual outcomes, but they have not achieved the systems change needed to be truly effective. These efforts have often focused on easier, incremental changes (e.g., support for reentry or decreased punishment for low-level, nonviolent crimes) and are driven by an interest in reducing the financial costs of mass incarceration. They rarely address the ineffectiveness and inhumanity that undergirds the American system of punishment as a whole.

While many examples of bipartisan reform were being devised and implemented—including the passage of the First Step Act in 2018,[17] a relatively symbolic law that impacted few people and is unlikely to create lasting change—community demands and advocacy for police accountability remained largely ignored. Rather than confronting violent police behavior or addressing the systemic roots of poverty and violence, surveillance tools are reinforcing these problems. In response, communities of color are predominant among those rallying against the use of technology that further criminalizes them, especially against technologies that are created with inherent biases. Examples of these kinds of biased technologies include predictive policing and risk assessment tools, which imply that crime or criminal pathology of a person can be pre-determined based on the environment a person lives in or aspects of their race and/or class standing. The data used by these tools is also based on historically racist information that already exists in the legal system, and is further used to create new algorithms to predict an individual's "risk" to society. Other problematic technologies include facial recognition technology, which is far from perfect and continues to misidentify Black people and people of color, and surveillance cameras and gunshot detection technology that can also record conversations, which have made their way into public housing.[18] Additionally, counterterrorism efforts, which were ramped up during the global "war on terror", have been used to justify increased surveillance of both Muslim Americans and protesters exercising their First Amendment rights.[19]

While the 21st Century Policing effort started by the Obama Administration acknowledges that people of certain demographics are more policed and criminalized than others, the proposed solutions to racial bias in policing that rely on automation and technology have only perpetuated these disparities. For example, current policy recommendations for reforms to reduce police violence and racial bias involve adopting technologies such as body cameras, big data policing, data transparency policies, or electronic monitoring systems to track police behavior and practices.[20] Such reforms enrich law enforcement technology companies, but do little to reduce the funding and power of policing or meaningfully reduce the effects of police violence.[21] Claims of efficiency and progress tied to surveillance technology unfortunately still come at the cost of continued or increased racial profiling and over-policing of historically marginalized communities.

While use of surveillance technology that disproportionately harms people of color increases, companies that benefit financially from these technologies continue to impede regulation and transparency efforts. Technology is moving faster than legislation can regulate, blurring lines around privacy rights and what is considered invasive or outright unethical. In fact, the finance and technology industries work to prevent legislation which would hold emerging technologies accountable to privacy rights and civil liberties, ultimately creating the appearance of a government that is inefficient and unable to keep up with technology.[22]

Bolstered by lax enforcement, this technology exacerbates the privatization of police. Already, cities are heavily reliant on contracts with tech companies, and every day residents opt into purchasing surveillance technology that empowers them to criminalize their neighbors (e.g., Ring doorbell cameras and Nextdoor neighborhood apps). As surveillance technology rises in popularity and accessibility, it strengthens the relationship between tech, finance,

and policing to create a safety net of support for the super-rich and executive classes. This is racial capitalism shape shifting, as it pretends to respond to the moment while actually using it as an opportunity to enrich the already wealthy and minimize the rights of people of color.

The Growth of Law Enforcement Technology and the Role of Public Money

Racial unrest and injustice are profitable. Black and Brown people pay the highest cost, but as public money is increasingly directed toward private interests and profit, we all pay. As social unrest continues, the financial interest in surveillance technology companies also increases.[23] On June 4, 2020, in the midst of the Black Lives Matter uprising across the United States, the official Nasdaq website informed investors that "law enforcement stocks are suddenly attracting attention, as new police reform policies and improvements to police procedures could accelerate an adoption of law enforcement technology."[24] The two companies referenced were Axon, known for developing body cameras and TASER "smart weapons", and ShotSpotter, a company known for gunshot detection technology. These companies are among those poised to make a profit from police responses to unrest; the law enforcement and police modernization market is projected to reach $59.9 billion by 2025.[25]

For profit companies, including Oracle, Microsoft, Axon, ShotSpotter, IBM, Tyler Technologies, and Fulcrum Biometrics, have contributed to police, surveillance, and incarceration infrastructure that receive public funds from a variety of government programs. including the Community Oriented Policing Services (COPS) program, the Department of Justice Assets Forfeiture Funds, and Housing and Urban Development (HUD) Safety and Security grants.[26] In fact, government contracts—funded by taxpayers' dollars—are a major source of revenue for law enforcement technology companies.[27]

In general, firms whose revenue strategies focus on government contracts have a positive relationship to finance investment in the form of venture capital, private equity, Silicon Valley incubators, or stock market valuation.[28] For example, Axon (formerly called TASER International) saw its stock price increase after the uprisings in response to the murders of Michael Brown in 2015 and George Floyd in 2020.[29] As one of the leading law enforcement technology firms, Axon promotes its products as having the ability to reduce use of force by police, going as far as to claim it has "averted over 200,000 potential deaths by police deadly force."[30] Law enforcement technology firms have been adept at marketing their tools as being able to reduce crime through prevention (through the use of predictive policing), allow for accountability and deterrence in cases of racist police violence (through the use of body cameras), and decrease the number of people incarcerated (through bail algorithms).

University of Illinois scholar Brian Jefferson explains that though the trend may seem new, computer and digital technology companies, financial firms, and government law enforcement agencies have worked together since the 1960s to build out the modern police, surveillance, and incarceration technology industry, as seen with the advent of the Law Enforcement Assistance Administration (LEAA).[31] The LEAA was a part of a package of federal policing reforms passed in response to the civil unrest of the late 1960s that called out police violence against Black people.[32] One of the aims of the reforms was the professionalization of the police, touted as a path toward police accountability and better community/police relations with the communities in which they work.[33]

Achieving so-called professionalization—and thus police accountability to the communities they serve—was to occur through the computerization of local police data, which led to the LEAA distributing $247 million in grants to local governments from the 1970s through the early 1980s to ensure data standardization.[34] In addition, Congress appropriated another $500 million in 1970 for the expansion of police technology and equipment, which helped create the marketplace for information technology companies in the law enforcement, surveillance, and incarceration industry.[35] The LEAA was thus instrumental in standardizing data and information protocols for these technologies, and it operated the same way as other government agencies (e.g., Department of Defense, Department of Homeland

Security) in its relationships to private industry, particularly the technology industry. Government agencies like the LEAA created the private and public marketplace for the law enforcement, surveillance, and incarceration industry overall, while also creating the regulatory and administrative framework for how the financial sector would interact with the public sector side of these industries.

Various government agencies have pushed the technological ambition of policing, surveillance, and incarceration technology. Since 9/11, the Department of Homeland Security (DHS) has set the terms of the law enforcement technology marketplace. Multiple government grant systems, including from the Department of Homeland Security and the Department of Justice, funded the private sector creation of data center companies, digital camera tracking companies, and license plate reader technology.[36] Another Department of Homeland Security program is the DHS Science and Technology Directorate Silicon Valley Innovation Program, which has awarded $3 million to small tech companies since 2015.[37] The program exists to facilitate the transition of police, surveillance, and incarceration technologies from the stage of incubation into the marketplace.[38] Still, it is important not to oversell the value of this DHS venture capital inspired program, which as of last year was under threat of folding.[39] It is also important to observe the quixotic adventures of government venture capital finance, which ensure a marketplace for other private sector actors. This is demonstrated by the public safety venture capital firm Responder Ventures, which bills itself as the go-to firm for investing in other private firms to make money selling its technology services, primarily to police. Responder Ventures has also teamed up with Amazon Web Services to provide experiment labs that connect entrepreneurs to public safety agencies and public safety technology firms to develop best practices for marketing and selling surveillance technology.[40]

The behaviors of the surveillance technology and finance industries overlap in many ways, including in the ability to amass wealth, power, and size. Both are also predatory towards communities of color and historically marginalized communities, and when it comes to surveillance, these two industries essentially work in tandem. Many surveillance technology companies are funded by private equity and hedge funds, or get their valuation through being traded on Wall Street. In many instances, this dynamic allows tech companies to take on public sector bids and contracts even when they are not profitable due to lack of funding by the finance industry.

The financial opportunities tied to surveillance technology advancement have led to the proliferation of data buying and selling, a phenomenon referred to as "**surveillance capitalism**," which we further explore in the next section. ■

Section 2.

How Technology is Used to Police Communities

From police militarization and the disproportionate surveillance of Black and Brown communities to deep relationships between the public and private sectors, the rise and reach of 21st century technology has had deeply insidious consequences. Here, we define surveillance capitalism and examine core examples of it to bolster our case for the recommendations we provide in Section 5.

Defining Surveillance Capitalism

The concept of surveillance capitalism was popularized by social psychologist Shoshana Zuboff, and explains the ways in which private human experiences (e.g., conversations, buying habits, travel habits) are collected, computed, and then sold off to private businesses as behavior prediction technology.[41] As it stands, surveillance technology is ubiquitous. From Facebook, which was previously exploited by companies like Clearview AI to scrape images for facial recognition[42] and social media more generally,[43] to agencies like Immigration and Customs Enforcement (ICE) that utilize it to track down immigrants for arrest and deportation, surveillance technology is becoming increasingly pervasive. The potential for wealth-building from surveillance capitalism has meant it is in the best financial interests of tech companies and law enforcement agencies to have the general population oblivious to the potentially insidious uses of buying, selling, and sharing individuals' data. As writer and activist Cory Doctorow said when referring to the symbiotic relationship and data exchange between big tech and law enforcement, "there is no mass state surveillance without mass commercial surveillance." [44]

Every time someone uses certain technologies (such as web browsers, phone apps, and the like) they create data. Data brokers collect this data and sell it to companies using it for advertisement purposes. Often, these companies then sell that information to law enforcement agencies,[45] who can use it for movement tracking or behavior prediction. For example, ICE uses this information to track immigrants for detention and eventual deportation. Other database broker companies offer local law enforcement and private investigators access to collect individuals' addresses, phone numbers, e-mail addresses, social media accounts, family members, neighbors, credit reports, property records, criminal records, and more.[46]

Surveillance capitalism has also flourished due to the growth of underground economies (e.g., sex work, the drug trade, and under-the-table work), in which more and more communities of color are pushed to work—as a result of long-term public disinvestment and poverty—and which are heavily surveilled and criminalized. This makes Black and Brown people more vulnerable to contact with law enforcement, through methods such as stop-and-frisk,[47] or to immigration enforcement through workplace raids.[48] Attempts to crack down on underground economy activity have included police intervention in small business affairs, on construction building sites, in restaurants, in contracted work (such as families hiring domestic workers like cleaners and nannies), on Indigenous reservations, and more.[49]

Surveillance, poverty, debt, and incarceration are all inextricably linked, and scholars have argued that policing and incarceration inevitably serve the function of social control and maintenance of broader racial and class orders.[50] Google, Facebook, and Amazon are some of the well-known corporations making headlines[51] for their growing influence on law enforcement and on surveillance more broadly.[52] For example, as the US funnels more money into ICE specifically, the agency has solicited the help of Silicon Valley and entered into explicit contracts with companies like Amazon and Palantir to collect, store, and manage the data it uses to arrest, detain, and deport immigrants.[53]

Overall, data collection and surveillance technology are, in one way or another, supporting and reinforcing capitalist structures of race, class, and criminalization because they are often used as justification for more

policing rather than evidence to support fully funding public services that reduce poverty and violence.

The Targeted Surveillance of Marginalized Communities

Though often touted as a way to resolve issues of human bias in law enforcement, surveillance technology has historically been used to disproportionately target, monitor, and ultimately criminalize communities of color.

Surveillance that disproportionately impacts people of color in the US can take different forms depending on who is targeted, though many of these forms overlap. As outlined above, surveillance technology is racist by design, and it serves and preserves racial capitalism, racial injustice, and racial inequality.

Immigrants, especially those who are Latinx, are often targeted by surveillance that ties back to ICE. This includes gang policing, which adds individuals to a database to be shared with federal law enforcement agencies and is in turn used to conduct gang raids for the purpose of detention and deportation of undocumented people.[54] Muslim, Arab, and South Asian (MASA) communities are often targeted by counterterrorism surveillance efforts, which were especially heightened after the 9/11 attacks.[55] In 2014, President Obama introduced a new surveillance program that shifted from surveillance efforts solely being carried out by law enforcement to Countering Violent Extremism (CVE) programs that recruited community members (like mental health professionals, religious leaders, and school administrators) to partner with law enforcement and share information about people who might be prone to terrorist radicalization.[56]

Black Americans are often targeted by surveillance in the form of gang policing and the gang databases it fuels,[57] as well as through the FBI's "Black Identity Extremist" designation.[58] With more protests against police brutality and social movements focused on Black liberation, leaked documents have shown that the federal government has increased its focus on Black activists as potential sources of radical, and therefore dangerous, behavior.[59] Much as CVE programs are used to surveil MASA communities, the "Black Identity Extremist" designation is used to surveil and potentially detain Black individuals engaged in First Amendment-related activity.

Black communities and other communities of color are often subject to precision and predictive policing tactics that surveil neighborhoods to collect crime data and predict future criminal activity, often leading to racial disparities in who is being watched and who is being criminalized. This "dirty data" then becomes the basis of algorithms used to make policing decisions, further perpetuating the racial disparities in law enforcement.[60] In New York City, for example, police have been working in conjunction with the local housing authority in furtherance of gang conspiracy cases to electronically monitor public spaces in an effort to link people together.[61] This monitoring is not only meant to identify illegal behavior, but also to establish social relationship networks so officers can make claims about people's gang affiliations. To further establish these connections, the New York City Police Department (NYPD) also engages in social media surveillance, browsing public posts or creating fake social media accounts to become associated with individuals in whom they are interested.[62]

Police Militarization and the Revolving Door

Surveillance technology fuels and is fueled by the militarization of policing, which has been demonstrated through both police behavior, such as law enforcement's treatment of Black Lives Matter protestors, and the equipment police departments have acquired, including weapons of war.[63] The 1033 Program was authorized in the 1997 defense budget, and facilitates the transfer of surplus military equipment to domestic law enforcement agencies around the US, including the large armored vehicles that, over the past decade, have most often been seen threatening protesters.[64]

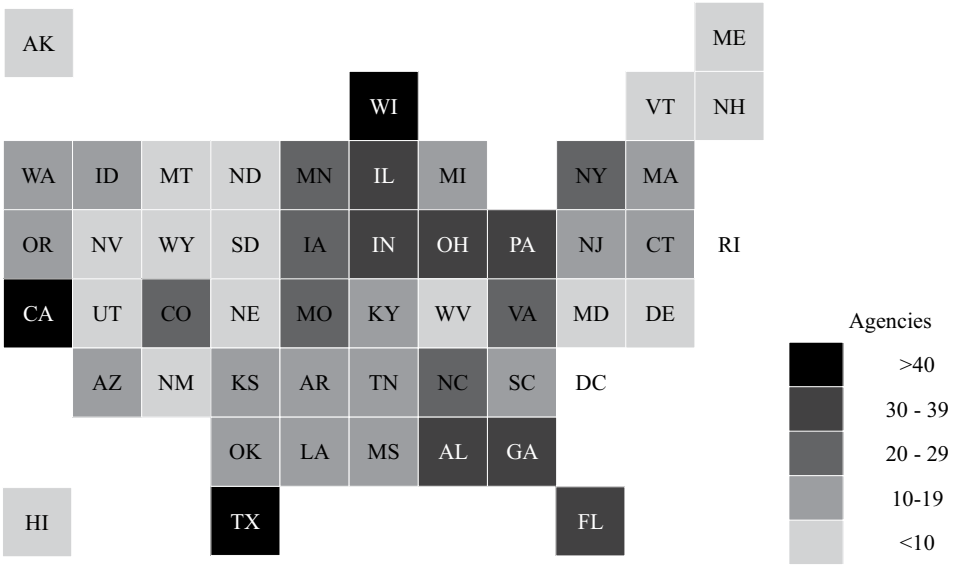
More recently, police technology has also become more militarized through the acquisition and development of intelligence software and information technology. This includes everything from large-scale aerial surveillance tools such as drones or planes, cell phone tracking capabilities, and facial recognition software,[65] to departmental database management

tools that can handle vast amounts of raw data input, analyze this data, and produce critical insights about individuals so officers can make decisions in situations that may otherwise be time-consuming if done manually.[66] Much of this technological equipment is transferred through the federal procurement process, just as physical military equipment is transferred.[67] A major concern about this federal procurement process is that it is often facilitated under the justification of combatting terrorism, and therefore often sheltered from local oversight and input. This means that local police departments are able to adopt highly developed surveillance technology tools with no official record of attempting to explore their efficacy or the potential civil rights violations they bring.[68]

Likewise, companies that once specialized in military intelligence operations, such as Palantir, have shifted to creating surveillance technology for domestic use in the US. Palantir was founded in 2004 and was initially partnered with the Central Intelligence Agency (CIA) and information-gathering units of the US military, but has since expanded its partnerships to include domestic law enforcement agencies.[69] Palantir technology provides law enforcement with the ability to collect large amounts of data from incident reports, officer field interviews, automated license plate readers, and other surveillance tools around a city and compile it into organized files.[70] These militarized surveillance responses are often justified as counter-terrorism efforts, but that justification is nothing more than a loophole to allow law enforcement to use this technology beyond monitoring potential violent extremism. For example, in the case of gang policing and precision policing, officers will collect information on individuals (e.g., license plate numbers and vehicle descriptions, tattoos, physical characteristics, etc.) and use technology to organize and store this information for future policing of those individuals.[71] Palantir has become ubiquitous in the US through its partnerships with all levels of law enforcement, from the CIA to ICE to state and local-level police departments. Despite its growth in popularity, little is known about the full reach (and profits) of Palantir's surveillance systems, in particular what kinds of information its tools collect and share and its potential civil rights violations.[72]

Another tool often associated with US military operations abroad is the drone. Some experts argue that the availability and use of drones, or small unmanned aircraft systems (sUAS),[73] have been largely overlooked when discussing surveillance transparency and oversight within the US.[74] Researchers from Bard College have found that, as of May 2018, at least 910 state and local law enforcement agencies had purchased drones (see image below).[75]

Map of Public Safety Agencies with Drones by State



Gettinger, D., 2018. Public Safety Drones: An Update. Retrieved from https://dronecenter.bard.edu/files/2018/05/CSD-Public-Safety-Drones-Update-1.pdf

As overhead surveillance develops, marginalized communities, communities of color, and often over-policed neighborhoods are likely to be targeted. For example, drone surveillance testing by the Boston Police Department in 2017 focused mainly on a predominantly Black and low-income neighborhood in Jamaica Plain, and drone usage in Baltimore, currently making a comeback, has often disproportionately targeted communities of color.[76] Because of the reintroduction of Baltimore's Aerial Investigation Research (AIR) program and the controversy surrounding it, the NYU School of Law Policing Project has taken on the task of performing an independent audit of the program to assess its implications for privacy, racial justice, First Amendment rights, and other ethical concerns, results pending.[77]

The 2014 uprisings following the murder of Michael Brown by police in Ferguson, Missouri, emphasized the extent to which domestic law enforcement agencies had transformed into military-style operations. Though the purchase of military weapons, vehicles, and SWAT gear has since become more visible, the acquisition of domestic intelligence tools for the purpose of surveillance remains opaque.[78] Despite US military officials pointing out the ethical concerns around using military-style intelligence against American people, domestic law enforcement agencies continue to engage in these tactics.[79] Telephone call data picked up by the National Security Agency (NSA) is meant to track international communications, but the NSA has been known to collect data from purely domestic calls as well. Additionally, international military agencies have been caught engaging in domestic intelligence operations to spy on protesters engaged in activities protected by the First Amendment and sharing this information with the FBI as well as with state and local law enforcement data fusion centers[80] It is important to note that exposing these types of technologies is difficult, and often squashed on the basis of "state secrets" privileges that allow the federal and state governments to withhold information about intelligence operations.[81] The secretive and unregulated nature of police militarization when it comes to technological equipment, heightened by increasing tensions between civilians and police brutality protesters and law enforcement, can ultimately erode community trust and safety, as well as impede reform efforts—especially if the lack of transparency and oversight of these military equipment acquisitions continues.

As mentioned earlier, the 1033 Program is one way that the federal government provides support and physical equipment to local police departments that want military-grade tools. Every year the federal government also makes billions of dollars available through its numerous agencies to local police departments for the broad purposes of public safety. The US Department of Justice (DOJ) and the Department of Homeland Security are the main suppliers of funds related to enhancing and strengthening all levels of law enforcement, but the US Department of Agriculture, the Department of Health and Human Services, and the Department of Energy have also provided grant funding to local law enforcement agencies.[82]

The Revolving Door of Surveillance Tech

While federal agencies have shown willingness to make billions of dollars available for policing and surveillance, tech companies have worked to establish strong relationships with the federal government. A report from Mijente, "Who's Behind ICE: Tech and Data Companies Fueling Deportations," details how in 2010, the Federal Chief Information Officer (CIO) of DHS, Vivek Kundra, instituted a "Cloud First" policy that "encouraged the private contracting of $20 billion in cloud services across the federal government and projected DHS as the largest potential client."[83] This has created the opportunity for a "revolving door" effect between cloud service providers and the federal government.[84] Specifically, tech lobbyists have made significant campaign contributions to Congresspeople, former and future tech lobbyists have taken executive level positions in government agencies, and former government officials have gone on to take jobs at major tech companies. More specific examples include:

- The first Federal CIO and author of the Cloud First policy, Vivek Kundra, left the office in 2011 to take a job at Salesforce;
- The second Federal CIO, Steven Roekel, worked at Microsoft from 1994 to 2009;
- The third Federal CIO, Tony Scott, was CIO of Microsoft from 2008 to 2013 and CIO of cloud provider VMware from 2013 until his 2015 federal appointment; [85] and

- Most recently, the Biden administration appointed former employees of Facebook and Amazon to its transition team.[86]

These "revolving doors" provide direct lines between federal government agencies and technology companies, which could make it possible to solidify common priorities between the federal government and the tech industry, and allow for them to inform each other of needs and trends within their institutions and create more opportunities for profit.

Similarly, the DHS Science & Technology (S&T) Directorate—DHS' research and development arm—works to promote research, development, and investment needs and priorities, and to build relationships with contractors to support the creation and acquisition of technology to help DHS carry out its law and order priorities. The investments that the S&T Directorate have established for Fiscal Years 2018-2021 include the following technical categories:

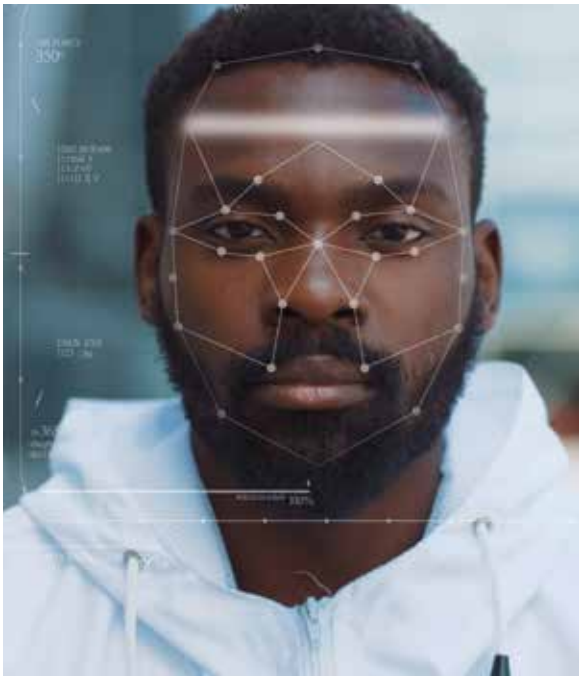
- Sensors, Detection Devices, and Screening Systems
- Data Exploitation, Pattern Recognition, and Analysis
- Communication Systems and Networks
- Information Sharing and Display Environments
- Cyber and IT Monitoring, Vetting, and Security Assurance
- Robotics and Autonomous Systems
- Modeling and Simulation
- Biometrics Collection and Utilization

To bring some of these investments to life, the S&T Directorate offers grants and development tools to move the process along more rapidly so DHS can create or acquire technology.[87]

As federal agencies have worked to make it easier for tech companies to get their technology in the door and used on the ground by law enforcement, tech companies have also worked to facilitate this. For example, ShotSpotter has staff dedicated to helping local police departments identify grants and acquire funding to purchase ShotSpotter equipment and support. ShotSpotter has managed to make itself an approved acquisition under the US Department of Justice, the US Department of Housing and Urban Development, and the Department of Homeland Security.[88] There are also a number of resources available, such as PoliceGrantsHelp.com, that provide avenues for local police departments to identify state, federal, philanthropic, and corporate grants and sponsorships for technology.

Beyond Facial Recognition: Biometric Technology

Facial recognition is not the only nor the gravest concern when it comes to biometric technology.[89] Other types of biometric technology—such as those that collect DNA and fingerprints or those that utilize gait recognition or recognition of other body parts—are increasingly used by law enforcement. Unlike clothing choices, hairstyle, or facial hair, a person's biometric traits are permanent and immutable, so once their biometric data is in the system, a person can face over-policing and continued surveillance for the rest of their lives. DNA and other biometric data are sometimes collected or provided for seemingly innocuous reasons, such as ancestry tests, but once in the hands of private companies they can be used to obtain other information about a person. For example, in addition to being used to identify a person and their line of heritage, DNA can also help predict what a person looks like through genetic phenotyping. Genealogy technology companies have created programs that attempt to render what a person's face may look like based on DNA analysis to aid law enforcement investigations; however, the results are often average and not always helpful or detailed enough on their own.[90] Nonetheless, law enforcement has taken advantage of genealogy technology to construct possible faces of individuals and examine DNA from ancestry databases and



genome research databases for connections to DNA collected in their investigations, referred to as forensic genealogy.[91] This method's increasing popularity among law enforcement, especially after investigators used forensic genealogy to identify the Golden State Killer in 2018, poses potential privacy risks for individuals who voluntarily participate in genetic testing for ancestry or health screening purposes.[92] (This genetic data can also be used to make predictions about types of behavior or the probability of physical or mental illnesses and how to treat them, among other applications).[93]

While this scientific advancement has benefits for wellbeing, it can potentially come at the cost of assumptions about behavior and criminality[94] that can be used to discriminate against certain populations. Beyond DNA, experts are also concerned about emerging tools, such as gait recognition technology that analyzes the shape of ears or other body parts and stores this information in a personally identifiable profile,[95] aggression-detection based on facial expressions or voice recognition,[96] and thermal imaging to monitor body temperature—an especially concerning tool in the age of COVID-19 surveillance.[97]

Big Data and Data Fusion Centers

As surveillance technology becomes more commonplace in domestic law enforcement, it is important to remember that its use does not exist in a vacuum. Rather, American law enforcement agencies belong to and uphold a vast network of surveillance tools, data, and information sharing from the local to the national level. Though evidence shows the existence of some level of data sharing before 9/11, it was this moment in American history that catalyzed the massive expansion of the practice, as the federal government investigated why American intelligence agencies had no knowledge of the planned attacks and were unable to prevent them.[98]

To facilitate more efficient inter-agency information sharing, state governments and the federal government invested heavily into building the infrastructure for what we now call data fusion centers.[99] Data fusion centers rely on accumulating large amounts of data from various sources (e.g., surveillance cameras, telecommunications data, facial recognition, gang databases, etc.) and then organizing and coordinating the sharing of this information among state, local, and federal police, as well as with intelligence agencies and in some cases private companies.[100] The proliferation of data fusion centers post 9/11 was originally justified as a necessary counterterrorism effort; however, the mission creep—the expanded use of a program beyond its original intended purposes—of data fusion centers has resulted in their use for other purposes, like basic policing and spying on social movements.[101] As of 2017, there are currently 79 data fusion centers operating around the US.[102]

The role of data fusion centers as tools for law enforcement has continued to expand throughout different communities across the country. As the number of these centers has grown, leaked documents have shown that the surveillance data they have collected and shared has been used to investigate relationships between Muslim civil rights organizations and the anti-war movement; to classify state universities, colleges, and historically Black colleges as potential threats for radicalization; and to spy on abortion protesters.[103] Data fusion centers are not controlled by the federal government; they are instead typically designated by state governors and run by state law enforcement agencies. However, larger cities (e.g., Los Angeles, Chicago, Houston, etc.) will have data fusion centers established and run by city police departments, who work closely with state-level law enforcement counterparts and maintain relationships with federal agencies.[104] The Chicago Police Department (CPD), for example, has a fusion center with the express purpose of facilitating data sharing between the FBI; Homeland Security; the Drug Enforcement Administration (DEA); the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); state police; and local municipal police departments.[105] This center is equipped with new surveillance technology and new data integration platforms gained through the federal government—most of them paid for with funds from the Federal Emergency Management Agency (FEMA), which is an agency under the Department of Homeland Security.[106]

As mentioned earlier, data fusion centers originated from counterterrorism efforts but have spread to basic policing practices, border and immigration surveillance, and targeted policing of marginalized communities. In Chicago, the language around terrorism soon became

a justification for expanding surveillance of all Black and Brown people, poor communities, and so-called radical movements across the city.[107] The gang database in Chicago—used as a clearinghouse of information on primarily Black and Latinx individuals believed to be involved in gang activity, regardless of whether the individual is actually part of a gang—has been an integral part of the data fusion center. To date, at least 500 agencies around the country have access to CPD's Clear Data System, and one of those agencies is ICE, which uses this data to search for alleged gang members and target them for deportation.[108]

Though ICE has relationships with state and local police departments that allow it to access their data fusion centers, ICE has also contracted out its own data fusion efforts to companies such as Palantir and Vigilant Solutions.[109] The technologies created and utilized for ICE data fusion efforts involve the collection of vast amounts of data from the internet and mobile devices; Smart Cities technology like cameras, microphones, and sensors; and cell phone stimulators like Stingray technology, as well as collecting data from other surveillance sources like Automated License Plate Readers, all of which is considered big data.[110]

As a result, immigration advocates note that big data has come to play an integral part in family separation and immigrant detention at the border. Research and reporting have revealed that ICE uses surveillance and big data to amass large amounts of information on those it is processing and targeting, with many companies and even university research departments benefiting in the process. The federal government has increasingly contracted with private companies and institutions of higher learning to pay for research on data collected via surveillance to track and target undocumented or so-called dangerous immigrants for detention and deportation, resulting in a $23.7 billion immigration enforcement budget by 2018.[111] In 2019, the New York Times reported that ICE had collected terabytes of information from various sources of surveillance technology, state and local governments, private data collection companies, and social media websites, piggybacking on software and sharing agreements originally intended for counterterrorism and criminal investigations and instead using them to create files on persons and communities of interest for targeted immigration enforcement.[112] ICE has also used biometric surveillance to collect DNA from detained immigrants in an effort to track down members of their families, an effort that extends beyond undocumented immigrants to lawful permanent residents and poses civil liberties concerns.[113]

International Context

Some of the surveillance trends seen in the United States actually originate outside the country, such as from the Israeli Defense Forces (IDF). The Israeli military works with a range of private Israeli corporations that develop technology and test it in the occupied territories, then advertises the surveillance tools on the global homeland security market as tested and proven effective.[114] These devices are often featured at policing conferences, like the annual International Association of the Chiefs of Police (IACP) conference, where companies display and promote their latest technologies to police chiefs, who then test out or purchase these tools to bring them into the US.[115]

Section 3.

Follow the Money: the Funding Sources and Systems That Support Surveillance Technology

Technology's rapid rise and massive reach are possible because of the profits, public and private, that support it. Here, we map notable examples of corporate and private sources that fuel—and profit from—the tools that disproportionately harm people of color.

Corporate Support for Policing and Sponsorship for Law Enforcement Technology

Corporations play an important role in making surveillance technology accessible to law enforcement. Technology corporations have built strong relationships with and receive contracts from the federal government and local police departments. Even corporations with seemingly little interest in public safety are deeply invested in the growing surveillance state. Corporations have been known to donate directly to police departments, police foundations, and philanthropies that support policing.

On a local law enforcement level, surveillance industry company blogs acknowledge there is a growing trend of public-private partnerships to promote public safety,[116] including police departments gaining access to privately owned and operated cameras in a given city.[117] Essentially, these companies provide a list of approved or suggested vendors to the public and encourage residents to buy cameras and have them registered with the local police department. Two examples of this are Project Green Light in Detroit[118] and the Private Security Camera Incentive Program in Washington, D.C.[119] In many ways, these are examples of public-private partnerships and corporations explicitly supporting policing.

Police foundations are a notable source of corporate sponsorship of police-serving technology. Reports show that in August 2016, the Baltimore Police Department had been flying a drone over the city of Baltimore—a city that already has over 700 cameras, predominantly in poor, Black neighborhoods—for nearly four months without knowledge of the public. The drone was created and being tested by Persistent Surveillance Systems, based in Ohio. It had been kept a secret because there was no public money spent on it; instead, the technology was paid for with donations made by the Laura and John Arnold Foundation[120] to the Baltimore Community Foundation.[121] In 2019, the Laura and John Arnold Foundation again offered to cover the cost of a $2.2 million-a-year drone program that would give the Baltimore Police Department three surveillance planes.[122]

Corporate sponsorship and donations prompt questions about the vested interests of donors. In the US and around the globe, there is a history of large donations being used as leverage for political and social power and influence. When corporations provide financial support to police departments and their foundations, we can assume that this is a blatant ask to not only keep corporate interests in mind but to also keep them safe. In other words, police departments are incentivized to prioritize private interests over public wellbeing.

Case Study: Atlanta Police Foundation

The Atlanta Police Foundation was created in 2003, and launched its flagship program, Operation Shield, in 2007.[123] In 2011, the foundation's video integration center (VIC) was equipped with 17 cameras. By 2014, the number of cameras had reached 1800, comprising both publicly funded and privately owned cameras.[124] As of 2020, there were at least 10,000 publicly and privately owned cameras feeding into the VIC,[125] making it one of the largest surveillance networks in the world.[126] In 2012, the Loudermilk Family—the namesake of Loudermilk Companies, a real estate investment and operating company in Georgia—gave

the VIC a $1 million donation, for which the department renamed the facility the Loudermilk Video Integration Center.[127] Robin Loudermilk, who is the President and CEO of Loudermilk Companies, is also the Chairman of the Atlanta Police Foundation Executive Committee. [128]

Other board members of the Atlanta Police Foundation are John F. O'Neill III of Cushman & Wakefield Inc. (real estate); Calvin Darden, who is retired from United Parcel Service (UPS); Tye Darland, general counsel for Georgia-Pacific (consumer products and chemicals); Bob Peterson, the Chairman of Carter (real estate); Dave Wilkinson, the President and CEO of the Atlanta Police Foundation; and Christine St. Clare, a retired partner from KPMG LLP (financial services).[129] The Board of Trustees of the Atlanta Police Foundation includes executives from the Federal Reserve Bank of Atlanta, Waffle House, Merrill Lynch, Pierce, Fenner & Smith Inc., GE Energy Connections, Ernst & Young LLP, and Porsche Cars North America.[130]

The key takeaway is that both the foundation's executive committee and board of trustees comprise people whose primary jobs or experiences are not related to public safety. Despite this lack of expertise, the Atlanta Police Foundation is very well resourced; its net assets for 2018 were reported as $11,931,089, with $7,457,413 from contributions and grants.[131]

Case Study: Amazon Ring

Through its home-security system Ring, Amazon demonstrates how corporate power trumps public power—and safety. Originally launched in 2012 as Doorbot, Ring was acquired by Amazon in 2018 for $1.1 billion and re-launched as a more full-service home security company that sells a number of tools including security cameras, "smart lighting," alarm systems, and the video surveillance doorbell. [132] The Ring doorbell in particular has been linked to a number of racist incidents and exacerbates "broken windows policing" through its Neighbors App, which allows people with the doorbell service to talk to their neighbors about things they see and experience in the neighborhood.[133]

Through Freedom of Information Act (FOIA) requests, we learned that Ring provides local police departments access to the Neighbors app free of charge, and that the partnership is formalized through a Memorandum of Understanding (MOU). The MOU's contain statements similar to the following: "Ring will make the Neighbors app available to City residents free of charge; make the Neighbors app available to [police] Agency free of charge, including ongoing support and training for Agency employees;" and the Agency will "maintain appropriate access controls for Agency personnel to use the Neighbors portal."[134] Neither Ring nor the police department receive any compensation for this.

In December of 2019 alone, nearly 400,000 Ring devices were sold,[135] ranging in price from $34 to $99.[136] In June 2020, 1,300 local law enforcement agencies had a partnership with Amazon Ring,[137] and by late January of 2021, that number had risen to more than 1,700.[138]

Company Case Studies: Motorola Solutions and ShotSpotter

The following case studies about Motorola Solutions and ShotSpotter further illustrate how investors and police departments work hand in hand to institute profitable policing and surveillance technologies.

MOTOROLA SOLUTIONS

Motorola Solutions is a Chicago-based, multibillion-dollar technology manufacturer that markets some of its products to police. Motorola was one of the most dominant[139] cellular tech corporations in the late 1990s, but as a result of the 2008 financial crisis it split[140] into two businesses in 2011. Motorola Mobility handles consumer-facing hardware, such as cell phones

and cable boxes, while Motorola Solutions handles the government and business-facing hardware and software. Motorola Solutions provides a wide range of equipment to police including body cameras[141] and license plate scanners,[142] as well as services, programs, and infrastructure to support policing and commercial communication networks such as CommandCentral Aware.[143] Motorola Solutions was able to raise $1 billion in private equity funding from Silver Lake Management to support the 2011 breakup. Motorola Solutions also received funding from Verizon Communications and ValueAct Capital Management for undisclosed amounts at undisclosed dates.[144]

A Deepening Focus on Law Enforcement Contracts

In recent years, Motorola Solutions has excelled in profitability by pivoting to aggressively investing in security software marketed to law enforcement.[145] Motorola Solutions made almost $4 billion in gross profits in FY2019, up from $3 billion in FY2017. That same year, JP Morgan Chase Bank lent Motorola Solutions $2.2 billion in credit.[146] Motorola Solutions has acquired similar businesses with the goal of creating a fully integrated array of products and services for police, and spends hundreds of millions of dollars annually. Motorola Solutions has acquired companies like Avigilon (closed-circuit television, body cameras, and software) for around $1 billion in 2018, VaaS International Holdings (automated license plate readers) for almost half a billion dollars in 2019, WatchGuard (in-car and body-worn cameras) for $250 million in 2019,[147] Avtech (dispatch systems) for $136 million in 2019, and Airbus DS (command center software for 911) for $237 million in 2018.[148]

Investments by Motorola Solutions

Motorola Solutions is able to dominate the police technology market further through its own venture capital arm, which invests millions of dollars in many technologies that are complementary to what it manufactures. These businesses include ShotSpotter (gunshot detection), Integrian (mobile surveillance cameras for law enforcement vehicles), VidSys (command center software), RapidSOS (emergency response systems), and Neurala (drone software).[149] These investments have been quite lucrative for Motorola Solutions; for example, in 2018, Motorola Solutions sold its shares in ShotSpotter the year after it went public for $14.2 million. According to Crains Chicago Business, Motorola Solutions originally obtained the stock for $500,000 in 2012, and held a 15.6 percent stake in the company.[150]

Cozy Relationships with Police

To complement its operations strategies, Motorola Solutions maintains close relationships with elected officials and police associations, and spends millions on lobbying and donations. In 2015, Motorola Solutions became a prominent supporter of the National Law Enforcement Museum by pledging to donate $15

million.[151] In 2020, the Motorola Solutions Foundation gave over $10 million to various organizations including police trade associations and officer training programs, as well as directly to police departments via police foundations in Phoenix, Los Angeles, San Diego, Chicago, St. Louis, Philadelphia, Seattle, and Washington D.C.[152] Many of the cities that benefit from Motorola Solutions' philanthropy also maintain contracts with the company through their police departments. Motorola has provided radio communications and body camera systems to the Las Vegas Metropolitan Police Department worth at least $45 million since at least 2013.[153] In 2016, the Motorola Solutions Foundation counted the Friends of the Las Vegas Metropolitan Police Department among its beneficiaries.[154] The Foundation has also supported the Chicago Police Memorial Foundation for years,[155] and has held contracts valued at around $100 million with Chicago since 2007, mostly for two-way, camera, and radio systems, including a $52 million contract for "camera infrastructure."[156]

Lobbying Efforts and Contracts

In addition to philanthropy, Motorola Solutions invests heavily in lobbying. It has spent $17.5 million in federal lobbying and around $2.5 million in political contributions since 2011.[157] Often, its philanthropic and lobbying strategies are intertwined: Motorola Solutions Foundation has been a longtime supporter of the Association of Public Safety Communications Officials,[158] which pushed for Congress to set uniform standards for radios used by law enforcement, with active participation from Motorola representatives.[159] Motorola currently maintains many federal contracts valued at over $1 billion with the US Military, Department of Homeland Security, and Department of Justice.[160]

Motorola Solutions has succeeded in being the supplier of choice for other cities as well; New Orleans uses its emergency dispatch communication systems and command center software,[161] and Motorola Solutions instituted the same technology in a pilot program in Dallas called "Starlight," which integrates into the police department's Fusion Center (its intelligence unit).[162]

SHOTSPOTTER

ShotSpotter is a San Francisco Bay Area-based corporation that manufactures gunshot detection technology. ShotSpotter is contracted by local police departments to install audio sensors around an area to be able to identify when a gunshot occurs and triangulate the location.[163] Despite concerns over false positives[164] and a lack of noticeable effectiveness[165] that have led cities to cancel contracts, ShotSpotter continues to gain new contracts and generate a profit for shareholders. ShotSpotter nearly doubled its revenue from 2017 ($24 million) to 2020 ($42 million).[166] In 2018, ShotSpotter stepped up its predictive policing capabilities by acquiring crime forecasting software company Azavea.[167] CEO Ralph Clark told analysts in 2020 that ShotSpotter planned to open an office in D.C. to be "closer to national law enforcement opinion leaders and decision makers," and to lobby Congress.[168]

Through the years, ShotSpotter has received over $100 million in venture capital funding from Lauder Partners, Shatas Partners, City Light Capital, Claremont Creek Ventures, Levensohn Venture Partners, Labrador Ventures, the Westly Group, Norwest Venture Partners, Broidy Capital, Band of Angels, the Golden Hixon Fund, Motorola Solutions Venture Capital, ORIX Ventures, Dolby Family Ventures, the Global Business Funding Group, and Madison Bay Capital Partners. Notably, as mentioned in the previous case study, Motorola Solutions Venture Capital owned a 15.6 percent stake in ShotSpotter before selling its shares in 2018. Motorola Solutions bought shares for $500,000 in 2012 and sold them for $14.2 million in 2018, taking in a profit of $13.7 million.[169] In 2012, Lauder Partners held a 37.4 percent stake, and Claremont Creek held an 11.3 percent stake.[170] Lauder Partners also invests in database software corporation Palantir.[171]

Lobbying and Relationship to Public Officials

ShotSpotter is known for its aggressive lobbying practices,[172] on which it spends hundreds of thousands of dollars each year.[173] From 2006 to 2013,[174] it retained the Ferguson Group, which was awarded $7 million in federal funding to secure ShotSpotter's presence in 90 cities across the country.[175] In 2019, ShotSpotter was found to be in violation of Oakland lobbying laws for failing to register as a lobbyist despite appealing to City Council members who were considering ending its contract.[176] ShotSpotter advocated not just for Oakland to keep the contract, but to expand it as well.

ShotSpotter has a "revolving door" with public officials.[177] Former Senior Vice President of Public Safety at ShotSpotter David Chipman is also a former senior official at the Bureau of Alcohol, Tobacco,

Firearms and Explosives; former New York Police Department commissioner William J. Bratton served as a board member of ShotSpotter; and ShotSpotter Sales Director Ron Teachman was formerly Chief of Police in New Bedford, Massachusetts and South Bend, Indiana, where his department secured contracts with ShotSpotter during his tenure.[178]

Accuracy Concerns and Failed Contracts

ShotSpotter has struggled to pinpoint gunshots accurately. A 2013 investigation showed that 75 percent of the shots reported by ShotSpotter were false positives.[179] In 2017, Fall River, Massachusetts reported ShotSpotter had a 41 percent error rate, which wasted staff time and led the Fall River Police Department to cancel their contract worth $90,000 annually.[180] In 2019, Durham, North Carolina's City Council voted down a contract with ShotSpotter over efficacy concerns,[181] three years after a neighboring police department decided not to renew their $160,000 annual contract with ShotSpotter for the same reasons.

ShotSpotter's Current Contracts

ShotSpotter still holds lucrative contracts across the country. We identified six contracts worth a total of $75 million, but as of this writing, the company listed 109 contracts with municipalities on its website.[182] (See table below). Federally, ShotSpotter holds nearly $850,000 in federal contracts with the Secret Service and the Department of Justice.[183]

Examples of ShotSpotter Contracts in the U.S. (not comprehensive)

Municipality	Contract Term	Contract Amount
Chicago[184]	2018-2021	$33 million
Miami-Dade County[185]	unknown	$5.7 million
San Diego[186]	unknown	$1 million
New York City[187]	2016-2021	$28 million
West Palm Beach[188]	2019-2022	$1.2 million
Puerto Rico[189]	2020-2023	$4.3 million
Totals:	**2016-2023**	**$75 million**

Section 4.

The Push Back: Wins in Legislation, Organizing, and Awareness

The growth of the technology industry as a whole—and the markets for individual pieces of technology—can feel massive and overwhelming, especially given the speed of growth and the profits that continue to support it. However, organizers, workers, advocates, scholars, and many others in between recognize the dangers of tech industry expansion and are actively pushing back.

Ending the Targeted Surveillance of Marginalized Communities

Stopping the Countering Violent Extremism (CVE) Program

One method of surveilling marginalized populations is through the federal counter-terrorism program called Countering Violent Extremism (CVE). Started in 2011 by the FBI, DHS, and DOJ, CVE programs have primarily targeted Muslim youth within the US. In some states, like Illinois and Massachusetts, these programs have also been referred to as Targeted Violence Prevention Programs (TVPPs), but serve the same purpose as CVE programs.[190] Social scientists researching the efficacy of CVE programs have noted that there are no reliable indicators, risk factors, or warning signs that can predict whether an individual will be radicalized and/or engage in terrorism.[191] Instead, the network of surveillance of primarily Muslim youth criminalizes their free speech activity, religious practices, and political activism. This surveillance has recently expanded in scope to target Black Lives Matter activists who have been dubbed "Black Identity Extremists" by the FBI.[192]

#StopCVE is a coalition of organizations and individuals with chapters around the country working to expose and push back against CVE policies.[193] The Chicago chapter has utilized FOIA requests to compile information on the forms CVE programs can take, what actors are involved in this type of surveillance (e.g., mental health professionals, community members, and more), how to spot CVE and TVPP programs and resist them, and policy recommendations for local and state leaders to take action and cease these surveillance operations.[194] Advocacy efforts made by the Muslim Justice League in Boston, an affiliate of #StopCVE, include legal aid resources for individuals targeted by CVE and toolkits for residents to pressure their city council leaders to end CVE operations in their communities.[195]

NYC and Chicago: Ending Gang Databases

As mentioned in section two, gang policing and the compilation of gang databases are one form of law enforcement surveillance that primarily targets Black and Latinx youth, increasing their chances of being funneled into the school-to-prison pipeline or targeted by ICE for deportation. Gang policing and gang databases are particularly dangerous for civil liberties because criteria for inclusion in these databases is highly subjective (e.g., based on friendships, clothing color, tattoos, or accessories worn by an individual) and individuals added to these databases are often unaware of their status. Even if they do find out, it can be nearly impossible to be taken out of the system.[196] Admission to the gang database does not require a criminal conviction, and often leads to hyper-policing of not only that specific individual but also their family and community.[197] Though data about exactly how many people have been entered into these gang databases is not available, reports from both Chicago and New York City estimate that around 20,000 people have been added to the databases each year within the past 17 years,[198] and that over 80 percent of these individuals are not white.[199]

In Chicago, a coalition of racial justice organizers, immigrant rights advocates, and members of academia formed the Erase the Database campaign to expose the behind-the-scenes functions of gang policing, to show its role in violating notions of Chicago as a Sanctuary City that protects immigrants, and to eliminate this method of policing. Through FOIA

requests and advocacy efforts, organizers working on the Erase the Database campaign were able to highlight the dangerous effects of Chicago's gang database, called the Regional Gang Intelligence Database (RGID).[200] By early 2019, the RGID was decommissioned and taken offline to be stored on encrypted hard drives within a vault created by the Cook County Sheriff's Office (CSSO). However, the Erase the Database campaign still had concerns about ensuring the abolition of this database in a responsible, publicly accountable, and permanent manner.[201] The campaign called on county leaders to make this effort, resulting in the enactment of an ordinance requiring the permanent destruction of RGID files and the prohibition of sharing gang designation information in the future, as well as requiring public hearings about the gang database and its impacts on the community.[202]

In New York City, gang policing tactics have largely been developed in secret, and efforts to eradicate the gang database there have not yet succeeded, though they have been successful in raising awareness around its impact. Academics have engaged in surveys of defense attorneys and residents of the city to highlight and uplift the voices of those directly impacted by gang policing tactics.[203] Experts have recommended investigating and auditing current gang policing practices, abolishing the NYPD's gang unit and any kind of gang database, discontinuing policing methods such as precision policing, and ending digital and social media surveillance.[204]

The Fight Against ICE and Immigrant Surveillance

Mijente

Through their #NoTechForICE campaign, the Latinx and Chicanx organizing and advocacy organization Mijente has become a leader in exposing surveillance technology use; the tech companies behind these surveillance tools; and the role of law enforcement surveillance in policing, detaining, and deporting members of immigrant communities.[205] In their 2018 report, Who's Behind ICE?, Mijente and its partners were able to reveal the role of companies like Palantir and Amazon Web Services in building the databases, computer programs, cloud-based storage systems, and other surveillance technologies used to monitor immigrant communities and communities of color for law enforcement targeting.[206] The lack of oversight and regulation leading to the unprecedented scale of mass surveillance for deportation is a major concern, and could render Sanctuary city and state-level protection policies obsolete.[207] Using its extensive research into the role of tech companies in fueling ICE operations, Mijente has created popular education materials to boost community awareness and organizing to push back against the unchecked surveillance power of the US immigration enforcement system, including comic books, workshop facilitation guides, and digital advocacy actions.

Just Futures Law

A partner organization of Mijente, Just Futures Law, has also created a toolkit that enables advocates and organizers to analyze policy and lobby their elected officials to regulate and oversee surveillance technology acquisition and use in their communities.[208] The toolkit gives a step-by-step process for challenging surveillance technology use by doing research, collecting evidence, and considering a range of policy solutions that already exist to formulate campaign demands and organizing efforts.[209] Just Futures Law also brings lawsuits against ICE and other government agencies to sue on behalf of immigrant activists who have been systematically targeted, surveilled, detained, and deported with the help of surveillance technology tools.[210] The organization has also created educational materials to inform communities of the ways government and companies

are using the current COVID-19 health crisis to expand surveillance efforts, and the dangers involved with leaving this expansion unchecked.[211]

Community Control of Police Surveillance, Oversight, and Bans

ACLU and the Community Control Over Police Surveillance (CCOPS) Model

In the absence of precedential legislation around surveillance technology use by law enforcement, the American Civil Liberties Union (ACLU) created a model legislation template for cities to use in their own efforts to push for transparency and oversight. The Community Control of Police Surveillance (CCOPS) model has been adopted by the city of Oakland and their Privacy Advisory Commission (PAC) in the form of their Surveillance and Community Safety Ordinance,[212] and serves as the basis for New York City's current proposed Public Oversight of Surveillance Technology (POST) Act.[213] Overall, 12 cities across the US have passed legislation based on the CCOPS model, with over a dozen other cities currently considering adopting this legislation.[214]

Oakland: The Domain Awareness Center (DAC) and the Privacy Advisory Commission (PAC)

A common consensus by experts in the field is that advocacy, organizing, and legislative pushback against rapidly growing surveillance technology is best exemplified by the work done in Oakland, California. In 2013, the city of Oakland began planning a massive network of citywide surveillance tools aimed at reducing or solving crime.[215] The multimillion-dollar proposal included surveillance cameras, gunshot detection, and automated license plate readers (ALPRs), all linked back to a central hub called the Domain Awareness Center (DAC).[216] Activists were concerned about the possibility of this vast network being abused, and were proven right in their fears after leaked emails revealed that the Oakland Police Department had already been using some of the technology to monitor protesters engaged in activity protected by the First Amendment.[217]

As the city planned its DAC project, a new coalition of community members called the Oakland Privacy Working Group formed to push back against the proposed surveillance expansion.[218] The group brought together local organizations and citizens to spread awareness about potential civil liberties violations and to lobby city officials and explain the community's concerns, while also flooding City Council chambers to demand public input on the DAC project and on law enforcement's role in surveillance of the community.[219] The Oakland Privacy Working Group gained victory when the City Council, in a tied 2014 vote ultimately decided by the Mayor, agreed to confine the DAC's surveillance capabilities to the Port of Oakland and to prohibit the use of facial recognition and ALPRs, as well as eliminating retention of any data.[220] Members of the working group were given the task of drafting a privacy policy to govern what remained of the DAC—a group that became what is now known as the Oakland Privacy Advisory Commission (PAC).[221] The limits placed on the DAC project led to its eventual defunding, and its remaining equipment is no longer in use by the city. [222]

The Oakland PAC, born out of the struggle against the DAC, has now become the leading example of what a successful surveillance oversight body in the US can look like. This local oversight body can advise City Council on best practices around surveillance technology, such as local-level facial recognition bans, as well as educate and protect citizens' privacy rights in the absence of state or federal-level guidance and oversight.

According to the Commission's Chair, Brian Hofer, there are now several ordinances that regulate surveillance equipment acquisition and use, which are based on the ACLU's Community Control of Police Surveillance model policy.[223] With these ordinances, law enforcement agencies looking to adopt surveillance technology must first get approval from the Commission. Police departments must perform an impact analysis (e.g., address the potential threat to civil liberties) and create a draft of the policy surrounding the use of this new technology to mitigate negative impacts. The adoption process also allows for the public to be involved in the decision making, as Commission meetings are open to the public. Members of the Commission are subject-matter experts who, as Chair Brian Hofer said in an interview,

"stay vigilant, train staff on what concerns are, and work with staff to write use policies."[224]

The Commission also has the right to deny an entire technology, such as facial recognition, outright.[225] Brian Hofer also explained in an interview that to combat criticisms of legislation being too slow or too narrow to keep up with evolving technology, the surveillance ordinances created by the Commission have been written in a broad and future-proof manner that captures the dynamic nature of surveillance technology creation and acquisition, and also includes provisions that exclude relatively benign surveillance technology, such as copy machines that require fingerprint sign-in.[226] The broad definitions that require technology to be evaluated and approved by the Commission before being used aim to mitigate the expansive privacy concerns of technologies found in Smart Cities initiatives and in the field of biometrics.

NYC: The Surveillance Technology Oversight Project (STOP)

Similar to groups in Oakland, California, advocate groups in New York City have organized around the adoption of a surveillance technology ordinance based on the ACLU CCOPS model legislation, exemplified by Public Oversight of Surveillance Technology (POST) legislation passed in July 2020.[227] One prominent group is the Surveillance Technology Oversight Project (STOP), which plays myriad roles in this field—STOP members litigate on behalf of victims of biased surveillance practices (e.g., Muslim individuals targeted by counter-terrorism surveillance), craft and testify on behalf of model legislation like the POST Act, harness the media to amplify advocacy efforts and reach wide audiences, and empower communities targeted by surveillance to understand their rights and ways they can engage in resisting discriminatory surveillance practices.[228]

The passage of the POST Act is a major focus of STOP and would be a major win.[229] Since the NYPD is the country's largest police force with the largest budget, the passage of the POST Act would have major implications for exposing the depth and scope of surveillance technology it uses and its connection to other agencies such as the FBI and ICE.[230] Extensive research and FOIA requests have shown that the NYPD uses a collection of surveillance tools—like cameras, license plate readers, gunshot detection microphones, and unmarked x-ray vans to scan cars and buildings—that are linked back to a Microsoft-supported platform called the Domain Awareness System.[231] The ultimate goal of the POST Act is to increase transparency around what types of surveillance technologies are used in NYC and how they are used, especially when it comes to the disproportionate impacts they have on marginalized communities, and to provide ways to curb abusive surveillance tactics.[232]

Facial Recognition: Bans Across the US

While an increasing number of surveillance technologies are being critiqued and delegitimized by activists and policymakers alike, facial recognition technology bans have gained the most traction in the advocacy space. Though a focus strictly on facial recognition can be limiting, it also presents opportunities to increase awareness and advocacy around other emerging surveillance technology. This section highlights some of the legislation, organizing, and advocacy efforts targeted at limiting or ending law enforcement use of facial recognition technology, law enforcement partnerships with technology companies that often go unchecked, and other surveillance tools and programs law enforcement uses.

Criticisms regarding the privacy violations of facial recognition technology have spurred this advocacy work, as well as the fact that law enforcement use of facial recognition is often biased and inaccurate, therefore leading to exacerbated racial disparities in its use for criminal investigations.[233] In the absence of state and federal-level guidance, some cities have proactively taken steps to protect their citizens from increased surveillance within city limits. However, despite privacy concerns, the global market for facial recognition technology is expected to grow to $12 billion by 2027.[234]

City councils taking the initiative to ban facial recognition technology (and potentially other invasive surveillance technologies), rather than waiting for civil rights violation lawsuits or grassroots advocacy/protest demands, demonstrate an important proactive method for addressing privacy safety and taking swift action while awaiting similar oversight policies

on the state or federal level. Additionally, the effort to ban facial recognition is not one made only by local city council members or a select few state senators. The nonprofit digital rights advocacy group Fight for the Future also works to educate people across the US on their privacy rights and to campaign against the unchecked and growing use of facial recognition surveillance around the country.[235] In partnership with Students for Sensible Drug Policy, Fight for the Future has campaigned and organized with university students, staff, and faculty to empower them to demand their campuses cease the use of facial recognition technology.[236] Their campaign homepage provides a list of universities that have banned the use of facial recognition technology, as well as those who have not yet done so and ways concerned community members can take action to ask university officials to consider enacting a ban. This homepage also includes a toolkit for students to introduce resolutions to their student government body and lobby their administrators to ban facial recognition.[237]

Examples of Local Facial Recognition Technology Restrictions

City	Details
San Francisco, CA	The San Francisco Board of Supervisors voted to ban the use of facial recognition technology in May 2019, becoming the first major American city to implement an outright ban on this type of surveillance.[238] The ban prohibits the use of facial recognition by city agencies, bans the use of information collected from facial recognition technology in other locations, and is part of a larger legislative effort to establish policies for use and oversight of surveillance tools.
Oakland, CA	In July 2019, Oakland became the second California city to ban local government use of facial recognition technology by amending its preexisting Surveillance and Community Safety Ordinance.[239] The original version of this ordinance required approval from the Chair of Oakland's Privacy Advisory Commission before any city agency could seek, solicit, or receive funds to acquire surveillance tools.[240] Rather than requiring approval before adopting facial recognition technology, Oakland City Council voted unanimously to ban the technology outright, citing concerns about its inaccuracy, lack of established ethical standards, invasive nature, and potential for government abuse.[241]
Berkeley, CA	In October 2019, an ordinance to ban the use of facial recognition within the city, introduced by Berkeley councilmember Kate Harrison, was unanimously voted into adoption.[242] With an abundance of support from the community, councilmembers cited concerns around the dragnet nature of facial recognition surveillance and its potential to violate Fourth Amendment rights to protection from unlawful search and seizure.[243]
Portland, OR	In late 2020, Portland passed one of the broadest facial recognition bans in the country, banning its use by all city departments including local police, and banning its use among businesses like stores, restaurants, and hotels.[244]
Somerville, MA	Across the country, the ACLU of Massachusetts has been campaigning to enact a statewide ban on facial recognition technology.[245] While not yet passed, cities throughout the Commonwealth have taken action to ban this technology on the local level, similarly to California cities. In mid-2019, Somerville became the second city in the US to ban the use of facial recognition outright.[246]

City	Details
Brookline, MA	Brookline city officials followed Somerville's lead and banned facial recognition technology in December 2019.[247]
Cambridge, MA	Cambridge voted in early 2020 to amend its previous ordinance allowing facial recognition use with prior approval to instead align with other cities in banning its use outright.[248]
Northampton, MA	Outside the Boston metropolitan area, the City Council in Northampton agreed that the technology was outpacing regulation and also voted unanimously to ban the use of facial recognition surveillance outright.[249]
Michigan	Despite the overall lack of state-level legislation on facial recognition technology regulations or bans, Michigan provides one example of an effort to pioneer this move. In July 2019, Michigan lawmakers introduced two bills—one to place a five-year moratorium on the use of facial recognition technology, and the other to completely ban it.[250] As of December 2019, the Michigan state Senate agreed to advance the bill banning facial recognition, co-sponsored by Democratic Senator Stephanie Chang and Republican Senator Peter Lucido.[251] Senator Lucido justified the bill's necessity due to rapidly advancing technology that can be used to search people without a warrant, something with which he and critics said that state laws cannot catch up.[252] The bill now awaits House review, with an added exception that will allow for the use of facial recognition technology in the case of emergency with immediate risk of harm to a person.[253]
California, Oregon, New Hampshire state-levels	While not comprehensive facial recognition bans, some states, such as California, Oregon, and New Hampshire, have passed laws expressly prohibiting facial recognition use on police body cameras.[254]

Illinois: Biometric Information Privacy Act (BIPA)

The Illinois Biometric Privacy Act (BIPA) is one of the most comprehensive state biometric privacy laws, requiring written consent before a company (including social media companies like Facebook and Google) can collect someone's fingerprints, retina/iris scans, voiceprint, face geometry, or other forms of biometric information.[255] The Act also regulates the safeguarding, handling, storage, retention, and destruction of the biometric identifiers and information it collects, and does not allow this information to be sold or traded.[256]

First introduced by Illinois Senator Terry Link in 2008, the BIPA was rationalized as a form of protection.[257] Because of the unique qualities of one's biological features, if a person's biometric identity is compromised they will have no recourse from identity theft, especially given ties between this biometric information and financial and personal information.[258] When individuals' biometric information is collected, stored, and used without their consent, they can sue the company collecting this information; when companies collect this information en masse, such as through Facebook's facial recognition capability with posted photographs, class-action lawsuits can be brought against the company.[259] Though the original BIPA sponsor, Senator Link, attempted to amend the BIPA to exclude photographic facial recognition on social media from being grounds for a privacy infringement, US Courts ultimately sided with plaintiffs, concluding that "the development of face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests."[260]

Recently, facial recognition surveillance technology company Clearview AI has faced its own onslaught of lawsuits that claim the company's scraping of more than three billion photos from social media sites to train its facial recognition algorithm violates the BIPA.[261] As a result, Clearview AI has announced it will cancel accounts of every private business not associated with law enforcement or another federal, state, or local government entity.[262] While this provides protection from private businesses collecting and using biometric information for profit purposes, the added caveat that allows law enforcement to use Clearview AI's technology is a continued concern for privacy and civil liberties. Though data has revealed that private businesses had been using Clearview AI to search photographs—including loss prevention companies, retail giants like Macy's and Amazon, financial institutions such as Bank of America, and Major League Baseball teams—the biggest consumers of Clearview AI's product are law enforcement agencies, a customer base that Clearview AI's own CEO has repeatedly stated as the intended market.[263] In the midst of the COVID-19 pandemic, Clearview AI has also begun soliciting itself as a partner with law enforcement agencies seeking to conduct contact tracing of individuals infected with the virus, raising concerns over privacy and civil liberty protections.[264] Ultimately, this demonstrates that though the BIPA is a useful tool for protecting against surveillance done by private companies, it does not yet do enough to protect civilians from law enforcement's use of biometric surveillance.

MuckRock: Building a Database of Facial Recognition and Algorithm Use

Advocates working to heighten transparency around surveillance technology capabilities and the kinds of technology being used by law enforcement often rely on FOIA requests to obtain information. The non-profit government accountability organization MuckRock has utilized FOIA requests and provides educational material for others to learn the process. Its website hosts both a facial recognition database[265] and an algorithm database[266] that share information on what types of technology police departments are using, where else the technology is used, and model policies that can guide regulations of algorithm use by police departments. In a 2020 interview, Projects Editor and Senior Reporter at MuckRock Beryl Lipton stated that the databases are a way to consolidate efforts to increase understanding of the ways surveillance technology is acquired and utilized, as well as a way to highlight and establish a pattern of the different areas where algorithms and artificial intelligence (AI) are being used.[267] With the FOIA request database, which houses material received from these requests as well as comments on why some requests have not been fulfilled or have been only partially fulfilled, MuckRock workers wanted an easy way for advocates and organizers to engage with the problem of expanding surveillance technology that they might not otherwise get involved in due to the difficult and often stressful task of asking police departments to share information.[268] A collaborative effort to file FOIA requests and upload results to the database means that organizers throughout the country can save time by using what already exists in the database to help their campaigns. Lipton does note, however, that the databases are only helpful if they are maintained, so organizations that have already been using FOIA and public records requests to glean information about surveillance technology should consider participating in their maintenance.

Community Organizing Against Data Fusion Centers and Surveillance Networks

Detroit: Stopping Project Green Light

In 2016, the City of Detroit launched a partnership with the technology company DataWorks Plus to install real-time video surveillance systems with facial recognition capability throughout the city. The justification for this surveillance network was to deter crime, but the presence of cameras tracking people's faces in places like reproductive and health care centers[269] raised privacy concerns. As of 2019, there were over 500 properties throughout Detroit participating in this network—called Project Green Light—including churches, apartments, businesses, and schools.[270] The city planned to spend $4 million by July 2019 to expand the project through increased real-time crime centers to monitor video footage.[271] While community surveys have shown that some Detroit residents do not mind the presence of these

cameras, many residents and privacy advocates have expressed concern over the way the footage is stored and used.[272] The major concern from policy analysts has been the equation of surveillance with public safety that fuels the desire to expand the project—these justifications are often used for things like predictive policing that exacerbate racial disparities, leading to an overrepresentation of marginalized people tied up in the criminal justice system.[273] Also of great concern is the lack of oversight and regulation around use policies for the program. For example, though the Detroit Police Department (DPD) does not explicitly allow the use of Project Green Light footage for immigration enforcement, their partnership with DHS does allow this.[274] There is also a lack of regulation for the uses of facial recognition, meaning that DPD can use their network of cameras to monitor First Amendment-protected activity as well as assist non-law enforcement entities (like banks) in tracking down individuals from those businesses' incident reports.[275] Additionally, Project Green Light does not have a transparency mechanism in place, meaning that the public may or may not be notified about their presence in the facial recognition database and any possible security breaches of that database.[276]

Despite the City Council's eventual agreement to expand the program,[277] grassroots organizations pushed back and drew attention to criticisms of the surveillance program, most notably through research and analysis done by the Detroit Community Technology Project.[278] Through its Green Light Black Futures campaign, the Detroit chapter of Black Youth Project 100 (BYP100) called for divestment from surveillance and for transparency around how the already-collected footage is used.[279] BYP 100 also coordinated a letter-writing campaign that ultimately succeeded in urging City Council not to make participation in Project Green Light mandatory for certain businesses like restaurants and bars.[280]

Los Angeles: The Stop LAPD Spying Coalition

The Stop LAPD Spying Coalition has successfully engaged in organizing to resist surveillance policing. The Coalition has worked to resist and dismantle government-sanctioned surveillance efforts, utilizing persistent and extensive public records requests, public education efforts, lawsuits, and support for targets of surveillance to boost their cause and achieve success.[281] One major victory came in December 2019, when the Coalition was able to reveal that the Los Angeles Police Department (LAPD) was engaging in racially biased surveillance[282] and predictive policing through the Los Angeles Strategic Extraction and Restoration (LASER) program and the Chronic Offender program—programs that also lacked official oversight.[283] The efforts to expose and end these programs came through the Coalition, whose co-director noted the absence of the Los Angeles Police Commission, which is a civilian oversight body meant to monitor such police activity.[284]

In addition to physically showing up to City Council proceedings to advocate for the community, the Coalition has an extensive repository of resources on law enforcement surveillance, including reports on body cameras, drone surveillance, data fusion centers, and law enforcement surveillance during the current COVID-19 pandemic.[285] The Coalition has also created a series of video webinars on the ways law enforcement surveillance targets different marginalized communities (e.g., youth, LGBTQIA individuals, and so on) to highlight the work and voices of leaders within this advocacy movement.[286]

Recommendations and Conclusion

As pressure to defund the police grows louder, and as local, state, and federal governments make the unfortunate return to austerity budget measures in the face of the ongoing COVID-19 recession, those in power will adapt and continue to find ways to criminalize communities as a way to bolster private profits. It's clear that this is not in response to community demands but instead is a choice to maintain corporate greed.

As long as community safety is defined as the presence of law enforcement instead of as a system to ensure strategic and targeted community investments, surveillance technology will continue to be prevalent. After defining the issue, naming who is profiting, and providing examples of where the push back is working, here we lay out the following **five key recommendations:**

1. Defund the police and invest in community safety

Reforms that only moderately regulate police surveillance are not sufficient to make a meaningful impact. In order to see a shift in the abuses of power that take place within the system of policing, there must be a significant shift in the way that money is spent within the system. Increased police presence, whether physical or via surveillance technology, does not address the root cause of violence. Directly investing in communities, after years of divestment, is true public safety.

We stand with public calls to defund the police and create democratically determined investments into community safety. We stand with the public calls to defund the police and, with those reclaimed public dollars, create democratically determined investments into community safety.

2. End police surveillance data collection and sharing practices

In addition to defunding the police, we must defund public and private forms of surveillance. Surveillance technology, such as biometric identification, facial recognition, video surveillance, automated license plate readers, and any other form of surveillance technology used to gather information by police, must end. When used by police, such technologies have been shown to criminalize people, especially Black, Indigenous and other people of color, and do little to meaningfully reduce harm or ensure public safety. This comes at the expense of genuine investments in community safety. Ending data collection and sharing practices by police will move us toward the end of unfair criminalization of people of color.

3. End all federal funding for police surveillance technology

As surveillance technology becomes more prevalent within police departments, there is an increase of federal money going to municipalities. Federal grants, along with asset forfeitures, are the primary ways police departments fund their surveillance technology programs. Community Oriented Police Services (COPS), Justice Assistance Grants from the Department of Justice and Urban Area Security Initiative, and Operation Stone Garden from the Department of Homeland Security are all federal grants that incentivize surveillance technology use at the local level and should be ended immediately. We can blunt the dangerous rise and reach of surveillance technology if we cut off all federal funding streams.

4. End all private funding of police departments

Police are the muscle of racial capitalism and have shown throughout history that they exist to protect property and systems of white supremacy—not people. Private funding provided by corporations and the rich worsen an already violent institution.

Private benefactors, private foundations, police foundations (funded by corporations) and contracts, and revenue and information sharing agreements between surveillance technology companies and police departments should be banned. Such practices increase the size of the surveillance state and lead to less public accountability while ensuring the wealthy control the public agenda around policing and safety.

5. Incentivize Public Accountability and Control of Public Safety

We need independent publicly and democratically controlled bodies to audit, monitor, and report law enforcement surveillance technology usage to the public. One way to have transparent access to police surveillance technology information that hacks the cumbersome FOIA process is to require full reporting of police and incarceration surveillance tools through a publicly controlled body not housed in a police department or police-adjacent agency. Such a body, which would be independent and democratically controlled, could also investigate and report abuse, brutality, and violation of people's rights due surveillance technology. ▪

Demands of accountability from public officials to police and surveillance companies can also occur through suspending and cancelling all police surveillance contracts; investigating tech companies to determine if abuse, brutality or violations of rights occurred due to surveillance tech usage; and investigating and auditing all police surveillance technology contracts for financial wrongdoing and negligence.

The rise and reach of technology in the 21st century have exacerbated policing and the harm and trauma borne from it. In a moment when progressives and leftists are demanding police accountability and that public funds be directed away from this system and toward public safety—and the public good—police departments, and the corporations and institutions that finance them, are doubling down on extraction, exploitation, and violence.

No matter how it's framed, surveillance technology is a threat to the safety and security of all people, but especially to communities of color. All forms of capitalism must go, especially the surveillance capitalism that feeds racial capitalism.

Policing has cost us too much, in lives lost, and in the quality of our lives. And so, we are no longer asking for reform. Until Black and Brown people are safe from state violence and structural racism, we will not stop demanding systems change that can deliver liberation and justice.

1. Vestby, Annette, and Jonas Vestby. "Machine Learning and the Police: Asking the Right Questions." n.d. *Policing: A Journal of Policy and Practice*. Accessed 27 Jan 2020. https://doi.org/10.1093/police/paz035
2. Brayne, Sarah. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82, no. 5 (29 Aug 2017): 977–1008. https://doi.org/10.1177/0003122417725865
3. Segal, Troy. "Big Data." 01 Jan 2021. Investopedia. https://www.investopedia.com/terms/b/big-data.asp
4. Balko, Radley. *Rise of the Warrior Cop: The Militarization of America's Police Forces.* 2013. https://www.publicaffairsbooks.com/titles/radley-balko/rise-of-the-warrior-cop/9781610392129/; Brayne, Sarah. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82, no. 5 (29 Aug 2017): 977–1008. https://doi.org/10.1177/0003122417725865
5. Braga, Anthony and David Weisburd. "The Effects of Focused Deterrence Strategies on Crime: A Systematic Review and Meta-Analysis of the Empirical Evidence." *Journal of Research in Crime and Delinquency* 49, no. 3 (01 Aug 2012): 323–58. https://doi.org/10.1177/0022427811419368; Brayne, Sarah, Alex Rosenblat, and Danah Boyd. "Predictive Policing." Data & Civil Rights Conference. 2015. http://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf
6. Lane, Jeffrey. "The Digital Street: An Ethnographic Study of Networked Street Life in Harlem," *American Behavioral Scientist* 60, no. 1 (01 Jan 2016): 43–58. https://doi.org/10.1177/0002764215601711
7. Borger, Julian. "Insurrection Day: When White Supremacist Terror Came to the US Capitol." *The Guardian*. 09 Jan 2021. https://www.theguardian.com/us-news/2021/jan/09/us-capitol-insurrection-white-supremacist-terror
8. "Stingray Tracking Devices: Who's Got Them?" American Civil Liberties Union. Nov 2018. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them
9. Smith, Stephen W. "Policing Hoover's Ghost: The Privilege for Law Enforcement Techniques." *American Criminal Law Review* 54, no. 233 (2017). https://papers.ssrn.com/abstract=2740075
10. Joh, Elizabeth E. "Policing by Numbers: Big Data and the Fourth Amendment." *Washington Law Review* 89, no. 35 (01 Feb 2014): 34. https://ssrn.com/abstract=2403028
11. Lerman, Amy E. and Vesla M. Weaver. *Arresting Citizenship: The Democratic Consequences of American Crime Control.* The University of Chicago Press. 2014. https://press.uchicago.edu/ucp/books/book/chicago/A/bo18008991.html
12. Brayne, Sarah. "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment." *American Sociological Review* 79, no. 3 (01 Jun 2014): 367–91. https://doi.org/10.1177/0003122414530398
13. "Final Report of the President's Task Force on 21st Century Policing." Office of Community Oriented Policing Services. 2015. https://cops.usdoj.gov/RIC/Publications/cops-p311-pub.pdf
14. Thompson, Taahira. "NYPD's Infamous Stop-and-Frisk Policy Found Unconstitutional." The Leadership Conference Education Fund. 21 Aug 2013. https://civilrights.org/edfund/resource/nypds-infamous-stop-and-frisk-policy-found-unconstitutional/
15. Neoliberalism is an economic and political ideology asserting that there is a "market" for everything. It calls for channeling public services into private hands and disguising this privatization as an innovative solution to some of society's biggest issues.
16. "Bipartisan Support for Justice Reinvestment Legislation." The Pew Charitable Trusts. 04 May 2018. https://www.pewtrusts.org/en/research-and-analysis/fact-sheets/2018/05/bipartisan-support-for-justice-reinvestment-legislation
17. Davie, Fred and Julio Medina. "First Step Act Is Failing Some Who Find Themselves Fearing Reincarceration after Release." *USA Today*. 31 Jan 2020, sec. Opinion. https://www.usatoday.com/story/opinion/policing/2020/01/30/first-step-act-failing-some-who-live-fear-after-release/4558354002/
18. "Street level surveillance: Acoustic Gunshot Detection." Electronic Frontier Foundation. Accessed 03 Feb 2021. https://www.eff.org/pages/gunshot-detection
19. In response to the white supremacist attack on the US Capitol, ACRE co-executive director Saqib Bhatti outlined why we should not use the terms "terrorism" or "domestic terrorism" to refer to this event: https://twitter.com/snbhatti/status/1347603727105089537?s=20; "Suspected & Surveilled: A Report on Countering Violent Extremism in Chicago." #StopCVE Chicago. 2019. http://www.stopcve.com/uploads/1/1/2/4/112447985/cvereport_final_fordigitaluse%5b3%5d_2.pdf; Schoolov, Katie. "As Protests over the Killing of George Floyd Continue, Here's How Police Use Powerful Surveillance Tech to Track Them." *CNBC*. 18 Jun 2020. https://www.cnbc.com/2020/06/18/heres-how-police-use-powerful-surveillance-tech-to-track-protestors.html
20. Moraff, Christopher. "Beware of 'Big Data Hubris' When It Comes to Police Reform." Next City. 07 Mar 2016. https://nextcity.org/daily/entry/big-data-police-reform-police-transparency-sites; Bui, Tiffany. "Would an Updated Early Intervention System Help MPD Avert Excessive Force Incidents?" MinnPost., 26 June 26, 2020. https://www.minnpost.com/metro/2020/06/would-an-updated-early-intervention-system-help-mpd-avert-excessive-force-incidents/; Cahill, Meagan, John S. Hollywood, Dulani Woods, and John Harrison. "Protests and Police Reform: Q&A with RAND Experts." RAND Corporation., 18 June 18, 2020. https://www.rand.org/blog/2020/06/protests-and-police-reform-qampa-with-rand-experts.html
21. Torres, Ella. "What to Know about Police Reforms after George Floyd's Death and Why 'Defunding' Might Be a Solution." *ABC News*. 12 Jun 2020. https://abcnews.go.com/US/police-reforms-george-floyds-death-defunding-solution/story?id=71069779
22. Kerry, Cameron F. "Why Protecting Privacy Is a Losing Game Today—and How to Change the Game." The Brookings Institution. 12 Jul 2018. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/
23. Bowman, Jeremy. "2 Law Enforcement Stocks to Watch Right Now." Nasdaq. 4 Jun 2020. https://www.nasdaq.com/articles/2-law-enforcement-stocks-to-watch-right-now-2020-06-04
24. *Ibid.*
25. "Global Law Enforcement & Police Modernization Market 2020-2025 - ResearchAndMarkets.com." Businesswire. 10 Dec 2019. https://www.businesswire.com/news/home/20191210005687/en/Global-Law-Enforcement-Police-Modernization-Market-2020-2025

26. Jefferson, Brian. "Digitize and Punish: Introduction." University of Minnesota Press. Apr 2020. https://manifold.umn.edu/read/digitize-and-punish/section/5d70850d-46b7-4655-aa8b-3697faed33a9; "Funding Information for Gunfire Reduction Programs." ShotSpotter. 25 July 2018. https://www.shotspotter.com/funding/

27. Jefferson, Brian. "Digitize and Punish: Introduction." University of Minnesota Press. Apr 2020. https://manifold.umn.edu/read/digitize-and-punish/section/5d70850d-46b7-4655-aa8b-3697faed33a9

28. Paglia, John and Maretno A. Harjoto, "The Effects of Private Equity and Venture Capital on Sales and Employment Growth in Small and Medium Sized Businesses." *Journal of Banking and Finance* 47 (5 Jun 2014): 177-197. https://ssrn.com/abstract=2479574; Esqueda, Omar A, Thanh Ngo, and Jurica Susnjara. "The Effect of Government Contracts on Corporate Valuation" *Journal of Banking and Finance* 106 (2019). https://ssrn.com/abstract=3543192

29. Brustein, Joshua. "Head of the Biggest Body Camera Maker Says George Floyd Was a Wake-Up Call." *Bloomberg*. 05 Jun 2020. https://www.bloomberg.com/news/newsletters/2020-06-05/should-police-officers-wear-body-cameras; O'Grady, Patrick. "Taser Stock Hits New High amid Sales, Unrest." *Phoenix Business Journal*. 01 May 2015. https://www.bizjournals.com/phoenix/blog/business/2015/05/taser-stock-hits-new-high-amid-sales-unrest.html

30. Partovi, Hadi. "Axon 2030: Rethinking Law Enforcement." Axon. 24 Jun 2020. https://www.axon.com/news/technology/axon-2030-rethinking-law-enforcement

31. Jefferson, Brian. "Digitize and Punish: Computation and Criminalization." University of Minnesota Press. Apr 2020. https://manifold.umn.edu/read/digitize-and-punish/section/2184e8f0-be95-495e-a98b-392105a1ff3d

32. Schrader, Stuart. "To Protect and Serve Themselves: Police in US Politics since the 1960s." *Duke University Press: Public Culture* 31, no. 3 (01 Sep 2019): 601-623. https://read.dukeupress.edu/public-culture/article-abstract/31/3/601/140085/To-Protect-and-Serve-ThemselvesPolice-in-US?redirectedFrom=fulltext

33. Rosen, Charlotte. "Abolition or Bust: Liberal Police Reform as an Engine of Carceral Violence." The Abusable Past. 25 Jun 2020. https://www.radicalhistoryreview.org/abusablepast/abolition-or-bust-liberal-police-reform-as-an-engine-of-carceral-violence/

34. Jefferson, Brian. "Digitize and Punish: Punishment in the Network Form." University of Minnesota Press. Apr 2020. https://manifold.umn.edu/read/digitize-and-punish/section/598d0b51-612d-4aea-a56b-fbd86b4c09a8

35. Jefferson, Brian. "Digitize and Punish: Computation and Criminalization." University of Minnesota Press. Apr 2020. https://manifold.umn.edu/read/digitize-and-punish/section/2184e8f0-be95-495e-a98b-392105a1ff3d

36. Guariglia, Matthew and Dave Maass. "How Police Fund Surveillance Technology Is Part of the Problem." Electronic Frontier Foundation. 23 Sept 2020. https://www.eff.org/deeplinks/2020/09/how-police-fund-surveillance-technology-part-problem

37. Jefferson, Brian. "Digitize and Punish: How to Program a Carceral City." University of Minnesota Press. Apr 2020. https://manifold.umn.edu/read/digitize-and-punish/section/9b195bdd-9dc5-4b39-ac26-9fc3820e71e5

38. *Ibid.*; "Silicon Valley Innovation ProgramVIP." Department of Homeland Security,. 09 October 9, 2020. https://www.dhs.gov/science-and-technology/svip

39. Mazmanian, Adam. "Funding Dries up for DHS Emerging Tech Investments." FCW. 29 Apr 2019. https://fcw.com/articles/2019/04/29/svip-ota-funding-dries-up.aspx

40. Miller, Ben. "Responder Ventures, Amazon Web Services Create Program to Connect Emergency Responders to Tech." *Government Technology*. 07 Aug 2018. https://www.govtech.com/biz/Responder-Ventures-Amazon-Web-Services-Create-Program-to-Connect-Emergency-Responders-to-Tech.html

41. Laidler, John. "Harvard Professor Says Surveillance Capitalism Is Undermining Democracy." *Harvard Gazette*. 04 Mar 2019, sec. Business & Economy. https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

42. Porter, Jon. "Facebook and LinkedIn Are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech." *The Verge*. 06 Feb 2020. https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube

43. Levinson-Waldman, Rachel and Ángel Díaz. "How to Reform Police Monitoring of Social Media." *Brookings*. 09 Jul 2020, sec. TechStream. https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/

44. Doctorow, Cory. "How to Destroy Surveillance Capitalism." *OneZero*. 26 Aug 2020. https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59

45. One example of this is ICE buying utility bill data to find immigrants' addresses. "Who's Behind ICE? The Tech and Data Companies Fueling Deportations." National Immigration Project, National Immigration Project, and Mijente. Oct 2018. https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations_v3-.pdf

46. Coburn, Judith. "The Reach—and Limits—of Surveillance Capitalism." *The Nation*. 27 Aug 2018. https://www.thenation.com/article/archive/the-reach-and-limits-of-surveillance-capitalism/

47. Kelly, Erin. "Law Enforcement in an Unjust Society." Political Theory Workshop, Stanford University School of Humanities & Sciences - Department of Political Science. 02 Jun 2017. https://politicalscience.stanford.edu/events/political-theory-workshop/law-enforcement-unjust-society

48. In 2005, ICE agents posed as Occupational Safety and Health Administration (OSHA) agents during a workplace raid in order to detain immigrants. Bernhardt, Annette et al. *The Gloves-off Economy: Workplace Standards at the Bottom of America's Labor Market.* Labor and Employment Relations Association Series, University of Illinois at Urbana-Champaign. 2008, p. 220.

49. Lemieux, Pierre. "The Underground Economy: Causes, Extent, Approaches." Montreal Economic Institute Research Papers. Nov 2007. https:www.iedm.org/files/cdr_nov07_en.pdf

50. Tyler, Tom. "Police Discretion in the 21st Century Surveillance State." *University of Chicago Legal Forum* (2016): 579–614. https://heinonline.org/HOL/LandingPage?handle=hein.journals/uchclf2016&div=17&id=&page=; Armenta, Amada. "Between Public Service and Social Control: Policing Dilemmas in the Era of Immigration Enforcement." *Social Problems* 63, no. 1 (2016): 111–26. https://www.jstor.org/stable/44014897; Bernhardt, Annette et al. *The Gloves-off Economy: Workplace Standards at the Bottom of America's Labor Market, Labor and Employment Relations Association Series.* University of Illinois at Urbana-Champaign. 2008.

51. Haskins, Caroline. "Scars, Tattoos, And License Plates: This Is What Palantir And The LAPD Know About You." *BuzzFeed News.* 09 Sept 29, 2020. https://www.buzzfeednews.com/article/carolinehaskins1/training-documents-palantir-lapd; Ng, Alfred "Google Is Giving Data to Police Based on Search Keywords, Court Docs Show." *CNET.* 08 Oct 2020. https://www.cnet.com/news/google-is-giving-data-to-police-based-on-search-keywords-court-docs-show/; Guariglia, Matthew and Dave Maass. "How Police Fund Surveillance Technology Is Part of the Problem." Electronic Frontier Foundation. 23 Sept 2020. https://www.eff.org/deeplinks/2020/09/how-police-fund-surveillance-technology-part-problem; Guariglia, Matthew. "Police in Mississippi To Pilot a Program to Live-Stream Amazon Ring Cameras." Mozilla Foundation. 19 Nov 2020. https://foundation.mozilla.org/en/blog/police-mississippi-pilot-program-live-stream-amazon-ring-cameras/

52. *Who's Behind ICE? The Tech and Data Companies Fueling Deportations.* National Immigration Project, Immigrant Defense Project, and Mijente. Oct 2018. https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations_v3-.pdf

53. *Ibid.*

54. Davis-Cohen, Simon. "New Documentary Reveals Silicon Valley's Role in Notorious Bronx Gang Raid," *The Appeal.* 21 May 2020. https://theappeal.org/raided-part-2-documentary-bronx-gang-raid/

55. Beutel, Alejandro J. and Jelena Jankovic. *Strength Through Diversity: Four Cases of Local and State Level Coalition Success.* Institute for Social Policy and Understanding. Jan 2015. https://www.ispu.org/wp-content/uploads/2016/09/Strength-Through-Diversity-Full-Report.pdf?x43338

56. *Suspected & Surveilled: A Report on Countering Violent Extremism in Chicago.* #StopCVE Chicago. 2019. http://www.stopcve.com/uploads/1/1/2/4/112447985/cvereport_final_fordigitaluse%5b3%5d_2.pdf

57. Trujillo, Josmar and Alex S. Vitale. *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing.'* Brooklyn College of the City University of New York Policing & Social Justice Project. 2019. https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf

58. Speri, Alice. "Fear of a Black Homeland: The Strange Tale of the FBI's Fictional 'Black Identity Extremism' Movement." *The Intercept.* 23 Mar 2019. https://theintercept.com/2019/03/23/black-identity-extremist-fbi-domestic-terrorism/

59. *Ibid.*

60. Richardson, Rashida, Jason M Schultz, and Kate Crawford. "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *New York University Law Review* 94 (May 2019): 42. https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf

61. Trujillo, Josmar and Alex S. Vitale. *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing.'* Brooklyn College of the City University of New York Policing & Social Justice Project. 2019. https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf

62. Trujillo, Josmar and Alex S. Vitale. *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing.'* Brooklyn College of the City University of New York Policing & Social Justice Project. 2019. https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf

63. Bohm, Allie and Emma Anderson. "Towns Don't Need Tanks, but They Have Them." ACLU. 2013. https://www.aclu.org/blog/national-security/towns-dont-need-tanks-they-have-them

64. Mizokami, Kyle. "U.S. Lawmakers Want to Curb Transfers of Military Hardware to Police." *Popular Mechanics.* 11 Jun 2020. https://www.popularmechanics.com/military/weapons/a32827563/police-militarization/

65. Powers, Benjamin. "Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You." *Rolling Stone.* 06 January 2017. https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/

66. Vagle, Jeffrey L. "Tightening the OODA Loop: Police Militarization, Race, and Algorithmic Surveillance." *Michigan Journal of Race and Law* 22, no. 4 (2016): 101–37. https://doi.org/10.31228/osf.io/9z65d

67. Crump, Catherine. "Surveillance Policy Making By Procurement." *Washington Law Review* 91 (Dec 2016): 1595. http://lawcat.berkeley.edu/record/1127536

68. *Ibid.*

69. Harris, Mark. "How Peter Thiel's Secretive Data Company Pushed Its Way Into Policing." *Wired.* 09 Aug 2017. https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/

70. *Ibid.*

71. *Ibid.*

72. *Ibid.*

73. Valdovinos, Maria, James Specht, and Jennifer Zeunik. *Community Policing & Unmanned Aircraft Systems (UAS): Guidelines to Enhance Community Trust.* US Department of Justice & Police Foundation Community Oriented Policing Services (COPS). 2016. https://rems.ed.gov/docs/COPS_Community-Policing-UAS.pdf

74. Laperruque, Jake and David Janovsky. "These Police Drones Are Watching You." Project On Government Oversight. 25 Sept 2018. https://www.pogo.org/analysis/2018/09/these-police-drones-are-watching-you/

75. Gettinger, Dan. "Public Safety Drones: An Update." Center for the Study of the Drone at Bard College. May 2018. https://dronecenter.bard.edu/files/2018/05/CSD-Public-Safety-Drones-Update-1.pdf; Crockford, Kade. "Boston Police Bought Three Drones but Didn't Tell Anyone. We Need Accountability for Surveillance Now." American Civil Liberties Union. 27 Sept 2017. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/boston-police-bought-three-drones-didnt-tell

76. Stanley, Jay. "ACLU Lawsuit Over Baltimore Spy Planes Sets Up Historic Surveillance Battle." American Civil Liberties Union. 09 Apr 2020. https://www.aclu.org/news/privacy-technology/aclu-lawsuit-over-baltimore-spy-planes-sets-up-historic-surveillance-battle/

77. "Policing Project to Undertake Independent Audit of Baltimore PD's Aerial Investigation Program." The Policing Project at NYU School of Law. 13 Apr 2020. https://www.policingproject.org/news-main/2020/4/13/policing-project-to-undertake-independent-audit-of-baltimore-pds-aerial-investigation-program

78. German, Michael. "The Militarization of Domestic Surveillance Is Everyone's Problem." Brennan Center for Justice. 18 Dec 2014. https://www.brennancenter.org/our-work/analysis-opinion/militarization-domestic-surveillance-everyones-problem

79. *Ibid.*

80. *Ibid.*

81. *Ibid.*

82. Elkins, Faye. "Where to Find Funding for Equipment, Training, Hiring, and Programs." Community Policing Dispatch, Office of Community Oriented Policing Services (COPS). Feb 2020. https://cops.usdoj.gov/html/dispatch/02-2020/finding_funding.html

83. *Who's Behind ICE: The Tech and Data Companies Fueling Deportations.* National Immigration Project, Immigrant Defense Project, and Mijente. Oct 2018. https://mijente.net/wp-content/uploads/2018/10/WHO'S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf

84. Chopra, Rohit and Julie Margetta Morgan. *Unstacking the Deck: A New Agenda to Tame Corruption in Washington.* Roosevelt Institute. 2018. https://rooseveltinstitute.org/publications/unstacking-the-deck-agenda-tame-corruption-washington/

85. *Ibid.*

86. Naughton, John. "If you think Biden's administration will rein in big tech, think again," *The Guardian.* 2020. https://www.theguardian.com/commentisfree/2020/nov/21/if-you-think-biden-administration-will-rein-in-big-tech-think-again-facebook

87. *Industry Guide: R&D Investment Priorities and Business Opportunities.* Department of Homeland Security Science & Technology. https://www.dhs.gov/sites/default/files/publications/st_industry_guide.pdf

88. "Funding." ShotSpotter. 2021. https://www.shotspotter.com/funding/

89. Dastbaz, Mohammad, Edward Halpin, and Steve Wright. "Emerging Technologies and the Human Rights Challenge of Rapidly Expanding State Surveillance Capacities." *Strategic Intelligence Management,* (2013): 108-118. https://www.sciencedirect.com/science/article/pii/B9780124071919000107

90. Mak, Aaron. "Genetic Genealogy's Less Reliable Cousin." Slate Magazine. 25 Jul 2019. https://slate.com/technology/2019/07/parabon-nanolabs-genetic-genealogy-phenotyping.html

91. *Ibid.*

92. *Ibid.*

93. Winerman, Lea. "What Can We Learn from Our DNA?" *American Psychological Association Monitor on Psychology* 50, no. 3 (Mar 2019): 39. https://www.apa.org/monitor/2019/03/cover-dna

94. Winerman, Lea. "What Can We Learn from Our DNA?" American Psychological Association Monitor on Psychology 50, no. 3 (Mar 2019): 39. https://www.apa.org/monitor/2019/03/cover-dna

95. Kang, Dake. "Chinese 'gait Recognition' Tech IDs People by How They Walk." *Associated Press.* 06 Nov 2018, sec. Beijing. https://apnews.com/article/bf75dd1c26c947b7826d270a16e2658a

96. Gillum, Jack and Jeff Kao. "Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students." *ProPublica.* 25 Jun 2019. https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/

97. Guariglia, Matthew and Cooper Quintin. "Thermal Imaging Cameras Are Still Dangerous Dragnet Surveillance Cameras." Electronic Frontier Foundation. 07 Apr 2020. https://www.eff.org/deeplinks/2020/04/thermal-imaging-cameras-are-still-dangerous-dragnet-surveillance-cameras

98. Monahan, Torin and Neal A. Palmer. "The Emerging Politics of DHS Fusion Centers." *Security Dialogue* 40, no. 6 (11 Dec 2009): 617–36. https://doi.org/10.1177/0967010609350314

99. *Ibid.*

100. *Ibid.*

101. *Ibid.*

102. *Advancing the Homeland Security Information Sharing Environment: A Review of the National Network of Fusion Centers.* House Homeland Security Committee. Nov 2017. https://www.archives.gov/files/committee-on-homeland-security-fusion-center-report-2017.pdf

103. "More About Fusion Centers." American Civil Liberties Union. Accessed 05 Oct 2020. https://www.aclu.org/other/more-about-fusion-centers

104. Price, Michael. "National Security and Local Police." Brennan Center for Justice at New York University School of Law. 2013. https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf

105. Bonsu, Janaé and Andrew Clarno. *Tracked and Targeted: Early Findings on Chicago's Gang Database.* Policing in Chicago Research Group, University of Illinois at Chicago. Feb 2018. http://erasethedatabase.com/wp-content/uploads/2018/02/Tracked-Targeted-0217-r.pdf

106. Price, Michael. "National Security and Local Police." Brennan Center for Justice at New York University School of Law. 2013. https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf

107. Bonsu, Janaé and Andrew Clarno. *Tracked and Targeted: Early Findings on Chicago's Gang Database.* Policing in Chicago Research Group, University of Illinois at Chicago. Feb 2018. http://erasethedatabase.com/wp-content/uploads/2018/02/Tracked-Targeted-0217-r.pdf

108. *Ibid.*

109. Capps, Randy et al. *Revving Up the Deportation Machinery: Enforcement under Trump and the Pushback.* Migration Policy Institute. May 2018. https://www.migrationpolicy.org/research/revving-deportation-machinery-under-trump-and-pushback

110. "Big Data, Migration and Human Mobility." Migration Data Portal. 04 Aug 2020. https://migrationdataportal.org/themes/big-data-migration-and-human-mobility

111. Washington, John. "The Amount of Money Being Made Ripping Migrant Families Apart Is Staggering." *The Nation.* 28 Oct 2019. https://www.thenation.com/article/archive/immigration-ice-family-separation/

112. Fun, McKenzie. "How ICE Picks Its Targets in the Surveillance Age." *New York Times.* 02 Oct 2019. https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html

113. Hussain, Saira. "ICE's Rapid DNA Testing on Migrants at the Border Is Yet Another Iteration of Family Separation." Electronic Frontier Foundation. 02 Aug 2019. https://www.eff.org/deeplinks/2019/08/ices-rapid-dna-testing-migrants-border-yet-another-iteration-family-separation

114. *Deadly Exchange: The Dangerous Consequences of American Law Enforcement Trainings in Israel.* Researching the American-Israeli Alliance and Jewish Voice for Peace. Sept 2018. https://deadlyexchange.org/wp-content/uploads/2019/07/Deadly-Exchange-Report.pdf

115. Stanley, Jay. "A Look at the High-Tech Gadgets Being Marketed to Police." American Civil Liberties Union. 27 Oct 2017. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/look-high-tech-gadgets-being-marketed-police

116. Rausch, Sarah Ludwig. "How Strong Public-Private Partnerships Bolster Security Programs." *Security Magazine.* 09 Sept 2019. https://www.securitymagazine.com/articles/90868-how-strong-public-private-parnertships-bolster-security-programs

117. Sori, Andrea. "Public and private surveillance collaboration efficiently tackles crime." *Axis Communications.* 25 Feb 2019. https://www.axis.com/blog/secure-insights/smart-cities-safety/

118. "Project Green Light." City of Detroit. https://detroitmi.gov/departments/police-department/project-green-light-detroit

119. "Private Security Camera System Incentive Program." Office of Victim Services and Justice Grants, City of D.C. https://ovsjg.dc.gov/service/private-security-camera-system-incentive-program

120. Broadwater, Luke and Kevin Rector. "Report of secret aerial surveillance by Baltimore police prompts questions, outrage." *Baltimore Sun.* 24 Aug 2016. https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-secret-surveillance-20160824-story.html

121. *Ibid.*

122. Rector, Kevin. "Baltimore officials pitched on putting three surveillance planes in the sky at once, covering most of city." *Baltimore Sun.* 19 Sept 2019. https://www.baltimoresun.com/news/crime/bs-md-ci-cr-surveillance-pitch-20190919-dkurugpjdretrjzcevzlc7eabu-story.html

123. "The Atlanta Police Foundation, Atlanta Police Department, General Electric and Georgia Power join to host Inaugural Youth Field Day at the Georgia Dome." Atlanta Police Foundation. https://atlantapolicefoundation.org/atlanta-police-foundation-atlanta-police-department-general-electric-georgia-power-join-host-inaugural-youth-field-day-georgia-dome/

124. Meyer, Claire. "How Atlanta Increased Security by Sharing Surveillance." *Security Magazine.* 01 Sept 2014. https://www.securitymagazine.com/articles/85760-how-atlanta-increased-security-by-sharing-surveillance

125. "Technology & Innovation - Atlanta Police Foundation." Atlanta Police Foundation. https://atlantapolicefoundation.org/programs/technology-innovation/

126. Brett, Jennifer. "'Real-time crimefighting.' Around 11,000 cameras watch over Atlanta." *Atlanta Journal Constitution.* 01 Nov 2019. https://www.ajc.com/news/local/real-time-crimefighting-around-000-cameras-watch-over-atlanta/qlF76c7sgdwBvtla3luX8H/

127. "Loudermilk Family Donates $1 Million to the Atlanta Police Foundation." Atlanta Police Department Public Affairs. 16 Mar 2012. https://www.atlantaga.gov/Home/Components/News/News/1053/672?npage=65&arch=1

128. "Board Members." Atlanta Police Foundation. https://atlantapolicefoundation.org/about-us/board-members/

129. *Ibid.*

130. *Ibid.*

131. "Atlanta Police Foundation 990 form." Atlanta Police Foundation. https://990s.foundationcenter.org/990_pdf_archive/113/113655936/113655936_201812_990.pdf

132. Adams, Susan. "The Exclusive Inside Story of Ring: From 'Shark Tank' Reject to Amazon's Latest Acquisition." *Forbes.* 27 Feb 2018. https://www.forbes.com/sites/susanadams/2018/02/27/amazon-is-buying-ring-the-pioneer-of-the-video-doorbell-for-1-billion/#613e1ba706c2; Montag, Ali. "This $1 billion company was once rejected on 'Shark Tank'—here's how the founder proved everyone wrong." *CNBC Make It.* 30 Nov 2017. https://www.cnbc.com/2017/11/30/shark-tank-reject-doorbot-is-now-billion-dollar-company-ring.html

133. "Neighbors by Ring." Ring. https://store.ring.com/neighbors

134. Cohen, B., Novoa, S., Dietch, D., Gielchinsky, D., Paul, T., & Karukin, M. (2019, June 11). Resolution NO. 2019-2593: A resolution of the Town Commission of the Town of Surfside, Florida, approving a Memorandum of understanding with Ring, LLC relating to the neighbors by Ring application; providing for implementation; and providing for an effective date. Retrieved February 02, 2021, from https://www.townofsurfsidefl.gov/docs/default-source/default-document-library/town-clerk-documents/commission-resolutions/2019-commission-resolutions/resolution-no-2019-2593-ring-llc-memorandum-of-understanding.pdf?sfvrsn=ecad2794_2

135. Molla, Rani. "Amazon Ring sales nearly tripled in December despite hacks." *Vox.* 21 Jan 2020. https://www.vox.com/recode/2020/1/21/21070402/amazon-ring-sales-jumpshot-data

136. Vigderman, Aliza. "Ring Doorbell Camera." *Security.org.* 08 Jul 2020. https://www.security.org/doorbell-camera/ring/

137. Van Ness, Lindsey. "Police Ties to Ring Home Surveillance Come Under Scrutiny." *Stateline (Pew Charitable Trust).* 17 June 2020. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/06/17/police-ties-to-ring-home-surveillance-comes-under-scrutiny

138. Ring's "Active Agency Map" can be accessed at https://www.google.com/maps/d/u/0/viewer?mid=1eYVDPh5itXq5acDT9b0BVeQwmESBa4cB&ll=36.194591702507864%2C-103.969828764492 49&z=4; more information is available on the Ring website at https://support.ring.com/hc/en-us/articles/360035402811-Active-Agency-Map

139. Fishman, Ted. "What Happened to Motorola." *Chicago Magazine*. 25 Aug 2014. https://www.chicagomag.com/Chicago-Magazine/September-2014/What-Happened-to-Motorola/

140. "Motorola to Officially Split into Two Firms on Tuesday." *CNBC*. 03 Jan 2011. https://www.cnbc.com/id/40897532

141. "Body-Worn Cameras." Motorola Solutions. n.d. https://www.motorolasolutions.com/en_xu/video-security-analytics/body-worn-cameras.html

142. "License Plate Recognition (LPR) Camera Systems." Motorola Solutions. https://www.motorolasolutions.com/en_us/video-security-analytics/license-plate-recognition-camera-systems.html

143. "Commandcentral Aware - Situational Awareness." Motorola Solutions. https://www.motorolasolutions.com/en_xu/products/command-center-software/command-and-control/commandcentral-aware.html#taboverview

144. *Motorola Solutions Investors Profile*. Pitchbook. Retrieved 20 Jul 2020 from https://www.pitchbook.com

145. Cahill, Joe. "Motorola Solutions has solved its brig problem." *Crain's Chicago Business*. 09 Nov 2018. https://www.chicagobusiness.com/joe-cahill-business/motorola-solutions-has-solved-its-big-problem

146. *Motorola Solutions Investors Profile*. Pitchbook. Retrieved 20 Jul 2020 from https://www.pitchbook.com

147. "Motorola Solutions Acquires WatchGuard, Inc., Leader in Mobile Video for Public Safety." *Businesswire*. 11 Jul 2019. https://www.businesswire.com/news/home/20190711005632/en/Motorola-Solutions-Acquires-WatchGuard-Leader-Mobile-Video

148. *Motorola Solutions Investors Profile*. Pitchbook. Retrieved 20 Jul 2020 from https://www.pitchbook.com

149. *Ibid.*

150. Pletz, John. "Motorola Solutions cashes in on gunshot-tech company." *Crain's Chicago Business*. 16 Jan 2018. https://www.chicagobusiness.com/article/20180116/BLOGS11/180119929/motorola-solutions-sells-shotspotter-stock

151. Mulvany, Lydia and Greg Gordon. "Motorola spreads its money and influence far and wide." *Anchorage Daily News*. 28 Sept 2016. https://www.adn.com/economy/article/motorola-spreads-its-money-and-influence-far-and-wide/2014/03/25/

152. "Motorola Solutions Foundation." Motorola Solutions. n.d. https://www.motorolasolutions.com/en_us/about/company-overview/corporate-responsibility/motorola-solutions-foundation.html; "2019 United States Grant Recipients." Motorola Solutions Foundation. n.d. https://www.motorolasolutions.com/content/dam/msi/docs/about-us/cr/2019_us_grant_recipients.pdf

153. "Las Vegas Inks Contract with Motorola Solutions for Long-Anticipated Interoperable Police Communications Network." Motorola Solutions. 12 Jun 2013. https://newsroom.motorolasolutions.com/news/las-vegas-inks-contract-with-motorola-solutions-for-long-anticipated-interoperable-police-communications-network.htm; "Master Service Agreement No. 605006 for the Provision of Technology Services and Products." Las Vegas Metropolitan Police Department. n.d. https://www.lvmpd.com/en-us/Finance/FACAgendas/605006%20and%20604632%20Motorola.pdf

154. "2016 United States Grant Recipients." Motorola Solutions Foundation. n.d. https://www.motorolasolutions.com/content/dam/msi/docs/about-us/cr/2016-public-safety-grant-recipients.pdf

155. "Motorola Solutions Foundation Awards Over $9 Million to Nearly 250 Nonprofit Organizations Worldwide." *Businesswire*. 06 Nov 2017. https://www.businesswire.com/news/home/20171106005089/en/Motorola-Solutions-Foundation-Awards-9-Million-250; "2019 United States Grant Recipients." Motorola Solutions Foundation. n.d. https://www.motorolasolutions.com/content/dam/msi/docs/about-us/cr/2019_us_grant_recipients.pdf

156. "Contracts for MOTOROLA SOLUTIONS INC." City of Chicago Procurement Services. Accessed 02 Oct 2010. https://webapps1.chicago.gov/vcsearch/city/vendors/102500169P/contracts

157. This was found by adding the total lobbying dollars from the drop-down menu of different cycles on the right of this webpage on *Open Secrets*: https://www.opensecrets.org/orgs/summary?topnumcycle=2020&toprecipcycle=2020&contribcycle=2020&lobcycle=2020&outspendcycle=2020&id=D000000355

158. Mulvany, Lydia and Greg Gordon. "Motorola spreads its money and influence far and wide." *Anchorage Daily News*. 28 Sept 2016 https://www.adn.com/economy/article/motorola-spreads-its-money-and-influence-far-and-wide/2014/03/25/; "APCO International Awarded Grant From Motorola Solutions Foundation." *PSC Online*. 06 Sept 2018. https://psc.apcointl.org/2018/09/06/apco-international-awarded-grant-from-motorola-solutions-foundation-3/

159. Mulvany, Lydia and Greg Gordon. "Motorola spreads its money and influence far and wide." *Anchorage Daily News*. 28 Sept 2016 https://www.adn.com/economy/article/motorola-spreads-its-money-and-influence-far-and-wide/2014/03/25/

160. "Motorola Solutions Vendor Overview." Tech Inquiry. n.d. https://techinquiry.org/lobbying/vendor/motorola%20solutions%2C%20inc./?useModifiedDate=true

161. "New Orleans Relies on Motorola Solutions, Microsoft Next-Generation Emergency Technology." Motorola Solutions. n.d. https://newsroom.motorolasolutions.com/news/new-orleans-relies-on-motorola-solutions-microsoft-next-generation-emergency-technology.htm; "The City of New Orleans: Creating a Real-Time Crime Center to Proactively Prevent and Respond to Public Safety Issues." Motorola Solutions. n.d. https://www.motorolasolutions.com/en_us/products/command-center-software/nola.html

162. Jaramillo, Cassandra. "DPD Starlight camera program aims to monitor activity at crime-ridden convenience stores." *Dallas Morning News*. 04 Nov 2019. https://www.dallasnews.com/news/crime/2019/11/04/dpd-starlight-camera-program-aims-to-monitor-activity-at-crime-ridden-convenience-stores/

163. Ramprasad, Swathi. "A tale of two cities: Lessons for Durham about ShotSpotter." *9th Street Journal*. 13 Nov 2019. https://9thstreetjournal.org/2019/11/13/a-tale-of-two-cities-lessons-for-durham-about-shotspotter/

164. Fraga, Brian. "After Too Many Shots Missed, Fall River, Mass., Ends Deal with ShotSpotter." *Government Technology*. 23 Apr 2018. https://www.govtech.com/public-safety/After-Too-Many-Shots-Missed-Fall-River-Mass-Ends-Deal-with-ShotSpotter.html

165. Wootson, Cleve. "Charlotte ends contract with ShotSpotter gunshot detection system." *Charlotte Observer*. 10 Feb 2016. https://www.charlotteobserver.com/news/local/crime/article59685506.html

166. *ShotSpotter Investors Profile*. Pitchbook. Retrieved 20 Jul 2020 from https://www.pitchbook.com

167. "ShotSpotter announces acquisition of Hunchlab to springboard into AI-driven analysis and predictive policing." ShotSpotter Press release. 03 Oct 2018. https://www.shotspotter.com/press-releases/shotspotter-announces-acquisition-of-hunchlab-to-springboard-into-ai-driven-analysis-and-predictive-policing/

168. Calvey, Mark. "East Bay tech company's stock jumps on earnings as it plans D.C. office." San Francisco Business Times. 19 Feb 2020. https://www.bizjournals.com/sanfrancisco/news/2020/02/19/east-bay-tech-company-s-stock-jumps-on-earnings-as.html

169. Pletz, John. "Motorola Solutions cashes in on gunshot-tech company." *Crain's Chicago Business*. 16 Jan 2018. https://www.chicagobusiness.com/article/20180116/BLOGS11/180119929/motorola-solutions-sells-shotspotter-stock

170. *ShotSpotter Investors Profile*. Pitchbook. Retrieved 20 Jul 2020 from https://www.pitchbook.com

171. "Current portfolio companies (still private)." Lauder Partners. 20 Jun 2020. http://www.lauderpartners.com/investments/index.html

172. Fang, Lee. "Deployment of controversial urban sensor system aided by aggressive lobbying." *The Intercept*. 26 Mar 2015. https://theintercept.com/2015/03/26/rapid-deployment-shotspotter-controversial-urban-microphone-system-aided-aggressive-lobbying/

173. "Client Profile: ShotSpotter Inc." Center for Responsive Politics, OpenSecrets.org. Accessed 20 Jun 2020. https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2020&id=D000056684

174. *Ibid.*

175. Fang, Lee. "Deployment of controversial urban sensor system aided by aggressive lobbying." *The Intercept*. 26 Mar 2015. https://theintercept.com/2015/03/26/rapid-deployment-shotspotter-controversial-urban-microphone-system-aided-aggressive-lobbying/

176. "City of Oakland Public Ethics Commission Regular Meeting Agenda." City of Oakland Public Ethics Commission. 02 Dec 2019. https://oakland.granicus.com/DocumentViewer.php?file=oakland_d288a02c83e28440e6b3d03c4567ce30.pdf&view=1; BondGraham, Darwin. "ShotSpotter Lobbied Oakland Officials In Apparent Violation of Law." *East Bay Express*. 29 Apr 2014. https://www.eastbayexpress.com/oakland/shotspotter-lobbied-oakland-officials-in-apparent-violation-of-law/Content?oid=3907581

177. Fang, Lee. "Deployment of controversial urban sensor system aided by aggressive lobbying." *The Intercept*. 26 Mar 2015. https://theintercept.com/2015/03/26/rapid-deployment-shotspotter-controversial-urban-microphone-system-aided-aggressive-lobbying/

178. "Best practices on how to secure federal or state funding for ShotSpotter." ShotSpotter. n.d. https://www.shotspotter.com/webinar/best-practices-on-how-to-secure-federal-or-state-funding-for-shotspotter/

179. Fang, Lee. "Deployment of controversial urban sensor system aided by aggressive lobbying." *The Intercept*. 26 Mar 2015. https://theintercept.com/2015/03/26/rapid-deployment-shotspotter-controversial-urban-microphone-system-aided-aggressive-lobbying/

180. Fraga, Brian. "'False alarms' lead Fall River to ditch ShotSpotter system." *Herald News*. 27 Jul 2017. https://www.heraldnews.com/news/20170727/false-alarms-lead-fall-river-to-ditch-shotspotter-system

181. Ramprasad, Swathi. "A tale of two cities: Lessons for Durham about ShotSpotter." *9th Street Journal*. 13 Nov 2019. https://9thstreetjournal.org/2019/11/13/a-tale-of-two-cities-lessons-for-durham-about-shotspotter/

182. "ShotSpotter Cities". ShotSpotter. n.d. https://www.shotspotter.com/cities/

183. https://techinquiry.org/lobbying/vendor/shotspotter%2C%20inc./?useModifiedDate=true

184. Chicago Contract Summary. http://ecm.chicago.gov/eSMARTContracts/service/dpsweb/ViewDPSWeb.zul

185. ShotSpotter Could Save Lives, But Some Questioned Its Role in Reducing Crime". *NBC Miami*. 9 Oct 2019. https://www.nbcmiami.com/news/local/shotspotter-could-save-lives-but-some-questioned-its-role-in-reducing-crime/1935794/

186. Grant, Kara. "ShotSpotter Sensors Send SDPD Officers to False Alarms More Often Than Advertised". 22 Sept 2020. https://www.voiceofsandiego.org/topics/public-safety/shotspotter-sensors-send-sdpd-officers-to-false-alarms-more-often-than-advertised/

187. Sandoval, Gabriel. "'ShotSpotter' Tested as Shootings and Fireworks Soar, While Civil Rights Questions Linger". *The City*. 5 Jul 2020. https://www.thecity.nyc/2020/7/5/21312671/shotspotter-nyc-shootings-fireworks-nypd-civil-rights

188. Hitchcock, Olivia. "LATEST: West Palm plans to have ShotSpotter technology within a month, chief says". *The Palm Beach Post*. 14 Aug 2018. https://www.palmbeachpost.com/news/local/latest-west-palm-plans-have-shotspotter-technology-within-month-chief-says/JEIOzGp4dNZ10RUE2VsTNP/

189. Neufeld, Dorothy. "ShotSpotter Secures US$4.27 Million Deal with Puerto Rico Authority". *INN*. 27 NOV 2019. https://investingnews.com/daily/tech-investing/cybersecurity-investing/shotspotter-secures-us4.27-million-deal-with-puerto-rico-authority/

190. *Suspected & Surveilled: A Report on Countering Violent Extremism in Chicago*. #StopCVE Chicago. 2019. http://www.stopcve.com/uploads/1/1/2/4/112447985/cvereport_final_fordigitaluse%5b3%5d_2.pdf

191. *Ibid.*

192. *Ibid.*

193. *Ibid.*

194. *Ibid.*

195. "#BosCops Toolkit - Boston Residents Organizing to Challenge the Power of the Police!" Muslim Justice League. 2018. https://docs.google.com/document/d/e/2PACX-1vQLRdhUcJGZ8CJzhZPwugVjAQVWlk24EjsZ-7a5QSLwWX1dn6DxSb9jRXIryzz1oMQ8POY67klwQHOt/pub

196. Wences, Rey. *Accountability After Abolition: The Regional Gang Intelligence Database (RGID)*. Policing Research Group in Chicago, University of Illinois at Chicago. May 2019. http://erasethedatabase.com/2019/05/14/accountability-after-abolition/

197. Trujillo, Josmar and Alex S. Vitale. *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing.'* Brooklyn College of the City University of New York Policing & Social Justice Project. 2019. https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf

198. *Ibid.*

199. Wences, Rey. *Accountability After Abolition: The Regional Gang Intelligence Database (RGID).* Policing Research Group in Chicago, University of Illinois at Chicago. May 2019. http://erasethedatabase.com/2019/05/14/accountability-after-abolition/; Trujillo, Josmar and Alex S. Vitale. *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing.'* Brooklyn College of the City University of New York Policing & Social Justice Project. 2019. https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf

200. Wences, Rey. *Accountability After Abolition: The Regional Gang Intelligence Database (RGID).* Policing Research Group in Chicago, University of Illinois at Chicago. May 2019. http://erasethedatabase.com/2019/05/14/accountability-after-abolition/

201. *Ibid.*

202. *Ibid.*

203. Trujillo, Josmar and Alex S. Vitale. *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing.'* Brooklyn College of the City University of New York Policing & Social Justice Project. 2019. https://static1.squarespace.com/static/5de981188ae1bf14a94410f5/t/5df14904887d561d6cc9455e/1576093963895/2019+New+York+City+Gang+Policing+Report+-+FINAL%29.pdf

204. *Ibid.*

205. "About #NoTechForICE." Mijente. n.d. https://notechforice.com/about/.

206. *Who's Behind ICE: The Tech and Data Companies Fueling Deportations.* National Immigration Project, Immigrant Defense Project, and Mijente. Oct 2018. https://mijente.net/wp-content/uploads/2018/10/WHO'S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf

207. *Ibid.*

208. *Take Back Tech: How to Expose and Fight Surveillance Tech in Your City.* Mijente, Just Futures Law, and UCI Law Immigrant Rights Clinic. Jul 2019. https://justfutureslaw.org/wp-content/uploads/2019/07/Tech-Policy-Report_v4LNX.pdf

209. *Ibid.*

210. "Retaliation against Immigrant Activists & Organizations." Just Futures Law (blog). n.d. https://justfutureslaw.org/retaliation-against-immigrant-activists-organizations/

211. "Surveillance During COVID-19: Five Ways Governments and Companies Are Using the Health Crisis to Expand Surveillance." Just Futures Law. Apr 2020. https://justfutureslaw.org/wp-content/uploads/2020/04/COVID.SURVEILLANCE.JFLv4_.pdf

212. Saifuddin, Maryiam. "Smart Cities: Making Government Accountability Work." Sunlight Foundation. 01 Oct 2018. https://sunlightfoundation.com/2018/10/01/watching-the-watchers-oaklands-citizens-oversight-of-smart-city-surveillance/

213. Abraham, Roshan. "Inside the ACLU's Nationwide Campaign to Curb Police Surveillance." *The Verge.* 01 Jun 2017. https://www.theverge.com/2017/6/14/15795056/aclu-police-surveillance-curb-campaign-nationwide

214. "Community Control Over Police Surveillance (CCOPS)." American Civil Liberties Union. n.d. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance

215. Hofer, Brian. "How the Fight to Stop Oakland's Domain Awareness Center Laid the Groundwork for the Oakland Privacy Commission." ACLU of Northern California (blog). 21 Sept 2016. https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission

216. "The Domain Awareness Center (DAC) FAQ." Oakland Privacy. Jul 2016. https://oaklandprivacy.org//wp-content/uploads/2016/07/dac-faq-v13.pdf

217. Wheeler, Brian. "Police Surveillance: The US City That Beat Big Brother." *BBC News.* 29 Sept 2016, sec. Magazine. https://www.bbc.com/news/magazine-37411250

218. Hofer, Brian. "How the Fight to Stop Oakland's Domain Awareness Center Laid the Groundwork for the Oakland Privacy Commission." ACLU of Northern California (blog). 21 Sept 2016. https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission

219. *Ibid.*

220. *Ibid.*

221. *Ibid.*

222. "The Domain Awareness Center (DAC) FAQ." Oakland Privacy. Jul 2016. https://oaklandprivacy.org//wp-content/uploads/2016/07/dac-faq-v13.pdf

223. Interview with Brian Hofer from Secure Justice & the Oakland Privacy Advisory Commission, Audio Recording. 10 Feb 2020. https://docs.google.com/document/d/1P9lzQEwV8rnD0BKr1bfyCVtFCQUdgsM4AsLIi0J7k2U/edit

224. *Ibid.*

225. Ravani, Sarah. "Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns." *San Francisco Chronicle.* 17 Jul 2019, sec. Bay Area & State. https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

226. Interview with Brian Hofer from Secure Justice & the Oakland Privacy Advisory Commission, Audio Recording. 10 Feb 2020. https://docs.google.com/document/d/1P9lzQEwV8rnD0BKr1bfyCVtFCQUdgsM4AsLIi0J7k2U/edit

227. "NYC Mayor Signs NYPD Surveillance Bill." S.T.O.P. - The Surveillance Technology Oversight Project (blog). 15 Jul 2020. https://www.stopspying.org/latest-news/2020/7/15/nyc-mayor-signs-nypd-surveillance-bill

228. "What We Do." S.T.O.P. - Surveillance Technology Oversight Project. n.d. https://www.stopspying.org/programs

229. Satter, Raphael. "New York City Oversight Bill to Force Police to Detail Surveillance Tools." *Reuters.* 12 Jun 2020. https://www.reuters.com/article/us-minneapolis-police-surveillance-idUSKBN23J32Y

230. *Ibid.*

231. *Ibid.*

232. *Ibid.*

233. Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." Georgetown Law Center on Privacy & Technology. 18 Oct 2016. https://www.perpetuallineup.org/findings/racial-bias

234. *Facial Recognition Market Size, Share, Growth and Trends [2020–2027].* Fortune Business Insights. Jul 2020. https://www.fortunebusinessinsights.com/industry-reports/facial-recognition-market-101061

235. "Ban Facial Recognition." Fight for the Future. n.d. https://www.banfacialrecognition.com

236. *Ibid.*

237. *Ibid.*

238. Conger, Kate, Richard Fausset, and Serge F. Kovaleski. "San Francisco Bans Facial Recognition Technology." *New York Times.* 14 May 2019, sec. U.S. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

239. Sheard, Nathan. "Victory: Oakland City Council Votes to Ban Government Use of Face Surveillance." Electronic Frontier Foundation. 18 Jul 2019. https://www.eff.org/deeplinks/2019/07/victory-oakland-city-council-votes-ban-government-use-face-surveillance

240. Haskins, Caroline. "Oakland Becomes Third U.S. City to Ban Facial Recognition." *Vice.* 17 Jul 2019. https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz

241. *Ibid.*

242. Guariglia, Matthew. "Victory! Berkeley City Council Unanimously Votes to Ban Face Recognition." Electronic Frontier Foundation. 16 Oct 2019. https://www.eff.org/deeplinks/2019/10/victory-berkeley-city-council-unanimously-votes-ban-face-recognition

243. McKay, Tom. "Berkeley Becomes Fourth U.S. City to Ban Face Recognition in Unanimous Vote." *Gizmodo.* 16 Oct 2019. https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recogniti-1839087651

244. Metz, Rachel. "Portland Passes Broadest Facial Recognition Ban in the US." *CNN Business.* 09 Sept 2020. https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

245. "Press Pause on Face Surveillance," ACLU Massachusetts. 18 Jun 2019. https://www.aclum.org/en/campaigns/press-pause-face-surveillance

246. Lannan, Katie. "Somerville Bans Government Use Of Facial Recognition Tech." *WBUR.* 28 Jun 2019. https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech

247. Ruckstuhl, Laney. "Brookline Passes Ban On Municipal Use Of Facial Recognition Tech." *WBUR.* 12 Dec 2019. https://www.wbur.org/news/2019/12/12/brookline-facial-recognition-technology-ban

248. DeCosta-Klipa, Nik. "Cambridge Become the Largest Massachusetts City to Ban Facial Recognition." *Boston.Com.* 14 Jan 2020. https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition

249. Cote, Jackson. "Northampton Bans Facial Recognition Surveillance, Becoming Third Community in Mass. to Do So." *MassLive.* 27 Feb 2020, sec. News. https://www.masslive.com/news/2019/12/northampton-bans-facial-recognition-technology-becoming-third-community-in-massachusetts-to-do-so.html

250. Brennan, Mike. "Michigan House Bill To Create 5-Year Moratorium On Law Enforcement Facial Recognition Tech." *MITechNews* (blog). 10 Jul 2019. https://mitechnews.com/politics/38078/

251. Roth, Cheyna. "Facial Recognition Bill Moves in State Legislature, Law Enforcement Hoping for Changes." *Michigan Radio.* 09 Dec 2019. https://www.michiganradio.org/post/facial-recognition-bill-moves-state-legislature-law-enforcement-hoping-changes

252. *Ibid.*

253. *Ibid.*

254. "California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams." ACLU of Northern California. 08 Oct 2019. https://www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams

255. Pester, Rachel. "Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ('BIPA') Violation Suit." *Harvard Journal of Law & Technology Digest.* 14 Feb 2020. https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit

256. Rosenthal, Jeffrey N., David J. Oberly, and Ana Tagvoryan. "What Businesses Need to Know about the Illinois' Biometric Information Privacy Act." Biometric Update. 01 Oct 2019. https://www.biometricupdate.com/201910/what-businesses-need-to-know-about-the-illinois-biometric-information-privacy-act

257. "Illinois General Assembly - Bill Status for SB2400." Illinois General Assembly. 03 Oct 2008. https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2400&GAID=9&DocTypeID=SB&LegId=36373&SessionID=51

258. "CIVIL LIABILITIES (740 ILCS 14/) Biometric Information Privacy Act." Illinois General Assembly. 03 Oct 2008. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

259. Korte, Amy. "Amendment to Exclude Facebook Facial-Recognition Technology from Illinois' Privacy Law Put on Hold." Illinois Policy. 17 Jun 2016. https://www.illinoispolicy.org/amendment-to-exclude-facebook-facial-recognition-technology-from-illinois-privacy-law-put-on-hold/

260. Coldewey, Devin. "Facebook Will Pay $550 Million to Settle Class Action Lawsuit over Privacy Violations." *TechCrunch* (blog). 29 Jan 2020. https://social.techcrunch.com/2020/01/29/facebook-will-pay-550-million-to-settle-class-action-lawsuit-over-privacy-violations/

261. Mac, Ryan, Caroline Haskins, and Logan McDonald. "Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies." *BuzzFeed News.* 07 May 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies.

262. *Ibid.*

263. *Ibid.*

264. Ward, Jacob and Chiara Sottile. "A Facial Recognition Company Wants to Help with Contact Tracing. A Senator Has Questions." *NBC News*. 30 Apr 2020. https://www.nbcnews.com/tech/security/facial-recognition-company-wants-help-contact-tracing-senator-has-questions-n1197291

265. Martinez, Freddy and Beryl Lipton. "Police Surveillance: Facial Recognition Use in Your Backyard." MuckRock. 2019. https://www.muckrock.com/project/police-surveillance-facial-recognition-use-in-your-backyard-452/

266. Lipton, Beryl. "Smarter Government or Data-Driven Disaster: The Algorithms Helping Control Local Communities." MuckRock. 2020. https://www.muckrock.com/news/archives/2020/feb/06/smarter-government-algorithm-database-launch/

267. Interview with Beryl Lipton from MuckRock, Audio Recording. 17 Mar 2020. https://docs.google.com/document/d/1iq8EHUbDe-j198_QWeq-gjAOnaCkDTSB4XqbYs4ELak/edit

268. *Ibid.*

269. Garvie, Clare and Laura M. Moy. "America Under Watch - Real-Time Facial Recognition in America." Georgetown Law Center on Privacy & Technology. 16 May 2019. https://www.americaunderwatch.com

270. *Ibid.*

271. Nagl, Kurt. "Detroit Police plans $4 million expansion of real-time crime centers, scraps plan to mandate Project Green Light." *Crain's Detroit Business*. 15 Jul 2019. https://www.crainsdetroit.com/government/detroit-police-plans-4-million-expansion-real-time-crime-centers-scraps-plan-mandate

272. Urban, Noah et al. "A Critical Summary of Detroit's Project Green Light and Its Greater Context." Detroit Community Technology Project. 09 Jun 2019. https://detroitcommunitytech.org/system/tdf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force=

273. *Ibid.*

274. *Ibid.*

275. *Ibid.*

276. *Ibid.*

277. Nagl, Kurt. "Detroit Police plans $4 million expansion of real-time crime centers, scraps plan to mandate Project Green Light." *Crain's Detroit Business*. 15 Jul 2019. https://www.crainsdetroit.com/government/detroit-police-plans-4-million-expansion-real-time-crime-centers-scraps-plan-mandate

278. Urban, Noah et al. "A Critical Summary of Detroit's Project Green Light and Its Greater Context." Detroit Community Technology Project. 09 Jun 2019. https://detroitcommunitytech.org/system/tdf/librarypdfs/DCTP_PGL_Report.pdf?file=1&type=node&id=77&force=

279. "Green Light Black Futures." Black Youth Project 100 Detroit. n.d. https://www.byp100.org/copy-of-d-c

280. Nagl, Kurt. "Detroit Police plans $4 million expansion of real-time crime centers, scraps plan to mandate Project Green Light." *Crain's Detroit Business*. 15 Jul 2019. https://www.crainsdetroit.com/government/detroit-police-plans-4-million-expansion-real-time-crime-centers-scraps-plan-mandate

281. "About Us." Stop LAPD Spying Coalition. n.d. https://www.scribd.com/embeds/107374089/content?start_page=1&view_mode=scroll&access_key=key-1z4p6cc6opb4a6efgrgt

282. Morgan, Emmanuel. "Group That Sued LAPD over Controversial Data Policing Programs Claims Victory." *Los Angeles Times*. 10 Dec 2019, sec. California. https://www.latimes.com/california/story/2019-12-10/stop-lapd-spying-coalition-announces-lawsuit-victory-against-lapd

283. *Ibid.*

284. *Ibid.*

285. "Tools and Resources." Stop LAPD Spying Coalition. n.d. https://stoplapdspying.org/action/tools-and-resources/

286. "Webinars." Stop LAPD Spying Coalition. n.d. https://stoplapdspying.org/action/webinars/

21st Century Policing:

The RISE and REACH of Surveillance Technology

Find this report and more at:

www.ACRECampaigns.org/Research

ACRE
ACTION CENTER
ON RACE & THE ECONOMY

COMMUNITY
RESOURCE HUB
FOR SAFETY & ACCOUNTABILITY