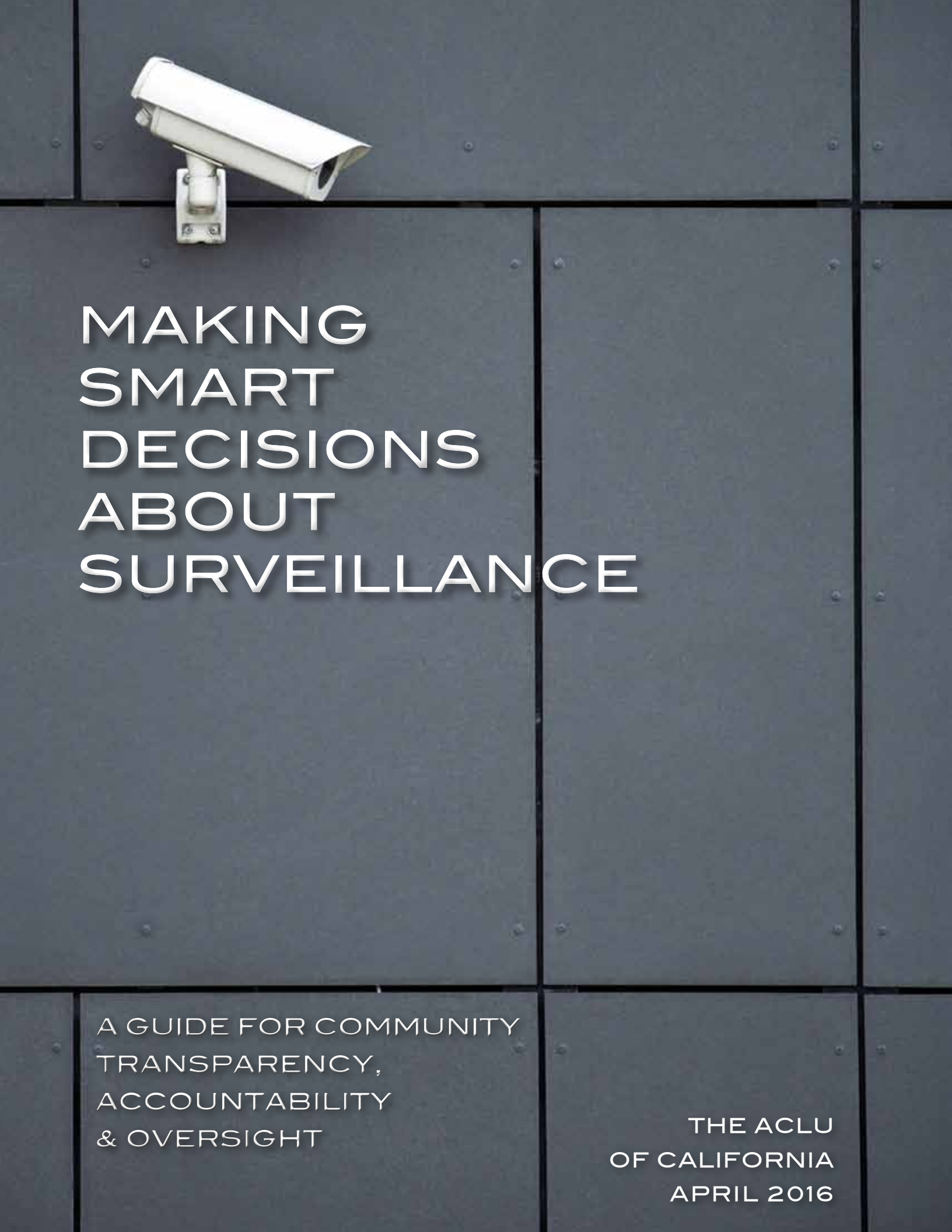

MAKING SMART DECISIONS ABOUT SURVEILLANCE

A GUIDE FOR COMMUNITY TRANSPARENCY, ACCOUNTABILITY & OVERSIGHT

THE ACLU
OF CALIFORNIA
APRIL 2016

Surveillance is on the rise in our communities, but basic transparency, oversight, and accountability remain the exception, not the rule. Police are spending billions of dollars on very sophisticated and invasive surveillance technology from license plate readers and cell phone trackers to facial recognition and drones. Too many of these programs are moving forward without public conversation, careful consideration of the costs and benefits, or adequate policies in place to prevent misuse and protect rights. As a result, surveillance may enable high-tech profiling, perpetuate systems of abusive policing, and undermine trust in law enforcement, particularly in communities of color where police misconduct has been rampant and community relationships have been strained. It's time for change.

Communities must be equal partners in any decision about the use of surveillance technology. They need to know when and why surveillance is being considered, what it is intended to do, and what it will really cost — both in dollars and in individual rights. They need to be certain that any proposal includes strong mechanisms for transparency, accountability, and oversight. Otherwise, public trust can be easily damaged, and communities can end up saddled with systems that are too invasive, very expensive, and much less effective at accomplishing community safety goals than initially imagined.

This guide provides a step-by-step framework to approach surveillance proposals, properly evaluate their true costs, and develop policies that provide transparency, oversight, and accountability. Its checklist walks community members, policymakers, and law enforcement officials through essential questions to ask and answer about surveillance proposals, and includes dozens of case studies highlighting smart approaches and missteps to avoid. The guide concludes with model language for policymakers to adopt to make sure the right process is used every time a surveillance proposal is considered.

We hope you will find this document and its supporting materials (available online at **aclunc.org/smartaboutsurveillance**) useful in ensuring your community is making informed decisions about surveillance.

Nicole A. Ozer
Technology and Civil Liberties Policy Director
ACLU of California

Peter Bibring
Police Practices Director
ACLU of California

CONTENTS

Authors: Chris Conley, Matt Cagle, Peter Bibring, Jessica Farris,

Linda Lye, Mitra Ebadolahi, and Nicole Ozer, ACLU of California

Contributing Writers: Addison Litton and Thomas Mann Miller

Design & Layout: Gigi Pandian & Daniela Bernstein

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

PUBLISHED BY THE ACLU OF CALIFORNIA
SECOND EDITION — APRIL 2016

TECHNOLOGY OVERVIEW

AUTOMATIC LICENSE PLATE READERS ("ALPRS"): Sophisticated camera systems mounted to police cars or light posts that scan license plates that come into view. They are often used to look for vehicles of interest, such as stolen cars, but in the process may record the time and place of every single vehicle that drives by.

BODY CAMERAS: Small cameras worn by police that record audio and video. These cameras can record anything from typical public interactions with police to sounds and images at rallies or even lewd banter in a squad car. Some body cameras are always on, others are controlled by the wearer.

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

VIDEO SURVEILLANCE: Camera systems that allow remote observation or recording of activity in public spaces. Video feeds may be actively monitored in hopes of spotting crime as it happens or recorded for potential use for investigation and prosecution. Studies have repeatedly shown cameras are costly and of limited use in preventing or solving serious crime.

FACIAL RECOGNITION: Software that identifies a person in photos or videos based on various characteristics of the person's face. The accuracy of facial recognition can vary widely.

LOCATION TRACKING: A range of techniques used to remotely track a person's location. GPS (Global Positioning System) devices, ranging from modern cell phones to "darts" that can be fired at a moving car, determine their own location based on satellite signals. Electronic communications devices including phones can also be tracked by identifying the cell towers or wireless networks the device uses. Location information can be obtained every few seconds and may be accurate to within a few feet.

AUTOMATED SOCIAL MEDIA MONITORING: Software tools that collects posts and other information on sites such as Twitter and Facebook. These tools may also analyze the collected data in order to derive information such as social connections or political views.

INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ("IMSI") CATCHERS: A device that emulates a cell phone tower in order to interact with nearby cell phones. IMSI catchers, commonly known as Stingrays (the brand name of one such device), identify nearby devices and can also be configured to intercept and capture the contents of communications including calls, text messages, or Internet activity. Many IMSI catchers operate in dragnet fashion, scooping up information about every phone in range.

DATA MINING: Techniques to discover statistical patterns, trends and other information in a collection of data. For example, analysis of connections on social networks can reveal hidden, sensitive information such as sexual orientation.

KEY QUESTIONS TO ANSWER BEFORE MOVING FORWARD WITH ANY SURVEILLANCE PROPOSAL

WHY ARE YOU CONSIDERING SURVEILLANCE?

- ❑ What specific problem is your community trying to address?
- ❑ How effective will surveillance be in addressing this concern?
- ❑ Are there alternatives that would be more effective, less expensive, or have less impact on civil liberties?

WHAT ARE THE COSTS AND RISKS?

- ❑ What are the financial costs of surveillance, including long-term training, operation and maintenance?
- ❑ What impact would surveillance have on privacy, free speech, and civil rights?
- ❑ How could surveillance affect trust in law enforcement?
- ❑ Have you completed a Surveillance Impact Report?

IS THE ENTIRE COMMUNITY ENGAGED IN EVALUATING THE PROPOSAL FROM THE OUTSET?

- ❑ Have you sought input on priorities, costs and risks from all segments of your community?
- ❑ Is there a Surveillance Impact Report and Surveillance Use Policy for the community to review?
- ❑ Will there be public hearings and debate before seeking any funds or purchasing any technology?

IS SURVEILLANCE THE RIGHT CHOICE?

- ❑ Have elected policymakers reviewed the Surveillance Impact Report and Surveillance Use Policy? Have they had an opportunity to hear public concerns?
- ❑ Will local policymakers specifically vote to approve the project moving forward? Will this happen before seeking any funds or purchasing any technology?
- ❑ Will your community re-evaluate any surveillance program annually and determine whether the program should be continued, modified, or abandoned?

WILL THESE QUESTIONS BE ANSWERED EVERY TIME?

- ❑ Has your community passed a Surveillance & Community Safety Ordinance to make sure these questions are consistently asked and answered every time surveillance is considered and to ensure proper transparency, oversight and accountability?

Why It Matters: The Costs and Consequences of Surveillance

Surveillance technology is often proposed as an efficient public safety tool. But too often, proposals ignore not only the true financial costs of surveillance technology but also their potential to infringe on civil rights and undermine public trust and effective policing. Communities should identify and assess all of the harms and costs of surveillance as early in the consideration process as possible in order to determine whether moving forward with a surveillance technology is really the right choice.

A. SURVEILLANCE IMPACTS CIVIL RIGHTS AND COMMUNITY TRUST

The community at large can pay a heavy price if surveillance technology is acquired and deployed without evaluating its impact on civil rights and its potential for misuse. Surveillance can easily intrude upon the individual rights of residents and visitors, perpetuate discriminatory policing, or chill freedom of expression, association, and religion — freedoms that public officials are sworn to protect.[1] As a result, surveillance can erode trust in law enforcement, making it harder for officers and community members to work together to keep the community safe.

> "[S]urveillance programs follow a long history of law enforcement targeting African American and other minority groups…. We need … a future in the city where our police department and other public institutions have true community oversight and accountability."
>
> The Rev. B.T. Lewis and Taymah Jahsi, Organizers, Faith in Community in Fresno[2]

1. *Surveillance Can Intrude Upon Community Members' Rights*

The greatest cost of surveillance technology may not be financial but personal: the invasion and infringement of civil rights. Various types of surveillance technology are capable of capturing and storing vast amounts of information about community members and visitors: the political rallies and religious services they attend, the health services they use, the romantic partners they have, and more. Just the perceived threat of surveillance has the potential to harm community members by discouraging individuals from participating in political advocacy, opposing police misconduct, evaluating reproductive choices, exploring their sexuality, and engaging in other activities that are clearly protected by the federal and California constitutions. And, too often, this perception is grounded in reality, as demonstrated by Fresno's use of social media monitoring software that flagged "#blacklivesmatter" as an indicator of criminal activity.[3]

> *Civil Rights Principles in an Era of Big Data,* signed by fourteen of the nation's leading civil and human rights groups, sounds the alarm on how surveillance technology often disproportionately affects communities of color and religious and ethnic minorities. It calls for technology to be "designed and used in ways that respect the values of equal opportunity and equal justice" and urges users to "stop high-tech profiling" and "preserve constitutional principles." The document further calls for search warrants and other independent oversight of law enforcement and "clear limitations and robust audit mechanisms to make sure that if these tools are used it is in a responsible and equitable way."[4]

There are many examples of the misuse of surveillance to target individuals based on their race, ethnicity, associations, or religious or political activities. Police in Santa Clara used a GPS device to track a student due to his father's association with the local Muslim Community Association.[5] Police in Michigan sought "information on all the cell phones that were congregating in an area where a labor-union protest was expected."[6] The NSA specifically monitored the email of several prominent Muslim-Americans with no evidence whatsoever of wrongdoing.[7] In Britain, where video surveillance is pervasive, a European Parliament

study showed that "the young, the male and the black were systematically and disproportionately targeted not because of their involvement in crime or disorder, but for 'no obvious reason.'"[8]

Surveillance programs that do not focus on individual targets can be particularly problematic. Tracking entire groups or communities extends "guilt by association" to those who have done nothing wrong, discourages participation in local activities, and alienates community members. And once members of the group are tainted with such suspicion, it becomes easy to justify prying into their private lives, or even threatening them with further consequences if they do not cooperate with additional surveillance efforts.[9]

SURVEILLANCE OF POLITICAL AND SOCIAL ACTIVISTS

The government has a long and troubled history of abusing surveillance powers to target political and social activists. From the "Red Squads" of the early 20th century to the FBI's efforts to infiltrate and discredit antiwar and civil rights activists in the 1960s, to recent surveillance of the Black Lives Matter movement:

- The Department of Homeland Security monitored the social media accounts of Black Lives Matter members and collected details about the locations of members and plans for peaceful protests in Ferguson, Baltimore, and New York City. This led many to question why the DHS — formed to combat terrorism — was surveilling members of a peaceful domestic social justice movement.[10]
- Police in Fresno, California, secretly acquired and tested multiple social media surveillance tools that encouraged surveillance of hashtags like #BlackLivesMatter, #dontshoot, and #wewantjustice and assigned individuals a "threat level." This led to nationwide negative press attention and calls for reform from community members, all of which forced the police chief to issue a public apology.[11]
- Authorities in the Oregon Department of Justice came under fire when it was revealed that a senior investigator had used software to conduct surveillance of hashtags including #BlackLivesMatter, which returned results for civil rights advocates, including the president of the Urban League of Portland. The story triggered a public apology by Oregon's Attorney General and led to an internal investigation.[12]

Intelligence reforms born from lawsuits and congressional inquiries have led many law enforcement agencies to bar the collection of information about political activism and other First Amendment-protected activities without a justifiable suspicion of criminal activity. But surveillance of Black Lives Matter demonstrates a need for similar restrictions on the use of surveillance technology today to ensure that it is not used to chill or undermine political and social activism.

"Dragnet" surveillance often targets communities of color: for example, in Oakland, the police have disproportionately used license plate readers in African-American and Latino neighborhoods.[13] In Compton, police flew a plane rigged with high-powered surveillance cameras overhead for weeks without the public's knowledge or consent.[14] Because it involves collecting vast amounts of information, dragnet surveillance also creates the potential for all sorts of abuse, from NSA analysts tracking romantic partners[15] to a Washington, D.C. police lieutenant blackmailing patrons of a gay bar.[16]

> "One of the most alarming parts of that history has been the ways that surveillance has been misused against Black people who have been advocating for their justice. It's been used to discredit, abuse, and incarcerate."
>
> Opal Tometi, Black Lives Matter co-founder[17]

Surveillance carries privacy and free speech threats even if it is conducted solely in public places. This is particularly true when surveillance information is aggregated to build a robust data profile that can "reveal much more in combination than any isolated record."[19] As Supreme Court Justice Sonia Sotomayor has noted, "a precise, comprehensive record of a person's public movements … reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." In addition, "[a]wareness that the Government may be watching chills associational and expressive freedoms."[20]

> "Those of us from marginalized communities grew up in environments very much shaped by surveillance, which has been utilized to ramp up the criminal justice system and increase deportations…."
>
> Steven Renderos, Center for Media Justice[18]

2. *Surveillance Can Erode Trust in Law Enforcement*

When law enforcement fails to fully engage with community members about the impact of surveillance — or, worse, entirely skirts the democratic process by acquiring and deploying surveillance technology without public discussion at all — it erodes trust even further, making it even harder for law enforcement officers to work with the community to solve crimes and protect public safety.

In the years after the September 11th attacks, the New York Police Department created a secretive intelligence wing that infiltrated Muslim neighborhoods with undercover officers, where they monitored the daily lives of and compiled dossiers about Muslim-Americans engaging in constitutionally protected activities in cafes, bookstores, and private residences with no evidence of illegal activity.[21] These activities gravely harmed the community's trust in law enforcement and led to a multi-year lawsuit and settlement that barred the NYPD from conducting investigations on the basis of race, religion, or ethnicity, and mandated implementation of a series of reforms designed to deter warrantless surveillance.

> "The effects of surveillance on New York Muslim communities have been devastating…. Community members' ties to local police precincts have deteriorated due to distrust and fear."
>
> Hina Shamsi, ACLU National Security Project Director[22]

In Compton, news broke about an aerial surveillance program that watched the whole community and was intentionally kept "hush-hush" by the Sheriff's Department to deter civil rights complaints. Both citizens and lawmakers were up in arms that they had been kept in the dark about such intrusive surveillance. Angry community members rightly questioned, "Why are we the target? As citizens we deserve [to know]. We are not all criminals.... It's an invasion of privacy." The Mayor called for a "citizen private protection policy," ensuring that the community would be notified before any new surveillance equipment was deployed or used.[23]

B. SURVEILLANCE CARRIES BOTH IMMEDIATE AND ONGOING FINANCIAL COSTS

In addition to the costs to civil rights and civil liberties, the fiscal impact of surveillance can be extensive. Modifying current infrastructure, operating and maintaining systems, and training staff can consume limited time and money, even if federal or state grants fund initial costs. Surveillance technologies may also fail or be misused, resulting in costly lawsuits. To calculate the full financial cost of surveillance technology, communities must look beyond the initial sticker price.

1. *Surveillance Requires Infrastructure, Staffing, Training, and Maintenance*

The hidden costs of infrastructure, training and staffing, operations and maintenance, and the potential for budget overruns, can dwarf the cost of acquiring surveillance technology in the first place. Communities that have failed to accurately estimate the full financial cost of a surveillance system have dealt with massive cost overruns and programs that failed to accomplish their stated purpose. For example, Philadelphia planned to spend $651,672 for a video surveillance program featuring 216 cameras. Instead, it spent $13.9 million on the project and wound up with only 102 functional cameras after a year, a result the city controller described as "exceedingly alarming, and outright excessive — especially when $13.9 million is equivalent to the cost of putting 200 new police recruits on our streets."[25] To avoid a similar incident in your community, it is essential to identify all of the costs required to install, use, and maintain surveillance technology before making a decision about whether to do so.

> "When you're considering a new technology, it's important to evaluate not only the upfront costs but also the costs of maintenance and upgrades that will occur down the road."
>
> Captain Michael Grinstead, Newport News (VA) Police Department[24]

2. *Surveillance Can Create Financial Risks Including Litigation and Data Breach*

Surveillance programs that fail to include proper safeguards to prevent errors or misuse and protect freedom of expression, association, and religion, or that inadequately enforce such safeguards, can lead to expensive litigation that diverts resources from other public services. For example, Muslim residents in Orange County filed a discrimination lawsuit when it was revealed that state agents were sending informants into mosques to collect information on the identities and activities of worshippers.[26] The NYPD paid $2 million in attorney fees for spying on New York's Muslim communities.[27] Even technical glitches can create the potential for costly lawsuits and other expenses: the City of San Francisco was embroiled in a multi-year civil rights lawsuit after wrongly pulling over, handcuffing, and holding at gunpoint an innocent woman due to an error by its ALPR system.[28]

> "After public backlash about Oakland's proposed Domain Awareness Center, we really had to regroup and think about how we needed to proceed."
>
> Renee Domingo, former Oakland Emergency Services Coordinator[29]

The collection of surveillance data also creates the risk of data breaches that can incur significant public costs as well as endanger residents' privacy and economic security. Even following best practices (which itself can entail significant expense) is not enough to prevent every breach. California law requires that a local agency notify residents about a security breach.[30] And the fiscal costs of a breach of sensitive surveillance data could be very high: a 2015 report found that companies spent an average of $3.7 million to resolve a data security breach.[31] The more information your community collects and retains, the greater the risk and potential cost of a breach.

3. *LACK OF PROPER PROCESS CAN WASTE TIME AND MONEY*

> "SJPD should have done a better job of communicating the purpose and acquisition of the UAS (Unmanned Aerial System) device to our community….The community should have the opportunity to provide feedback, ask questions, and express their concerns before we move forward with this project."
>
> San Jose Police Department[34]

Failing to thoroughly discuss surveillance proposals and listen to community concerns early in the process can result in massive backlash and wasted time and funds when plans are suspended or ultimately cancelled. Oakland was forced to scrap most of the planning for its ill-fated Domain Awareness Center and scale the project back considerably after community members protested the misleading mission statement and lack of transparency for the project.[32] In Santa Clara County, a secretive process to purchase a Stingray cell surveillance device was derailed by the County Executive after it sidestepped necessary community debate and county oversight.[33] Community members grounded San Jose's secret drone purchase and the police were forced to apologize for the lack of transparency and community input.[35] Engaging with the community before taking steps to go forward with a surveillance proposal is essential to avoiding similar mistakes that spark widepsread community outrage and waste time and resources.

C. SURVEILLANCE MUST TAKE EVOLVING PRIVACY LAW INTO ACCOUNT

The use of surveillance technology is facing increased scrutiny and limits. Courts and lawmakers at the state and federal level, driven by increased public concern about privacy, are acting to protect individual rights and civil liberties. As a result, your community needs to consider both the existing laws and the potential for legal change, including the policy and individual rights concerns that are driving that change, when evaluating a surveillance proposal.

In recent years, federal courts have repeatedly reinforced legal protections for individual rights in the context of today's technology. In 2015, the U.S. Supreme Court unanimously told law enforcement to "get a warrant" to search an arrestee's cell phone. In another unanimous decision, the Court also ruled a warrant is required to use a GPS beeper to track a suspect's vehicle, with a majority of the Court suggesting that using technology to track an individual's location — even in public — over an extended period of time triggers constitutional scrutiny.[37] Finally, multiple federal courts declared the NSA's warrantless collection of telephone metadata unlawful, with one criticizing its "almost Orwellian" scope.[38] Surveillance programs that fail to account for this trend may well be held unconstitutional, and criminal investigations based on evidence from those programs could be jeopardized.

> "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."
>
> *Riley v. California,* U.S. Supreme Court[36]

The California Constitution is even more protective of community members' privacy, including in public spaces. The state right to privacy expressly gives Californians a legal and enforceable "right to be left alone" that protects interests in privacy beyond the home.[39] The California Supreme Court has held that covertly "infiltrating" and monitoring the activities of students and professors at classes and public meetings without any indication of criminal activity violated the California Constitution,[40] as did warrantless aerial surveillance of a resident's backyard.[41] Californians' right to free expression also extends outside of the home, even to privately owned areas like shopping centers.[42]

Numerous laws and regulations also place limits or requirements on the use of surveillance technology. The federal Wiretap Act and its California counterpart limit the use of surveillance technology capable of

intercepting the contents of live communications. And in 2015, California lawmakers enacted three separate laws that specifically address issues related to surveillance technology:

- **Collection of Electronic Information**: The California Electronic Communications Privacy Act requires a search warrant when collecting electronic information with surveillance technology like cell phone tracking technology. It also requires a warrant for searching electronic devices or compelling email, location information, or other metadata from service providers. The law creates additional procedural safeguards, including notice to the suspect, and allows for suppression or court-mandated deletion of information obtained or retained in violation of the law.[43]
- **Automated License Plate Readers**: Newly enacted California law requires an opportunity for public comment, a written, publicly available use policy that is "consistent with respect for an individual's privacy and civil liberties," and reasonable security safeguards for any use of automated license plate readers. Individuals can sue for harms due to a security breach or other unauthorized disclosures.[44]
- **Cell Phone Tracking Technology**: Newly enacted California law requires public process, local legislative approval for all agencies other than sheriffs, a public use and privacy policy that is "consistent with respect for an individual's privacy and civil liberties," and the disclosure of agreements with other agencies concerning the use of IMSI catchers and other cell phone tracking technology. The law also allows an individual to sue an agency for violating these provisions.[45]

There have also been bipartisan legal changes at both the federal and state level to rein in surveillance. In 2016, federal lawmakers adopted reforms related to NSA spying.[46] Eighteen other states have enacted laws restricting law enforcement access to location information,[47] and a majority of states have introduced legislation aimed at curbing the use of drones for surveillance purposes.[48]

These state and federal changes are driven by a clear shift in public attitudes towards surveillance. Community members want and expect reform at both the state and local level to increase transparency, accountability, and oversight for surveillance technology. Two thirds of California voters want to see local elected officials like City Councilmembers or County Supervisors approve new surveillance technologies before they can be used. Similarly, a strong majority of voters want to see both local (65 percent) and state (64 percent) policies

SURVEY OF LIKELY 2016 CALIFORNIA VOTERS FINDS STRONG SUPPORT FOR REFORMS TO SURVEILLANCE TECHNOLOGY USE BY LAW ENFORCEMENT

Likely 2016 voters polled in a California statewide survey strongly favor local and state level reforms of law enforcement surveillance technology practices.[49] A summary of key findings from the survey:

Reform Proposal	Support
Require the local City Council or Board of Supervisors to vote to approve new surveillance technology before it is used by local police.	67%
Develop and enforce local policies to set limits on surveillance technology used by police.	65%
Develop and enforce statewide policies to set limits on surveillance technology used by police.	64%
Require law enforcement agencies to publicly report how often they are using surveillance.	62%
Provide public notification prior to local police buying new technology for surveillance.	58%

developed and enforced that set limits on police use of surveillance technology. Voters also want to see steps taken to require public reporting from law enforcement agencies regarding the frequency of use of surveillance technologies (62 percent) as well as public notification before the purchase of any new surveillance technologies (58 percent).[50]

All of these factors have led many communities to move forward with local ordinances that ensure transparency, accountability, and oversight for all surveillance technologies.[52] Your community should follow their lead and thoroughly evaluate any surveillance proposal in order to protect the rights of your community members, identify hidden costs and financial risks, and ensure that you comply with existing laws and are consistent with increasing public concerns about privacy.

> "With a surveillance equipment ordinance, any of the existing equipment that Oakland might already have or any that is soon to come out will have to go through the vetting process."
>
> Brian Hofer, Chair, Oakland Domain Awareness Center Privacy Committee[51]

ENACT A SURVEILLANCE & COMMUNITY SAFETY ORDINANCE TO MAKE SURE THE RIGHT PROCESS IS FOLLOWED EVERY TIME

Passing the Surveillance & Community Safety Ordinance included in the Appendix to this guide will help your community avoid problems down the line by following the right process every time. It ensures that there is community analysis of surveillance technology whenever it is considered, that local lawmakers approve each step, and that any surveillance program that is approved includes both a Surveillance Use Policy that safeguards individual rights and transparency and accountability mechanisms to ensure that the Policy is followed.

Necessary Steps when Considering a Surveillance Proposal

Surveillance can be misused in ways that harm community members, undermine public safety goals, and saddle taxpayers with unnecessary costs. That's why it is essential to publicly and thoroughly evaluate surveillance proposals. The following section will help your community — including diverse residents, public officials, and law enforcement — work together to determine whether surveillance really makes sense and put in place robust rules to ensure proper use, oversight, and accountability if your community decides to move forward with a surveillance proposal.

The Department of Homeland Security (DHS) Privacy Office and Office for Civil Rights and Civil Liberties issued *CCTV: Developing Privacy Best Practices*, a report that encourages government agencies to build privacy, civil rights, and civil liberties considerations into the design, acquisition, and operations of video surveillance systems. An appendix highlights the need to follow the Fair Information Practice Principles of Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, Accountability, and Auditing.[53]

A. COLLECTIVELY EVALUATE THE EFFECTIVENESS, COSTS AND ALTERNATIVES BEFORE MAKING DECISIONS ABOUT SURVEILLANCE

Surveillance should only be a means to an end, never an end in itself. That means that your community should have an actual purpose in mind or problem that needs to be addressed before even considering surveillance technology. Once you have that, you can collectively evaluate whether surveillance is likely to effectively accomplish your goals, as well as estimate the costs to both your community's budget and to individual rights.

1. *Decide as a Community: Involve the Entire Community from the Start*

Fewer than 15 percent of California communities publicly debated surveillance programs before moving forward. (ACLU 2014)[54]

The best way to consider whether surveillance is the right choice and to avoid costly mistakes is to engage the entire community — including law enforcement, local lawmakers, and members of the public — in a thorough discussion about any surveillance proposal. Different segments of your community are likely to bring valuable perspectives to the process of evaluating whether to acquire and use surveillance technology. And the time to engage with your community is at the very beginning of the process, *before* any funding is sought, technology is acquired, or system is used.

Several cities considering proposals to introduce or expand surveillance have found it useful to actively engage community members through working groups and ad-hoc committees to shape policy and provide oversight. The Redlands Police Department convened a Citizens' Privacy Council, open to any city resident of the city, to provide advice on surveillance-camera policies and oversee police use of the cameras.[55] Richmond formed an ad-hoc committee to evaluate policies for its video

"The public debate that the surveillance ordinance will require on new technologies and their uses will be beneficial for everyone, including city officials, to help them learn more about how these programs work and what they mean to the public."

Joe DeVries, Oakland Assistant to the City Administrator[56]

surveillance program.[57] And in 2014, following community backlash and the vote not to expand Oakland's Domain Awareness Center, the City Council created a Privacy and Data Retention Ad Hoc Advisory Committee comprised of diverse community members to create safeguards to protect privacy rights and prevent the misuse of data for a scaled-back system to be used at the Port of Oakland.[59] Oakland now has a formal Privacy Commission, which will provide advice to the City of Oakland on best practices to protect privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores data.[60]

> "Technology can only serve democracy to the degree that it is democratized."
>
> Malkia Cyril, Director, Center for Media Justice[58]

- *Is the community engaged in an informed debate about any surveillance proposal?*

It is never too early for a public debate about a surveillance proposal. Community members should know what kind of surveillance is being considered, what it is intended to do and how it will affect them at the earliest stages of the process, when their input can bring out important information, highlight community concerns, and help avoid unforeseen problems and community backlash.

CASE STUDY: SANTA CLARA COUNTY CANCELS STINGRAY BUY DUE TO TRANSPARENCY CONCERNS

In 2015, the Santa Clara County Executive rejected the Sheriff's proposal to purchase a Stingray after the Board of Supervisors questioned the expense and secrecy of the project. The Board questioned how they could be asked to spend more than $500,000 of taxpayer money to approve a purchase that was shrouded in secrecy even from the Board itself. The County Executive ultimately rejected the purchase because the company providing the Stingray refused to "agree to even the most basic criteria we have in terms of being responsive to public records requests… We had to do what we thought was right."[61]

The public should be given effective notice that surveillance is being considered. Effective notice means more than a line item in a public meeting agenda. Law enforcement should proactively contact community groups, including those representing ethnic and religious communities, and local media to increase public awareness early in the process and engage the entire community with the issue.

CASE STUDY: OAKLAND'S "DOMAIN AWARENESS CENTER" FORCED TO SCALE BACK AFTER KEEPING COMMUNITY IN THE DARK

In 2013, the City of Oakland tried to expand its "Domain Awareness Center," originally focused on the Port of Oakland, into a citywide surveillance network linking together video cameras from local streets and schools, traffic cameras, and gunshot microphones. Instead of soliciting early public input about the expanded system, Oakland tried to move forward without any meaningful engagement with the community. Residents were outraged, and the City Council voted against expanding the system.[62]

An informed debate also requires that your community have access to a wide range of information in order to assess how surveillance would work in practice and whether it would advance local goals. Community meetings with various speakers representing different perspectives (not just law enforcement and the technology vendor) can help the community understand how the surveillance technology actually works and its potential implications. The entity seeking to acquire new surveillance technology should also prepare and release a Surveillance Impact Report and a Surveillance Use Policy to help everyone understand how a technology will work, its potential costs, and the safeguards that will prevent its misuse if the proposal were approved. Your community may also consider convening an ad-hoc committee of local residents, experts and advocates who can work together to make recommendations or help complete these documents.

> "It is critical to our judicial system and our democracy that the public and our elected representatives be informed about the use of these devices so that we can have a discussion about their privacy implications and make informed decisions about policies for their use."
>
> Joe Simitian, Santa Clara County Supervisor[63]

USE A SURVEILLANCE IMPACT REPORT TO MAKE AN INFORMED DECISION

The scope and potential costs of a surveillance technology should be assessed and made available to the community through a Surveillance Impact Report. This report should include:

- Information describing the technology, how it works, and what it collects, including technology specification sheets from manufacturers;
- The proposed purposes(s) for the surveillance technology;
- The location(s) it will be deployed and crime statistics for any location(s);
- An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public; and
- The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.

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

CASE STUDY: SANTA CRUZ COUNCILMEMBERS LACK INFORMATION FOR ALPR DECISION

After the Santa Cruz City Council approved the use of federal funds to purchase ALPRs for the police department, councilmembers noted that they did not have a lot of information about the technology or its impact on the community at the time of its decision. When one councilmember was asked what effect the scanners might have on community members, he replied, "I don't know enough about the technology." Another was unaware of privacy issues, admitting, "The council didn't get much correspondence about the potential for the erosion of civil rights that these kinds of devices can cause...."[64]

➢ *How will the community decide whether to proceed with a surveillance proposal?*

Community members deserve more than just information about surveillance proposals: they need the opportunity to help determine whether the proposal actually benefits the community and how or whether it should move forward, either by giving input to local policymakers at public hearings or by casting their own ballot on the issue.

In either case, initial community approval should be obtained before any steps towards acquiring surveillance technology are taken, including applying for funding from outside entities. This ensures that external grants do not circumvent the proper democratic process and cut community members out of the loop. Local policymakers or the community as a whole should be given additional opportunities to weigh in if the proposal changes or as more details become available.

CASE STUDY: SAN JOSE'S DRONE GROUNDED UNTIL COMMUNITY APPROVES

San Jose residents were outraged when they learned that their police department had purchased a drone without any public debate. Amid critical media coverage and protests from community groups, civil-rights advocates, and local residents, police apologized and said they would ground the drone until they could conduct adequate public outreach.[65]

2. *Define the Purpose: Ask How and Whether This Technology Will Aid Your Community*

Your community cannot determine whether surveillance is an appropriate solution if you have not first identified the problem. Defining the specific purpose or issues that surveillance is intended to address is essential to evaluate the likely effectiveness of surveillance and to identify alternatives that might provide a better fit for your community's needs and budget. It can help highlight the individuals or communities who are likely to be most impacted by surveillance and ensure that their thoughts and concerns are fully understood. It also provides a starting point for crafting a Surveillance Use Policy by defining specific objectives for which surveillance is appropriate and barring its use outside of those purposes.

➢ *What specific community purposes will be aided by adopting this technology?*

A well-defined community purpose should include a specific problem and a measurable outcome that the community desires. Vague purposes such as "protecting our city from criminals" make it difficult for the community to understand how surveillance might be used or how its effectiveness might be measured. In contrast, a purpose such as "increase recovery of stolen vehicles" succinctly identifies an outcome desired by community members and helps frame public discussion. That discussion may in turn lead you to narrow or alter the purposes for which surveillance should be used, if you decide to use it at all.

CASE STUDY: OAKLAND SPENDS $2M ON "HARDLY USED" POLICE TECHNOLOGY

The cash-strapped city of Oakland learned the hard way that acquiring new police technology without a clearly defined purpose can be a waste of time and money. A city audit revealed that the city had squandered almost $2 million on hardly used police technology between 2006 and 2011. The auditor recommended steps to ensure that technology purchases were intended to fulfill specific strategic objectives and regular evaluation of their effectiveness.[66]

➢ *Will this surveillance technology help your community achieve that purpose?*

After your community identifies the purposes that surveillance technology might be able to address, you should evaluate whether the proposed technology would actually achieve them. Manufacturer's claims should not be taken at face value, and certainly not in isolation. Instead, your community should look at all of the evidence or arguments suggesting that surveillance will or will not effectively help you achieve your defined purpose.

CASE STUDY: SAN FRANCISCO RECONSIDERS PLANS TO EXPAND SAFETY CAMERA PROGRAM THAT FAILS TO IMPROVE COMMUNITY SAFETY

In 2005, San Francisco set out to deter violent crime and provide police with an investigative tool by installing video cameras in the City's high-crime, high-traffic areas. However, post-installation crime statistics published by mandate under a city ordinance revealed that the cameras neither reduced crime nor assisted in solving them in any meaningful way. In fact, the cameras only led to six suspects being charged by the SFPD between 2005 and 2008. As a result, the Police Commission reconsidered its plans to expand the program.[67]

➢ *Are there better alternatives to achieve your purpose?*

Even if the proposed surveillance technology does seem likely to help your community achieve its purpose, there still may be alternatives that are just as (or more) effective, less expensive, and/or less likely to be misused or otherwise negatively impact your community members.

In particular, you should compare the effectiveness and costs of technology-based solutions with non-technology-oriented approaches to address the problem. For example, multiple studies have shown that traditional approaches such as increased lighting and foot patrols significantly reduce crime.[68] You should not automatically assume that surveillance technology will be more effective.

CASE STUDY: CITIES REPLACE RED LIGHT CAMERAS WITH LONGER YELLOW LIGHTS

California cities are increasingly shutting down red light cameras as evidence mounts that the cameras increase, rather than decrease, traffic accidents. For example, in Walnut, CA, a study found that red light cameras resulted in dramatic increases in "red light running collisions" (400%), "rear end collisions" (71%) and "broadside collisions" (100%)" and that "no argument can be made that photo enforcement has improved safety . . . within the city of Walnut. In fact, the use of red light cameras appears to have decreased safety and put roadway users at increased risk." In light of this evidence, more than half of the California cities that once used red light cameras have ended their programs, turning instead to alternatives that have proven more effective at preventing accidents such as longer yellow lights at dangerous intersections.[69]

3. *Identify the Costs and Risks: Examine Financial, Legal, and Practical Consequences*

Even if a specific technology is appropriate for your community's purposes, there still may be financial, legal and practical concerns that may make adopting it undesirable. This section will help you measure the likely costs of surveillance so that you can determine whether they are truly outweighed by the expected benefits.

➢ *How much will the technology cost your community to acquire and operate?*

Deciding how to allocate funds is one of your community's most important tasks. Every dollar your community spends on surveillance technology is a dollar it cannot spend on some other community need. Costs related to surveillance technology will include personnel time, training costs, maintenance and upkeep, as well as any network and storage costs for the data your community may collect. Potential costs associated with risks of data breach or lawsuits based on abuse of surveillance also need to be recognized.

> "One more question to ask ourselves is whether we are carefully considering the infrastructure that is needed to support technology — the costs of monitoring it and of staffing technology units at a time when departments are laying off civilians. We really need to think about all of the aspects of technology when initial investments are being made."
>
> Police Executive Research Forum, "How Are Innovations in Technology Affecting Policing?"[70]

Questions about costs cannot be dismissed solely because your community is seeking grant funding to pay for the technology. These grants are attractive for obvious reasons: they appear to allow your community to buy a technology without having to spend local taxpayer dollars. But outside grants may not cover the costs that follow a technology's adoption, particularly the long-term costs of operation, repairs, and personnel. Estimating these costs as accurately as possible — and making sure those estimates are shared with the community and made part of the debate about adopting surveillance — is key.

➢ *What are the legal risks and associated potential costs of the surveillance proposal?*

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

CASE STUDY: FBI REMOVES GPS TRACKERS AFTER SUPREME COURT RULES THAT WARRANTLESS TRACKING IMPLICATES FOURTH AMENDMENT

The FBI had installed approximately 3,000 GPS trackers on cars throughout the United States, without a warrant, when the U.S. Supreme Court ruled in 2012 that their use implicated the Fourth Amendment. As a result, the FBI deactivated the warrantless trackers, and its agents had to physically retrieve them. Obtaining warrants before using those GPS trackers would have ensured the constitutionality of obtained evidence and saved the FBI considerable time and effort.[71]

➢ *How could the surveillance proposal negatively impact public safety or individual rights?*

A surveillance proposal designed to benefit your community may carry side effects that undermine that objective. Insecure systems can present a tempting target for hackers, potentially making your community less safe in the process. Surveillance programs that target or disproportionately impact communities of color or other marginalized groups can make it harder for law enforcement to work cooperatively with those groups to investigate crimes. And surveillance can chill political and social engagement such as attendance at political rallies, gun shows, or religious ceremonies if community members fear that their lives are constantly being monitored. Identifying the harms as well as benefits of surveillance is an important part of evaluating any proposal.

CASE STUDY: REDLANDS DEPLOYS INSECURE CAMERA NETWORK

The surveillance camera network in the city of Redlands made the news for the wrong reasons when computer security experts demonstrated how easily they could take control of the cameras. Although the police department expressed concern about "people with criminal intent using the public camera feed to case homes or businesses or track the police force," the network was deployed with no security at all. Even after the story broke, the network was secured with an outdated encryption protocol that a researcher described as "putting a diary lock on your front door."[72]

B. ESTABLISH A SURVEILLANCE USE POLICY TO MITIGATE HARMS AND PROTECT RIGHTS

If after careful consideration and public debate your community decides that a particular surveillance technology is worth adopting, you need to ensure that policies are in place so that it is used properly. A clear, legally enforceable Surveillance Use Policy that provides guidance about when and how to use surveillance can safeguard individual rights while protecting local law enforcement and your entire community from costly lawsuits, bad press, loss of community trust, and more. Recognizing the necessity of use policies, Seattle and Spokane, Washington, recently passed ordinances requiring police to develop use guidelines for new surveillance equipment before using it.[73]

CASE STUDY: ALAMEDA COUNTY SOLICITS PUBLIC INPUT FOR STINGRAY POLICY

Before upgrading its cell phone surveillance technology, the Alameda County District Attorney publicly released its draft use policy and solicited feedback from the community. In response to feedback, the District Attorney made changes that resulted in a policy requiring a warrant for the use of the device and strict limits on how data could be used. This transparent and democratic process helped build community trust and ensured a stronger set of safeguards would be in place from the start.[74]

Here are some of the key elements of a robust, legally enforceable Surveillance Use policy:

1. *Use Appropriately: Place Clear Limits on Surveillance*

If your community has been following this guide, you've already defined community purposes that justify a particular technology. Now it's time to use those purposes to decide and codify both the acceptable uses that will benefit the community and those that are simply prohibited. Doing so safeguards against use of the technology in a manner the community never intended.

➢ *When is surveillance permitted or prohibited?*

The first step is straightforward but essential: defining how and when the technology may be used. Every entity in your community that conducts surveillance should have a policy that clearly specifies appropriate uses of each technology and bars all other uses.

> Publicly available use policies were found for less than 1 in 5 local California surveillance programs (ACLU 2014 research).[75]

In order to benefit from and reflect community input and oversight, technology should only be used for the particular purposes for which it was acquired. Any proposed new uses should be subject to the same public discussion as the acquisition of new technology, allowing the community to weigh in on the appropriateness of any expanded purpose.

Your policy needs to be consistent with constitutional guarantees of privacy, equal protection, freedom of speech, and freedom of religion. In fact, your use policy should not only address clearly unlawful but also potentially unlawful uses of surveillance technology. If there are questions about the legality of a specific practice, your use policy should prohibit that practice until there is a definite answer.

> The police need to "have more of a dialog with the council, because we are the ones that . . . approve funding decisions and we want to make sure . . . that you are hearing everything that we hear as well."
>
> Seattle Councilmember Bruce Harrell [76]

➢ *What legal or internal process is required to use surveillance?*

It is also important to ensure that all legally required and internal processes are followed each time surveillance is used. These processes help to prevent unauthorized or outright illegal uses and also make sure that even appropriate uses of the surveillance technology minimize the impact on individual rights.

In many cases, the best way to ensure that legal requirements are satisfied is to require a search warrant prior to conducting surveillance, allowing the court system to play a role in overseeing the program. With the streamlined modern warrant process, officers can seek a judge's approval quickly and easily by simply placing a phone call or using a mobile device.[77]

Internal recordkeeping, including recording the reason for each use of surveillance, can also help ensure compliance with the appropriate use policy and create an audit trail for ongoing feedback and oversight.

➢ *How are officers trained before they conduct surveillance?*

Having clear policies is not helpful if the people using the technology or the data it collects lack the underlying knowledge to comply with those policies. Training programs for anyone involved with surveillance must be comprehensive, encompassing not just the technology and Surveillance Use Policy but the purposes and legal rules that inform the Policy. Training should spell out both the obligations of anyone using the technology and the consequences for policy violations.

➢ *Are you only collecting necessary data?*

Ensuring that surveillance technology is used in a way that accomplishes its stated purpose without collecting additional data is a straightforward way to reduce the risk of privacy invasions. That's why the federal statute authorizing wiretaps has from its inception required "minimization" — an effort to make sure that even after a warrant has been issued and collection is underway, police only intercept communications relevant to the investigation, not every communication made by the target.[78]

The same principle should be applied to other forms of surveillance, requiring a reasonable effort to avoid collecting superfluous information. For example, a police department that deploys drones to an accident scene to quickly identify any need for police or emergency intervention does not need to record and retain video footage.

CASE STUDY: OHIO STATE HIGHWAY PATROL RETAINS ONLY ALPR HITS

The Ohio State Highway Patrol policy for automated license plate readers (ALPRs) states, "all 'non-hit' captures shall be deleted immediately." The ALPR program is intended to detect stolen vehicles, Amber Alerts, and persons with outstanding warrants. As a result, retaining data about "non-hit" vehicles does not further that purpose, and a policy of deleting that data immediately protects the community from unnecessary risks.[79]

2. *Prevent Misuse of Data: Limit When Data Can Be Used and Who Can Access It*

Even data collected for a legitimate purpose can be put to illegitimate uses. It is essential that your community establish clear rules so that surveillance data is used only for approved purposes. Doing so not only prevents outright abuses of the data that can erode public trust but also keeps "mission creep" from altering the balance that you have already worked out between government actions and individual liberties.

➢ *How will surveillance data be secured?*

The first step in preventing misuse of data is ensuring that it is stored securely. Technical safeguards are necessary to help protect community members' data from accidental disclosure and misuse. You should consult with experts and implement safeguards at multiple levels that protect data at all points in its lifespan.

Your community may already possess secure storage space separated from other databases and computer systems. This provides you with an obvious level of control. If you choose to store data elsewhere, you must ensure that it is secure and subject to your safeguards. Your community should also designate someone as an authority or custodian with responsibility over community members' data and your storage systems.

CASE STUDY: MONTEREY COUNTY SUFFERS DATA BREACH DUE TO "TOTALLY OBSOLETE" DATA PRACTICES

Monterey County's computer systems were breached in 2013 and the personal information of over 140,000 local residents was stolen. A subsequent grand jury investigation concluded that the breach stemmed from "totally obsolete" data practices and a failure to follow privacy laws. The grand jury warned of "serious financial consequences" if the county failed to change its practices.[80]

➢ *Under what circumstances can collected data be accessed or used?*

In addition to technical safeguards to protect data, you should also limit the circumstances under which it can be legitimately accessed or used. These limits should be based on the specific purposes your community agreed to when it adopted the technology. For example, if the purpose of the technology is to address specific violent crimes, your policy might allow database searches only as part of an official investigation of a violent crime, and only for data that is related to that investigation. Data access and use policies that are consistent with the articulated purposes for the system will provide guidance to operators and engender community trust by deterring abuses that can follow unfettered access to surveillance data.

Your community's goal of balancing privacy and security will be easier to achieve if particular data access and use limits are accompanied by steps to ensure the rules are followed. Database access should be limited — for example, by only allowing junior staff to access data with the permission and guidance of a more senior officer, or by limiting data access solely to senior officers. As explained earlier, training is a must. Restricting data access to a limited set of trained employees decreases the potential that community members' data can be misused. To ensure targeted use of data, it may be appropriate to require a search warrant or similar external process before the data can be accessed at all.

CASE STUDY: LAX POLICIES LEAD TO "LOVEINT" ABUSE

Without strong policies limiting access to data, the temptation to misuse government databases for personal interests can be hard to resist. The NSA even has a specific term, LOVEINT, for employees who monitor their significant others. Two Fairfield, CA, officers could face criminal charges after using a statewide police database to screen women from online dating sites.[81]

➢ *What limits exist on sharing data with outside entities?*

Placing limits on how data use is a great step, but third parties that receive the collected data may not have the same limits in place. To protect residents' privacy and prevent uses of information contrary to community desires, it is important to articulate when — if ever — the technology's purposes justify sharing any collected information. During the public debate over your Surveillance Use Policy, the community should decide when sharing is permissible and when it is prohibited.

If data can be shared, your community must also determine how to ensure that the entity receiving the data lives up to your community's standards. This may require contractual language binding the third party to your data policies and safeguards. For example, the city of Menlo Park, California, specifically requires by ordinance that any agreement with Northern California's fusion center demand compliance with the City's own retention policy.[82] If a potential recipient of your data cannot agree with your policies or conditions, the best choice is to not share your data.

3. LIMIT DATA RETENTION: KEEP INFORMATION ONLY AS LONG AS NECESSARY

The longer you retain information, the greater the potential privacy and security risks. The easiest way to minimize these risks is to retain only necessary information and to delete it after the purpose for its collection is achieved.

➢ *Does retaining data help accomplish the purpose for which the technology was acquired?*

To maximize the usefulness of your technology and minimize civil liberties concerns, a retention period should not be longer than necessary to directly advance community purposes. For instance, deploying automated license plate readers to locate stolen or Amber Alert vehicles is not aided by the collection of historical data. Retaining data "just in case it becomes useful" increases the risk that data will be used contrary to the purpose agreed upon by the community or wind up in the hands of a bad actor. Retaining data can also increase the costs of surveillance by requiring expensive storage solutions and making it harder to effectively use the system. Focusing on the specific objective that surveillance is intended to accomplish can help you determine a retention period that balances that objective with the costs and risks associated with data retention.

> "If there's anything of a criminal nature recorded on video, it's grabbed and inventoried within hours. Most everything else is never looked at again, so it's purged automatically."
>
> Commander Steven Caluris, Chicago Police Department[83]

➢ *Are there other legal or policy reasons that inform your data retention policy?*

There may be other legal and policy issues that affect your data retention policy, informed by legal concerns unrelated to your community's purposes. For example, your community should choose a retention period that balances a desire to be responsive to public records requests with residents' civil liberties, including privacy. Responsiveness to records requests should not be a primary justification for an extended retention period, however, since community concerns about surveillance are better addressed by retaining less information in the first place.

➢ *What happens when the data retention period expires?*

To prevent misuse of data after your community's desired retention period has lapsed, ensure that data is regularly deleted after that time. This can be accomplished via automated technical measures or periodic audits.

Before data is collected, your community should also decide whether there are any specific circumstances that justify the retention of data beyond your community's chosen retention period. For instance, it might be appropriate to preserve data relevant to a specific ongoing investigation, data necessary to complete an investigation of internal data misuse, and data relevant to a criminal defendant's case. Any such conditions should be informed by your community's purposes and clearly articulated in your Surveillance Use Policy.

C. ENSURE ACCOUNTABILITY BY ENFORCING POLICIES AND ENCOURAGING ONGOING PUBLIC ENGAGEMENT

Even if your community has already deployed surveillance technology, the community as a whole has a crucial role in ensuring that the public interest is promoted through its use. One key question is whether your Surveillance Use Policy is effectively safeguarding individual rights and preventing abuses. A second is whether the assumptions you made when you approved surveillance in the first place still hold true after actual experience with the technology and its impact. Revamping or even cancelling an ineffective or imbalanced program is better than wasting time, money, and community trust on a tool that does more harm than good.

1. Identify and Address Abuses: Audit Use of Technologies and Data and Address Any Misuse

The safeguards in your Surveillance Use Policy are only worthwhile if the policy is actually followed. But given the secretive nature of many forms of surveillance, ensuring compliance takes conscious effort. Strong internal and external oversight and auditing can help identify isolated or systemic abuses of surveillance technology, and legally enforceable sanctions can deter both.

- *How are operators supervised?*

Personnel management and technical measures both facilitate internal oversight of your technology and data. Designating a chain of command for a given surveillance technology helps specific personnel understand what responsibilities they have over the equipment or data and makes it easy to trace where misuse occurred. All of this helps your community deter abuses and guarantee that resources are used wisely.

> "As stewards of the public's interests, we know the government doesn't get to simply say 'trust us' and carry on: we have to earn that trust on a daily basis. We have to be accountable and transparent…."
>
> Former Oakland Mayor Jean Quan[84]

- *How will misuses of the technology be identified?*

The best way to identify misuse of surveillance is to "watch the watchers" by keeping thorough records of each time surveillance is deployed or surveillance data is called up. The person or persons with oversight responsibility should be independent, given full access to the technology and database, and empowered to receive complaints about misuse and draw conclusions that can lead to legally enforceable consequences. To catch what human oversight misses, your community should ensure that technical measures including access controls and audit logs are in place. Placing the oversight authority with a third party such as the City Council or a citizen panel may also increase the likelihood that the misuses are accurately identified.

CASE STUDY: FRESNO ADOPTS ANNUAL AUDIT OF VIDEO SURVEILLANCE

When the Fresno Police Department proposed a citywide video-policing program using live-feed cameras, the city council required an annual independent audit to ensure that all of the privacy and security guidelines for the system's use were being followed. Fresno Police Chief Jerry Dyer said he supported the audit: "I have no doubt the audit will be very helpful to our ongoing video policing operations." The city appointed a retired federal district court judge as auditor, who then examined current use of the system and made specific policy recommendations.[85]

- *What legally enforceable sanctions exist to deter misuse and abuse of this technology?*

By establishing consequences for violations of the guidelines, your community encourages proper use of the technology and sends a message that community values apply to everyone. Depending on the circumstances, sanctions ranging from retraining to fines, suspensions, or termination may be appropriate for violations of your Surveillance Use Policy. In addition, your community should provide an appropriate remedy for anyone harmed by an abuse. Legally enforceable sanctions discourage misuse and guarantee that aggrieved community members will be made whole.

2. KEEP THE DIALOG OPEN: ENCOURAGE PUBLIC OVERSIGHT AND ONGOING DISCUSSION

Community oversight and feedback plays two essential roles in ensuring that any current surveillance program actually benefits your community. First, transparency about abuses of surveillance allows the community to determine whether the Surveillance Use Policy or any associated sanctions need to be revised to address the issue. Second, as your community learns first-hand whether surveillance is effective and how it impacts different individuals and groups, you may wish to reassess the purposes for which surveillance should be used or even whether it should still be used at all. Surveillance should be under the control of the community at all times, not just when it is initially being considered.

- *How will the community continue to be informed about the surveillance program?*

It is important that your community's oversight mechanisms not only are in place before surveillance is used but also remain available as long as the surveillance program continues or any collected data remains. This allows the community to continue to learn about and provide feedback on the effectiveness and impact of surveillance, and provides the information you will need to evaluate any changes going forward.

One of the most effective ways to keep your community informed is to produce an annual report about each surveillance technology that has been used in the past year. This report should include:

- A description of how and how often the technology was used;
- Information, including crime statistics, that indicate whether the technology was effective at accomplishing its stated purpose;
- A summary of community complaints or concerns about the technology;
- Information about any violations of the Surveillance Use Policy, data breaches, or similar incidents, including the actions taken in response, or results of any internal audits;
- Whether and how data acquired through the use of the technology was shared with any outside entities;
- Statistics and information about Public Records Act requests, including responses; and
- The total annual costs for the technology, including personnel and other ongoing costs, and any external funding available to fund any or all of those costs in the coming year.

In addition, there may be other ways to provide your community with information about the operation and effectiveness of the surveillance program. Responding to Public Records Act requests with as much information as possible, taking into account factors such as the privacy rights of individuals whose information may be included in the requested data, is one way to allow interested community members access to concrete information about the program. Creating standing committees of community members, regularly holding public events and forums, and establishing open inspection periods for the technology can also help keep the community informed.

- *How will local officials and the public re-evaluate the decision to engage in surveillance or the existing policies and safeguards?*

The community's decision to approve surveillance should be reconsidered on an annual basis. If there is evidence that calls into question the conclusion that the benefits of surveillance outweigh costs and concerns, or that there are better ways to achieve the same purpose with fewer costs or risks, policymakers should seek community input and take whatever action is appropriate to address these concerns. That may involve narrowing the purpose or scope of surveillance, requiring modifications to the Surveillance Use Policy, or exploring alternatives that better address community needs.

Conclusion

Communities increasingly understand the need to make smart choices about surveillance technology and ensure that time, energy, and resources are not spent on systems that cost more, do less, and threaten the rights of community members. Community members demand — and deserve — a voice in any decisions about surveillance technology. Proper transparency, accountability, and oversight must be the rule in considering any surveillance technology proposal. We hope the recommendations in this guide help you work to enact local and state policies to ensure consistent public process each time surveillance technology is considered.

Appendix: Model Surveillance & Community Safety Ordinance

A. KEY PRINCIPLES OF THE MODEL ORDINANCE

- **Informed Public Debate at Earliest Stage of Process**: Public notice, distribution of information about the proposal, and public debate prior to seeking funding or otherwise moving forward with surveillance technology proposals.
- **Determination that Benefits Outweigh Costs and Concerns**: Local leaders, after facilitating an informed public debate, expressly consider costs (fiscal and civil liberties) and determine that surveillance technology is appropriate or not before moving forward.
- **Thorough Surveillance Use Policy**: Legally enforceable Surveillance Use Policy with robust civil liberties, civil rights, and security safeguards approved by policymakers.
- **Ongoing Oversight & Accountability**: Proper oversight of surveillance technology use and accountability through annual reporting, review by policymakers, and enforcement mechanisms.

B. MODEL ORDINANCE TEXT

The [Council/Board of Supervisors] finds that any decision to use surveillance technology must be judiciously balanced with the need to protect civil rights and civil liberties, including privacy and free expression, and the costs to [City/County]. The [Council/Board] finds that proper transparency, oversight, and accountability are fundamental to minimizing the risks posed by surveillance technologies. The [Council/Board] finds it essential to have an informed public debate as early as possible about whether to adopt surveillance technology. The [Council/Board] finds it necessary that legally enforceable safeguards be in place to protect civil liberties and civil rights before any surveillance technology is deployed. The [Council/Board] finds that if surveillance technology is approved, there must be continued oversight and annual evaluation to ensure that safeguards are being followed and that the surveillance technology's benefits outweigh its costs.

NOW, THEREFORE, BE IT RESOLVED that the [Council/Board] of [City/County] adopts the following:

Section 1. Title

This ordinance shall be known as the Surveillance & Community Safety Ordinance.

Section 2. [Council/Board] Approval Requirement

1) A [City/County] entity must obtain [Council/Board] approval at a properly-noticed public hearing prior to any of the following:
    a) Seeking funds for surveillance technology, including but not limited to applying for a grant or soliciting or accepting state or federal funds or in-kind or other donations;
    b) Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
    c) Using new surveillance technology, or using existing surveillance technology for a purpose, in a manner or in a location not previously approved by the [Council/Board]; or
    d) Entering into an agreement with a non-[City/County] entity to acquire, share or otherwise use surveillance technology or the information it provides.
2) A [City/County] entity must obtain [Council/Board] approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (1)(b)-(d).

Section 3. Information Required

1) The [City/County] entity seeking approval under Section 2 shall submit to the [Council/Board] a Surveillance Impact Report and a proposed Surveillance Use Policy at least forty-five (45) days prior to the public hearing.
2) The [Council/Board] shall publicly release in print and online the Surveillance Impact Report and proposed Surveillance Use Policy at least thirty (30) days prior to the public hearing.

Section 4. Determination by [Council/Board] that Benefits Outweigh Costs and Concerns

The [Council/Board] shall only approve any action described in Section 2, subsection (1) of this ordinance after making a determination that the benefits to the community of the surveillance technology outweigh the costs and that the proposal will safeguard civil liberties and civil rights.

Section 5. Compliance for Existing Surveillance Technology

Each [City/County] entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a proposed Surveillance Use Policy no later than ninety (90) days following the effective date of this ordinance for review and approval by [Council/Board]. If such review and approval has not occurred within sixty (60) days of the submission date, the [City/County] entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 6. Oversight Following [Council/Board] Approval

1) A [City/County] entity which obtained approval for the use of surveillance technology must submit a Surveillance Report for each such surveillance technology to the [Council/Board] within twelve (12) months of [Council/Board] approval and annually thereafter on or before November 1.
2) Based upon information provided in the Surveillance Report, the [Council/Board] shall determine whether the benefits to the community of the surveillance technology outweigh the costs and whether civil liberties and civil rights are safeguarded. If the benefits do not outweigh the costs or civil rights and civil liberties are not safeguarded, the [Council/Board] shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve the above concerns.
3) No later than January 15 of each year, the [Council/Board] shall hold a public meeting and publicly release in print and online a report that includes, for the prior year:
    a. A summary of all requests for [Council/Board] approval pursuant to Section 2 or Section 5, including whether the [Council/Board] approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval; and
    b. All Surveillance Reports submitted.

Section 7. Definitions

The following definitions apply to this Ordinance:

1) "Surveillance Report" means a written report concerning a specific surveillance technology that includes all of the following:
    a. A description of how the surveillance technology was used;
    b. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
    c. A summary of community complaints or concerns about the surveillance technology;

d. The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
e. Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
f. Statistics and information about public records act requests, including response rates; and
g. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

2) "[City/County] entity" means any department, bureau, division, or unit of the [City/County].
3) "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group.
4) "Surveillance Impact Report" means a publicly released written report including at a minimum the following: (a) Information describing the surveillance technology and how it works, including product descriptions from manufacturers; (b) information on the proposed purposes(s) for the surveillance technology; (c) the location(s) it may be deployed and crime statistics for any location(s); (d) an assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public; and (e) the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.
5) "Surveillance Use Policy" means a publicly released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:
    a. **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance.
    b. **Authorized Use:** The uses that are authorized, the rules and processes required prior to such use, and the uses that are prohibited.
    c. **Data Collection:** The information that can be collected by the surveillance technology.
    d. **Data Access:** The individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.
    e. **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms.
    f. **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.
    g. **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants.
    h. **Third Party Data Sharing:** If and how other [City/County] or non-[City/County] entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.
    i. **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials.
    j. **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

Section 8. Enforcement

1) Any violation of this Ordinance constitutes an injury, and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance.
2) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought to enforce this Ordinance.
3) In addition, for a willful, intentional, or reckless violation of this Ordinance, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding $1,000 per violation, imprisonment in the county jail for not more than six months, or both such a fine and imprisonment.

Section 9. Severability

The provisions in this Ordinance are severable. If any part or provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 10. Effective Date

This Ordinance shall take effect on [DATE].

Endnotes

[1] For example, the San Francisco Police Department's Mission Statement states that "policing strategies must preserve and advance democratic values" and that "police must respect and protect the rights of all citizens as guaranteed by the state's Constitution." Police Department, Mission Statement, http://sf-police.org/index.aspx?page=1616.
[2] B.T. Lewis & Taymeh Jahsi, *Stop using social media to monitor south Fresno's protesters*, The Fresno Bee, Feb. 10, 2016, *available at* http://www.fresnobee.com/opinion/readers-opinion/article59388976.html.
[3] Matt Cagle. *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU of Northern California (Dec. 15, 2015), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter.
[4] *See* Press Release, Leadership Conference, Civil Rights Principles for the Era of Big Data, http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html.
[5] Terrence O'Brien, *Caught Spying on Student, FBI Demands GPS Tracker Back*, Wired.com, Oct. 7, 2010, http://www.wired.com/2010/10/fbi-tracking-device/.
[6] Michael Isikoff, *FBI Tracks Suspects' Cell Phones Without* a Warrant, Newsweek, Feb, 18, 2010 (updated Mar. 13, 2010), *available at* http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099.
[7] David Kravets, *Rights Groups Decry New NSA Leak: Snooping on Muslim-Americans' E-mail*, Ars Technica (July 9, 2014), http://arstechnica.com/tech-policy/2014/07/rights-groups-decry-new-nsa-leak-snooping-on-muslim-americans-e-mail/.
[8] Matt Apuzzo and Al Baker, *New York to Appoint Civilian to Monitor Police's Counterterrorism Activity*, N.Y. Times, Jan. 7, 2016, *available at* http://www.nytimes.com/2016/01/08/nyregion/new-york-to-appoint-monitor-to-review-polices-counterterrorism-activity.html; Case page, Raza v. City of New York – Legal Challenge to NYPD Muslim Surveillance Program, Jan. 7, 2016, https://www.aclu.org/cases/raza-v-city-new-york-legal-challenge-nypd-muslim-surveillance-program.
[9] *See* Tanvir v. Holder, Case No. 13-CV-6951 (S.D. N.Y. Apr. 22, 2014) (First Amended Complaint), *available at* http://apps.washingtonpost.com/g/documents/world/lawsuit-accusing-us-of-putting-people-on-no-fly-list-after-they-say-they-wont-spy/941/.
[10] George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, The Intercept, July 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.
[11] Matt Cagle. *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU of Northern California (Dec. 15, 2015), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter; *see also* Shaun King, *Fresno police join group of officials monitoring #BlackLivesMatter hashtag, labeling a peaceful movement a threat*, N.Y. Daily News, Dec. 17, 2015, *available at* http://www.nydailynews.com/news/national/king-monitoring-blacklivesmatter-labels-movement-threat-article-1.2468808.
[12] David Rogers, *Black Lives Matter Supporters in Oregon Targeted by State Surveillance*, ACLU Speak Freely blog, Nov. 11, 2015, https://www.aclu.org/blog/speak-freely/black-lives-matter-supporters-oregon-targeted-state-surveillance; Courtney Sherwood, *Oregon attorney general 'appalled' by probe of Black Lives Matter*, Reuters, Nov. 11, 2015, http://www.reuters.com/article/us-oregon-race-idUSKCN0T104N20151112.
[13] Jeremy Gillula and Dave Maass, *What You Can Learn from Oakland's Raw ALPR Data*, Electronic Frontier Foundation, Jan. 21, 2015, https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.
[14] Angel Jennings, *Richard Winston & James Rainey, Sherriff's Secret Air Surveillance of Compton Sparks Outrage*, L.A. Times, Apr. 23, 2014, *available at* http://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html.
[15] Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, Wash. Post, Aug. 24, 2013, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/.
[16] *See* Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, Wall St. J., Sep. 29, 2012, *available at* http://online.wsj.com/news/articles/SB10000872396390443995604578004723603576296.
[17] Jenna McLaughlin, *The FBI v. Apple Debate Just Got Less White*, The Intercept, Mar. 8, 2016, https://theintercept.com/2016/03/08/the-fbi-vs-apple-debate-just-got-less-white/.
[18] Rania Khalek, *Activists of Color Lead Charge Against Surveillance, NSA*, Truthout, Oct. 30, 2013, http://www.truth-out.org/news/item/19695-activists-of-color-at-forefront-of-anti-nsa-movement.
[19] Riley v. California, 134 S. Ct. 2473, 2489 (2014).
[20] *United States v. Jones*, 132 S.Ct. 945, 955, 56 (2012).

[21] Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, Huffington Post (Feb 25, 2012), http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html; Adam Goldman & Matt Apuzzo, *New York Drops Unit That Spied on Muslims*, N.Y. Times, April 15, 2014, *available at* http://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html.
[22] Hina Shamsi and Ramzi Kassem, *The NYPD spied on Muslim Americans. Will a court settlement change anything?*, The Guardian, Jan. 8, 2016, http://www.theguardian.com/commentisfree/2016/jan/08/nypd-spied-muslim-americans-will-court-settlement-bring-change.
[23] Angel Jennings, Richard Winston & James Rainey, *Sherriff's Secret Air Surveillance of Compton Sparks Outrage*, L.A. Times, Apr. 23, 2014, *available at* http://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html.
[24] *Police Executive Research Forum, How Are Innovations in Technology Transforming Policing?* 26 (Jan. 2012) [hereinafter PERF Report], *available at* http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.
[25] Press Release, Office of the Controller, *Butkovitz Alarmed by Police Camera Program*, June 20, 2012, http://www.philadelphiacontroller.org/page.asp?id=792.
[26] *See* Fazaga v. FBI, 844 F.Supp.2d 1022 (C.D. Cal. 2012).
[27] Adam Goldman, *NYPD settles lawsuits over Muslim monitoring*, Wash. Post, Jan. 7, 2016, *available at* https://www.washingtonpost.com/world/national-security/nypd-settles-lawsuits-over-muslim-monitoring/2016/01/07/bdc8eb98-b3dc-11e5-9388-466021d971de_story.html.
[28] *See* Tim Cushing, *Another Bogus Hit from a License Plate Reader Results in Another Citizen Surrounded by Cops with Guns Out*, TechDirt (May 23, 2014), https://www.techdirt.com/articles/20140513/07404127218/another-bogus-hit-license-plate-reader-results-another-citizen-surrounded-cops-with-guns-out.shtml.
[29] Symposium, *The Value of Privacy*, U. Cal.-Hastings School of L. Const. L. Q., Apr. 7, 2014 (oral remarks), *available at* http://livestre.am/4P7Lk.
[30] Cal. Civil Code § 1798.29 (2014).
[31] Larry Ponemon, *Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis,'* May 27, 2015, https://securityintelligence.com/cost-of-a-data-breach-2015/.
[32] Will Kane, *Oakland to Limit Surveillance Center to Port, Airport*, S.F. Gate, Mar. 6, 2014, *available at* http://www.sfgate.com/bayarea/article/Oakland-to-limit-surveillance-center-to-port-5290273.php.
[33] Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/.
[34] Press Release, *San Jose Police Provide Statement Regarding Purchase of Unmanned Aerial System (UAS)*, San Jose Police Dept., Aug. 5, 2014, *available at* http://www.sjpd.org/iNews/viewPressRelease.asp?ID=1874.
[35] Robert Salonga, *San Jose: Police apologize for drone secrecy, promise transparency*, San Jose Mercury News, Aug. 5, 2014, *available at* http://www.mercurynews.com/crime-courts/ci_26279254/san-jose-police-apologize-secret-drone-purchase-promise.
[36] *Riley v. California*, 573 U.S. (2014), Slip Op. at *28.
[37] U.S. v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, Ginsberg, Breyer, and Kagan, J., concurring in the judgment).
[38] Charlie Savage and Jonathan Wiseman, *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*, N.Y. Times, May 7, 2015, *available at* http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html; Klayman v. Obama, Civ. No. 13-0851 (D.D.C. Dec. 16, 2013).
[39] Ballot Pamplet., Proposed Amendments to Cal. Const. with Arguments to Voters, Gen. Elec. (Nov. 7, 1972).
[40] White v. Davis, 533 P.2d (Cal. 1975).
[41] People v. Cook 41 Cal. 3d 373 (1985).
[42] Robins v. Pruneyard Shopping Center, 592 P.2d 899 (Cal. 1979) (holding that, under the California Constitution, members of the public have a legal right to pass out pamphlets and seek signatures in a privately owned shopping center), *aff'd*, .447 U.S. 74 (1980).
[43] Cal. Penal Code §§ 1546-1546.4. *See generally* Tracy Seipel and Eric Kurhi, *California digital privacy laws boosted, protecting consumers from Big Brother, big business*, San Jose Mercury News, Oct. 9, 2015, *available at* http://www.mercurynews.com/health/ci_28948653/california-digital-privacy-laws-boosted-protecting-consumers-from.
[44] Cal. Gov't Code § 53166.
[45] Cal. Civil Code §§ 1798.29, 1798.82, and 1798.90.5.

[46] Jennifer Steinhauer and Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. Times, Jun. 2, 2015, *available at* http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html?_r=0; *see also* U.S.A. Freedom Act, H.R. 2048, 114th Cong. (2016).
[47] Allie Bohm, *Status of Location Privacy Legislation in the States*, ACLU Free Future (April 8, 2014), https://www.aclu.org/blog/technology-and-liberty-national-security/status-location-privacy-legislation-states (as of May 6, 2014).
[48] Allie Bohm, *Status of 2014 Domestic Drone Legislation in the States*, ACLU Free Future (April 22, 2014), https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states (as of May 6, 2014).
[49]*Smart About Surveillance*, ACLU of California, http://www.aclunc.org/smartaboutsurveillance.
[50] *Id.*
[51] Interview with Brian Hofer, *Transparency over secrecy: Oakland's surveillance policy*, KALW Local Public Radio, *available at* http://kalw.org/post/transparency-over-secrecy-oakland-s-surveillance-policy#stream/0.
[52] *See* Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, *available at* http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approves-ordinance-regulating-police-use; *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/.
[53] U.S. Dep't of Homeland Security, *CCTV: Developing Best Practices* (2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.
[54] *State of Surveillance in California – Findings and Recommendations,* ACLU of California, Jan. 2015, *available at* https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf.
[55] Redlands Police Department, Citizen Privacy Council, http://www.cityofredlands.org/police/CPC.
[56] Halima Kazen, *Watching the Watchers: Oakland Seeks Control of Law Enforcement Surveillance*, The Guardian, July 13, 2015, *available at* http://www.theguardian.com/us-news/2015/jul/13/oakland-law-enforcement-surveillance.
[57] Memorandum, *Establishing Ad Hoc Committee to Review the Community Warning System and Industrial Safety Ordinance* (Sept. 18, 2012), http://64.166.146.155/agenda_publish.cfm?mt=ALL&get_month=9&get_year=2012&dsp=agm&seq=12339&rev=0&ag=241&ln=23604&nseq=0&nrev=0&pseq=12303&prev=0.
[58] Keynote address of Malkia Cyril, *Targeted Surveillance, Civil Rights, and the Fight for Democracy*, Center for Media Justice, Oct. 13, 2015, *available at* http://centerformediajustice.org/2015/10/13/targeted-surveillance-civil-rights-and-the-fight-for-democracy/.
[59] *See* Memorandum, City Administrator's Weekly Report (Apr. 25, 2014), http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak046804.pdf.
[60] http://www2.oaklandnet.com/Government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm
[61] Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times, Mar. 15, 2015, *available at* http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0; Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/.
[62] Ali Winston, *Oakland City Council Rolls Back the Domain Awareness Center*, East Bay Express (Mar. 5, 2014), http://www.eastbayexpress.com/SevenDays/archives/2014/03/05/oakland-city-council-rolls-back-the-dac.
[63] Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/.
[64] John Malkin, *Surveillance City?* GoodTimes, Jan 29, 2014, http://www.gtweekly.com/index.php/santacruznews/goodtimescoverstories/5386surveillancecity.html.
[65] Robert Salonga, *San Jose: Police Apologize for Drone Secrecy, Promise Transparency*, San Jose Mercury News, Aug 5, 2014, *available at* http://www.mercurynews.com/crime-courts/ci_26279254/san-jose-police-apologize-secret-drone-purchase-promise.
[66] *See* Oakland City Auditor, *Police Technology Performance Audit: FY 2006–07 through 2010–11* (2012), *available at* http://www.oaklandauditor.com/images/oakland/auditreports/0pd%20tech.pdf.
[67] *See* Citris, *Cistris Study on SF Public Cameras Released* (Jan. 9, 2009), http://citris-uc.org/citris-study-on-sf-public-cameras-released/.
[68] *See* David P. Farrington & Brandon C. Welsh, *Effects of Improved Street Lighting on Crime: A Systematic Review,* Home Office Research Study 251 (Aug. 2002), p. 42; Ronald V. Clarke, U.S. Department of Justice, Office of Community Oriented Policing Services, *Improving Street Lighting to Reduce Crime in Residential Areas* (Dec. 2008), *available at* http://cops.usdoj.gov/Publications/e1208-StreetLighting.pdf; Jay Beeber, *Collision Analysis of the Photo Enforced Intersection in Walnut, CA*, http://www.thenewspaper.com/rlc/docs/2014/ca-walnut.pdf.
[69] *See* Steve Scauzillo, *Red Light Cameras Being Stopped*, L.A. Daily News (Jan. 21, 2014), http://www.dailynews.com/general-news/20140121/red-light-cameras-being-stopped.

[70] PERF Report, *supra* note 24, at 44.
[71] United States v. Jones, 132 S. Ct. 945 (2012); Joann Pan, *FBI Turns Off 3000 GPS Devices After Ruling*, Mashable (Feb. 27, 2012), http://mashable.com/2012/02/27/fbi-turns-off-3000-gps-devices/.
[72] Kashmir Hill, *Whoops, Anyone Could Watch California City's Police Surveillance Cameras*, Forbes.com (Aug. 21, 2014), http://www.forbes.com/sites/kashmirhill/2014/08/11/surveillance-cameras-for-all/.
[73] *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/; Jamela Debelak, ACLU of Washington, *Surveillance: Spokane Acts to Protect Privacy and Provide Transparency* (Aug. 21, 2013), https://aclu-wa.org/blog/surveillance-spokane-acts-protect-privacy-and-provide-transparency.
[74] Matt Cagle, *Alameda County Just Got a Privacy Upgrade – Alameda County, It's Your Move*, ACLU of Northern California blog, Nov. 17, 2015, https://www.aclunc.org/blog/california-just-got-privacy-upgrade-alameda-county-its-your-move.
[75] *State of Surveillance in California – Findings and Recommendations*, ACLU of California, Jan. 2015, *available at* https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf.
[76] Seattle City Council, Public Safety, Civil Rights and Technology Committee May 2, 2012, Seattle Channel, at 38:55, http://www.seattlechannel.org/mayor-and-council/city-council/20122013-public-safety-civil-rights-and-technology-committee/?videoid=x23397.
[77] Terry McFadden, *Technology Helping Police to Receive Warrants Faster*, WNDU.com (July 8, 2013), http://www.wndu.com/news/specialreports/headlines/Technology-helping-police-to-receive-search-warrants-faster--214651051.html.
[78] 18 U.S.C. § 2518(5) (2014).
[79] Ohio State Highway Patrol Policy No. OSP-103.29 (revised Dec. 23, 2008).
[80] Julia Reynolds, *Monterey County Grand Jury Finds Computer Data Risks*, Monterey Herald, Aug. 21, 2014, *available at* http://www.montereyherald.com/news/ci_26009592/monterey-county-grand-jury-finds-computer-data-risks.
[81] Dianne Feinstein, *NSA Officers Spy on Love Interests*, Wall St. J., Aug. 23, 2013, *available at* http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/; Anjali Hemphill, *Dating on Duty: Officers Accused of Screening Dates Using Police System*, CBS 13 Sacramento (Aug. 22, 2014), http://sacramento.cbslocal.com/2014/08/22/dating-on-duty-officers-accused-of-screening-dates-using-police-system/.
[82] *See* Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, *available at* http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approves-ordinance-regulating-police-use.
[83] PERF Report, *supra* note 24, at 36.
[84] Dan Brekke, *Oakland Approves Scaled-Back Version of Disputed Surveillance Center,* KQED.com, Mar. 5, 2014, http://ww2.kqed.org/news/2014/03/04/oakland-mayor-jean-quan-suggests-scaling-back-domain-awareness-center.
[85] George Hostetter, *Former Judge Wanger Writes Far-Ranging Audit on Fresno Video Policing*, Fresno Bee, Jan. 7, 2014, *available at* http://www.fresnobee.com/2014/01/07/3701754/judge-wanger-delivers-impressive.html.

Back Cover Citations

Editorial, *ACLU offers a smart safeguard for using surveillance technology*, The Los Angeles Times, Nov. 23, 2014, *available at* http://www. latimes.com/opinion/editorials/la-ed-surveillance-and-privacy-20141123-story.html.

Editorial, *Bay Area governments must protect citizen privacy*, San Francisco Chronicle, Feb. 25, 2015, *available at* http://www.sfchronicle. com/opinion/editorials/article/Bay-Area-governments-must-protect-citizen-privacy-6101993.php.

Steven Greenhut, *Surveillance is sneaking its way into cities*, The San Diego Union-Tribune, Nov. 17, 2014, *available at* http://www.sandiegouniontribune.com/news/2014/nov/17/surveillance-sneaking-cities-model-ordinance-aclu/.

Editorial, *ACLU push for surveillance policy is timely*, San Jose Mercury News, Nov. 13, 2014, *available at* http://www.mercurynews.com/ opinion/ci_26932183/mercury-news-editorial-aclu-push-surveillance-policy-is.

Police are spending billions of dollars on very sophisticated and invasive surveillance technology. Too many of these programs are moving forward without public conversation, careful consideration of the costs and benefits, or adequate policies in place to prevent misuse and protect rights.

This guide provides a step-by-step framework to ask and answer the right questions about surveillance proposals and build in proper mechanisms for transparency, accountability, and oversight. The guide also includes dozens of case studies highlighting smart approaches and missteps to avoid and model language for policymakers to adopt to make sure the right process is used every time a surveillance proposal is considered.

"The ACLU's approach to vetting new technologies is so pragmatic that cities, counties and law enforcement agencies throughout California would be foolish not to embrace it."
–Editorial, Los Angeles Times

"We urge more city and county governments to…[study] an ordinance that would set specific rules about what can be done with citizens' private information."
–Editorial, San Francisco Chronicle

"It's easy to see the value in [ACLU's] approach—in all areas of government..."
–Steven Greenhut, San Diego Union-Tribune

"Elected leaders, not police departments, should set policy for the use of surveillance equipment. This is the ACLU recommendation. It's also common sense. "
–Editorial, San Jose Mercury News

ACLU
AMERICAN CIVIL LIBERTIES UNION of CALIFORNIA