11-2014

Making Smart Decisions About Surveillance: A Guide for Communities

Chris Conley

Matthew Cagle

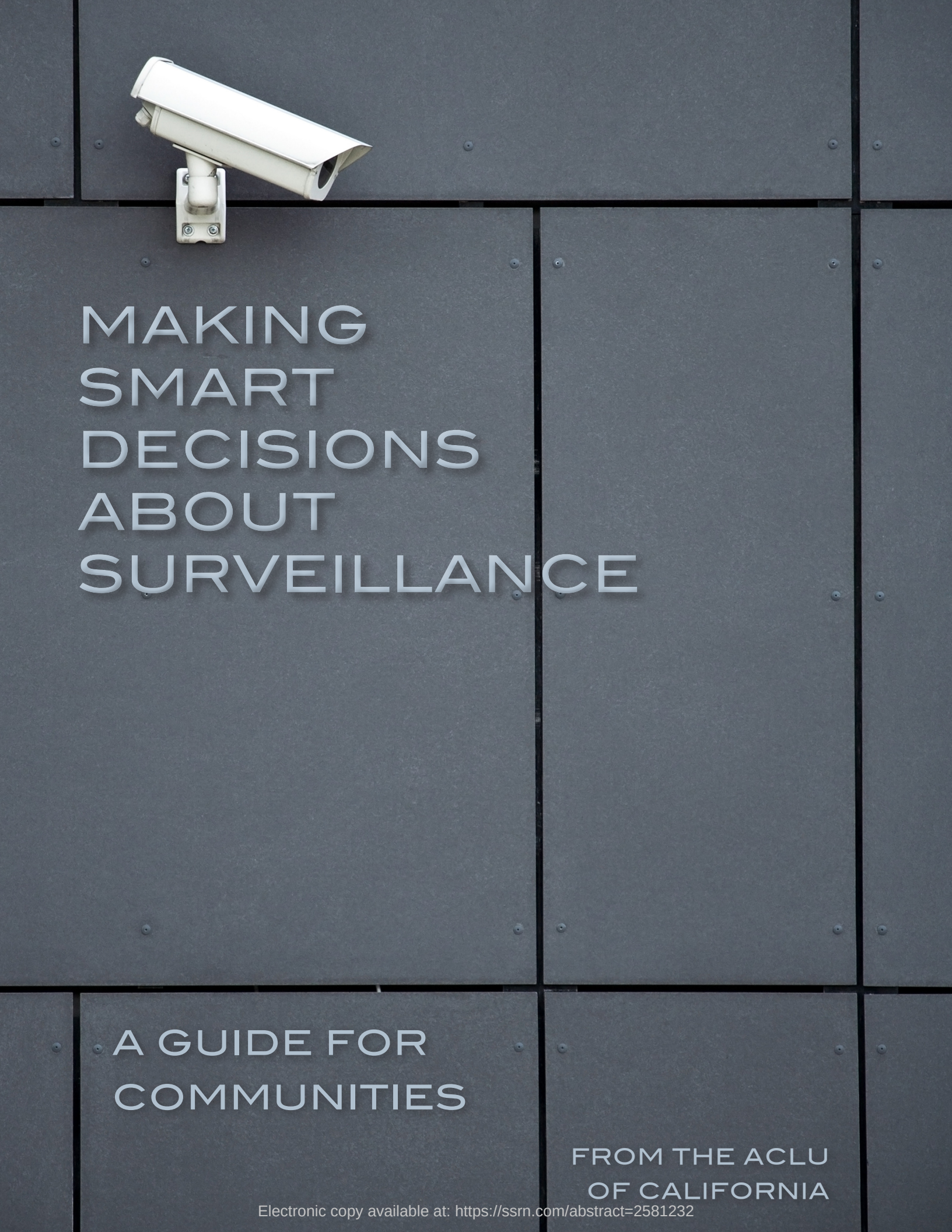
Peter Bibring

Jessica Farris

Linda Lye

See next page for additional authors

Authors
Chris Conley, Matthew Cagle, Peter Bibring, Jessica Farris, Linda Lye, Mitra Ebadolahi, and Nicole Ozer



MAKING SMART DECISIONS ABOUT SURVEILLANCE

A GUIDE FOR COMMUNITIES

FROM THE ACLU OF CALIFORNIA

California communities are increasingly grappling with whether to deploy new surveillance technologies ranging from drones to license plate readers to facial recognition. This is understandable, since public safety budgets are tight, technology vendors promise the ability to do more with less, and federal agencies or industry sponsors may even offer funding.

But surveillance can be both less effective and far more costly to local agencies and to the community at large than initially imagined, leaving communities saddled with long-term bills for surveillance that doesn't end up making the community safer. Surveillance can also be easily misused, leading to the erosion of community trust, bad press, and even costly lawsuits.

In the wake of the revelations about the National Security Agency's rampant warrantless spying and the use of military equipment in Ferguson, Missouri to quell protests, communities are increasingly focused on the need for greater transparency, oversight, and accountability of surveillance and local policing. More than ever, people are aware of how billions of dollars in federal funding and equipment provided directly to law enforcement is circumventing normal democratic processes and preventing communities from thoroughly evaluating the costs and risks of surveillance. As a result, many community leaders and residents are no longer willing to heed local law enforcement's call to "just trust us."

Instead, leaders and residents want 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 — before taking any steps to seek funding or acquire or deploy surveillance technology. They also want to craft robust rules to ensure proper use, oversight, and accountability if surveillance is used. Unfortunately, few resources exist to help communities make thoughtful decisions about surveillance. That's where this document comes in.

This first-of-its-kind guide provides step-by-step assistance to help communities ask and answer the right questions about surveillance. It includes case studies highlighting smart approaches and missteps to avoid. Because each community and each type of surveillance may present a different set of issues, there is no one-size-fits-all solution. Instead, this guide gives communities a flexible framework that policymakers, community members and law enforcement should use to properly evaluate a wide array of surveillance technologies and develop policies that provide transparency, oversight, and accountability. It also includes a Surveillance & Community Safety Ordinance that communities should adopt to ensure that the right process is followed every time.

We hope you will find this document and its supporting materials (available online at **aclunc.org/smartaboutsurveillance**) useful in making informed decisions about surveillance that recognize and address the costs, risks, and alternatives.

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

Peter Bibring
Police Practices Director
ACLU of California

Electronic copy available at: http://ssrn.com/abstract=2581232

CONTENTS

Authors: Chris Conley, Matthew Cagle, Peter Bibring, Jessica Farris, Linda Lye, Mitra Ebadolahi and Nicole Ozer, ACLU of California

Contributing Writers: Addison Litton & Thomas Mann Miller

Design & Layout: Gigi Pandian & Daniela Bernstein

Printing: InkWorks Press

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

PUBLISHED BY THE ACLU OF CALIFORNIA
NOVEMBER 2014

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

At first glance, surveillance technology may seem like an attractive way to increase public safety while decreasing the costs associated with policing, especially if potentially supported by outside funding. However, surveillance often has unexpected costs, including the expense of installing and maintaining equipment, the practical effect on law enforcement's ability to work with individuals who feel unfairly singled out, the impact on the rights of community members, and the potential for legal headaches as courts and legislatures continue to grapple with issues related to surveillance. Your community needs to identify and assess all of the costs of surveillance as early in the consideration process as possible in order to determine whether surveillance technology really is the right choice.

A. SURVEILLANCE CARRIES BOTH IMMEDIATE AND ONGOING FINANCIAL COSTS

The fiscal impact of surveillance can far exceed initial purchase prices for equipment. 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.[1] Surveillance technologies may also fail or be misused, resulting in costly lawsuits. Looking beyond the sticker price is essential.

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

The hidden costs of infrastructure, training and staffing, operations, and maintenance 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 fail 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."[3] 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[2]

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

Surveillance can carry a number of legal risks. Programs that fail to include proper safeguards for freedom of expression, association, and religion, or that inadequately enforce such safeguards, can lead to expensive litigation. 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.[4] Even technical glitches can create the potential for costly lawsuits and other expenses: the City of San Francisco is still 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.[5]

The collection of surveillance data also creates the risk of data breach liability. Even following best practices (which itself can entail significant expense) is not enough to prevent every breach. California law now requires that a local agency notify residents about a security breach.[6] And the fiscal costs of a breach of sensitive surveillance data could be very high: a 2012

> Under California Civil Code § 1798.29, local government agencies are required to notify affected individuals in the result of a data breach.

report found that companies spent an average of $5.5 million to resolve a data security breach.[7] The more information your community collects and retains, the greater the risk and potential cost of a breach.

3. *Funds Spent on Surveillance May Be Wasted Due to Community Backlash*

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 have to be suspended or even cancelled.

> "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, Oakland Emergency Services Coordinator[8]

Oakland was forced to scrap most of the planning for its Domain Awareness Center and scale the project back considerably after community members protested the misleading mission statement and lack of transparency for the project.[9] Engaging with the community before deciding whether to go forward with a surveillance proposal can help your community avoid a similar mistake.

B. SURVEILLANCE CARRIES COSTS FOR THE COMMUNITY AS A WHOLE

The community at large may also pay a heavy price if surveillance technology is acquired and deployed without public evaluation of the risks to the community and strong safeguards to prevent misuse. Surveillance can easily intrude upon the rights of residents and visitors if it is used, or creates the perception that it may be used, to monitor individuals and groups exercising their rights to freedom of expression, association, and religion — freedoms that public officials are sworn to protect.[10] In addition, surveillance can erode trust in law enforcement, making it harder for officers and community members to work together to keep the community safe.

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

Unfortunately, there are many examples demonstrating how readily surveillance can be misused to target individuals based on their 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.[11] Police in Michigan sought "information on all the cell phones that were congregating in an area where a labor-union protest was expected."[12] The NSA specifically monitored the email of several prominent Muslim-Americans with no evidence whatsoever of wrongdoing.[13] And in Germany, drones that were supposed to be used only for traffic monitoring and for serious kidnapping situations were later used to monitor an anti-nuclear protest.[14]

> "It is essential that big data analysis conducted by law enforcement outside the context of predicated criminal investigations be deployed with appropriate protections for individual privacy and civil liberties. The presumption of innocence is the bedrock of the American criminal justice system. To prevent chilling effects to Constitutional rights of free speech and association, the public must be aware of the existence, operation, and efficacy of such programs."
>
> "Big Data: Seizing Opportunities, Preserving Values" (White House Report)[15]

Surveillance programs that do not focus on individual targets can be particularly problematic. "Dragnet" surveillance of the entire public creates the potential for all sorts of abuse, from NSA analysts tracking romantic partners[16] to a Washington, D.C. police lieutenant blackmailing patrons of a gay bar.[17] And surveillance targeted at specific groups, such as members of a religious congregation or attendees at a political rally or gun show, can discourage participation in community activities and alienate the group from the rest of

the community. Even if specific members of the group are legitimate targets of investigation, tracking the entire group extends "guilt by association" to those who have done nothing wrong. 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, such as placement on the No-Fly List, if they do not cooperate with additional surveillance efforts.[18]

SURVEILLANCE AND POLITICAL ACTIVISM

In an age when surveillance is often justified by the need to combat terrorism, it's easy to forget that police across the U.S. have a long history of conducting surveillance on political activists, from the "Red Squads" dedicated to disrupting communist groups in the early 20th century to COINTELPRO and other efforts by the police and FBI to infiltrate and discredit the antiwar and civil rights movements in the 1950s, 60s and 70s. In fact, California has seen a long list of such abuses in its recent history:

- The California Office of Homeland Security collected detailed information about political demonstrations, including a rally outside a Canadian consulate office in San Francisco to protest seal hunting, a demonstration in Walnut Creek at which government officials spoke against the war in Iraq, and a Women's International League for Peace and Freedom gathering at a courthouse in support of a 56-year-old Salinas woman facing federal trespassing charges.[19]
- Local police have monitored peaceful political events, including a Code Pink antiwar protest on Mother's Day[20] and even a lecture on veganism at Cal State Fresno.[21]
- Undercover Oakland police officers infiltrated a group planning a peaceful protest against police brutality and even took a leadership role in directing the course of the march.[22]
- Santa Cruz police officers infiltrated planning meetings for a proposed alternative New Year's Eve march, leading to a media firestorm and a report from the Santa Cruz police auditor concluding that the department "violated … [parade] organizers' rights to privacy, freedom of speech and freedom of assembly."[23]

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 good reason to suspect that a particular individual is or has been involved criminal activity. There need to be similar restrictions on the use of surveillance technology to ensure that it is not used to chill or undermine political activism.

Just the perceived threat of surveillance has the potential to harm community members by discouraging political advocacy, efforts to seek counseling about reproductive choices, avenues to explore one's sexuality, and other activities that are clearly protected by the federal and California constitutions. Most recently, in the wake of the revelations of NSA surveillance, research has shown that Internet users are less likely to use search engine terms that they believed might "get them in trouble with the government."[24]

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."[25] 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."[26]

2. *Surveillance Can Erode Trust in Law Enforcement*

The use of surveillance can also reinforce justified concerns of profiling and discrimination, particularly in communities that have historically faced similar issues. Failing to fully engage with community members about the impact of surveillance — or, worse, skirting the democratic process by acquiring and deploying surveillance technology without public discussion at all — can erode trust even further, making it even harder for law enforcement officers to work with the community to solve crimes and protect public safety. Compton police learned this lesson the hard way: after news of an aerial surveillance program that was intentionally kept "hush-hush" broke, both citizens and lawmakers reacted negatively to the secrecy, with the mayor calling for a "citizen private protection policy" ensuring that the community would be notified before any new surveillance equipment was deployed or used.[27]

This fear that surveillance could be used in a discriminatory fashion is well-founded. 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 and compiled dossiers about Muslim-Americans engaging in constitutionally protected activities in cafes, bookstores, and private residences with no evidence of illegal activity.[28] And 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.'"[29] Acquiring and using surveillance technologies without recognizing these concerns can reinforce distrust of law enforcement, hindering rather than aiding the protection of public safety.

In a recent report, *Civil Rights Principles in an Era of Big Data,* fourteen civil and human rights groups highlighted the potential disparate impact of data collection on marginalized communities and called for technology to "be designed and used in ways that respect the values of equal opportunity and equal justice." The report called for an end to high-tech profiling and efforts to safeguard constitutional principles.[30]

C. SURVEILLANCE FACES INCREASED SCRUTINY FROM PUBLIC OFFICIALS

Public officials are increasingly tackling issues related to surveillance. There is broad, bipartisan political support for surveillance reform in both D.C. and at the state level, and courts are frequently grappling with cases involving surveillance technology. When evaluating a surveillance proposal, your community needs to consider the potential for legal change and the policy and individual rights concerns that are driving that change.

One of the most dramatic shifts in the legal landscape has been an increasing recognition that legal protections for individual rights must take into account the impact of modern technology. As a result, a majority of the Supreme Court has suggested that using technology to track an individual's location — even in public — over an extended period of time triggers constitutional scrutiny.[31] Similarly, a federal judge declared the NSA's warrantless collection of telephone metadata unconstitutional, criticizing its "almost Orwellian" scope.[32] 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.

"GPS monitoring — by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track — may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"

United States v. Jones (Sotomayor, J., concurring)[33]

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.[34] 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,[35] as did warrantless aerial surveillance of a resident's backyard.[36] Californians' right to free expression also extends outside of the home, even to privately-owned areas like shopping centers.[37]

There are also bipartisan legislative efforts to rein in surveillance at the federal and state level. Federal lawmakers are evaluating proposals aimed at reining in the NSA[38] and updating the Electronic Communications Privacy Act.[39] As of October 2014, 6 states have enacted laws restricting law enforcement access to location information, with 14 other states considering similar legislation.[40] 43 states have introduced legislation aimed at curbing the use of drones for surveillance purposes.[41] And in communities from Menlo Park to Seattle, local ordinances are placing specific restrictions on the use of surveillance technologies.[42]

Your community should follow the lead of courts and lawmakers and carefully evaluate the costs and risks of surveillance in order to protect both your investments in public safety and the rights of everyone.

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 end up being very costly, both in dollars and in personal freedom. That's why it is essential to publicly and thoroughly evaluate surveillance proposals. The following section will help your community — including public officials, law enforcement and diverse community members — 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, and Accountability, and Auditing.[43]

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 the costs to both your community's budget and to individual rights.

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

The best way to consider whether surveillance is the right choice and 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.

> "We need to have discussions with the public about new technologies and the robust privacy policies adopted to protect privacy. This lessens the pushback we get [and] benefits us in the long run."
>
> Chief Art Acevedo, Austin (TX) Police Department[44]

- *How is the community engaged in an informed debate about a 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.

Effectively notifying the public that surveillance is being considered requires more than a line item in a public meeting agenda. Proactively reaching out to community groups, including those representing ethnic and religious communities, and local media to increase public awareness early in the process can help your entire community engage 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.[45]

An informed debate also requires that your community has access to a wide range of information in order to assess how surveillance would work in practice and whether it would advance local goals. Hosting 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. Your community should also prepare and release a Surveillance Impact Report to help everyone understand the scope and potential costs of the proposal and a draft Surveillance Use Policy that details the safeguards that would be put in place 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.

CASE STUDY: CITIES ENGAGE WITH COMMUNITY MEMBERS TO EVALUATE SURVEILLANCE PROPOSALS

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 resident of the city, to provide advice on policy for surveillance cameras and oversee police use of the cameras.[46] Richmond formed an ad-hoc committee to evaluate policies for its video surveillance program.[47] 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.[48]

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.

➢ *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 weigh in on 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.[49]

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 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.

SURVEILLANCE AT THE "BORDER"

When you think of the border, you probably imagine a narrow line between our country and our neighbors. But federal regulations grant the U.S. Customs and Border Protection Agency broad authority within 100 miles of the edge of U.S. territory, which includes not just cities like San Diego but Los Angeles, San Francisco, and even Fresno, Redding, and Sacramento.[50] This means that the deployment of surveillance technology by border agencies, including technologies originally developed for military purposes, impacts individuals and communities throughout California.

Unfortunately, there is very little transparency about the use of surveillance technology by border agencies. Are local officials or lawmakers cooperating in surveillance activities? Are they even informed? Or is the federal government monitoring Californians far from the actual border without the safeguards that our democracy and Constitution demand?

A serious and informed discussion of the implications of widespread surveillance at the "border," whether by your local law enforcement or a federal agency, is absolutely necessary to prevent widespread violations of Americans' rights to privacy, property, liberty, equal protection, and due process. Even if your community can't easily prevent federal agencies from monitoring you, it can make sure that local law enforcement and lawmakers are transparent about their role. And it can clearly send a message to federal and state policymakers that you expect to be part of the discussion of any kind of surveillance in your area.

- *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.[51]

➢ *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.[52]

➢ *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 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.[53] 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.[54]

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. Residents deserve assurance that funds are being spent on mutually agreed-upon interests. 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?"[55]

These questions 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, in part because of rapid changes to privacy 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 you 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 without a warrant throughout the United States when the U.S. Supreme Court ruled in 2012 that their use implicated the Fourth Amendment.[56] As a result, the FBI deactivated the warrantless trackers and its agents had to physically retrieve them.[57] Obtaining warrants before using those GPS trackers would have ensured the constitutionality of obtained evidence and saved the FBI considerable time and effort.

➢ *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 appear to target — specific groups, especially those that already feel marginalized, 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 individual 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."[58]

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.[59]

CASE STUDY: LAPD BODY CAMERA POLICIES PROTECT OFFICERS AND THE PUBLIC

After announcing its intention to adopt body cameras, the Los Angeles Police Department reached out to the police union, the ACLU, and the public, to get input on the program and help designing policies that adequately safeguard privacy of officers and citizens. Being transparent about the program and soliciting input from the beginning can help ensure policymakers identify problems and address them from the start.[60]

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 memorialize 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.

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.

➢ *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.[61]

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. You need to ensure that training programs for anyone involved with surveillance are 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.

> "All of our officers receive First and Fourth Amendment training before they're allowed to access the system in any way."
>
> Jonathan Lewin, Chicago Police Department Office of Emergency Management and Communications[62]

➢ *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 issued and collection is underway, police only intercept communications relevant to the investigation, not every communication made by the target.[63]

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 that "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.[64]

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.[65]

- *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 the system for personal interests can be hard to resist. The NSA even has a specific term, LOVEINT, for employees who monitor their significant others,[66] and two Fairfield officers could face criminal charges after using a statewide police database to screen women from online dating sites.[67]

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

Placing limits on how you use the data is a great step, but third parties you share the information with 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 — your 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.[68] 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 the information you need and only for as long as you need it.

- *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, your 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.

➢ *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.

> "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[69]

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 and specify what specific condition(s) must be met in order to do so. 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 still being accomplished by surveillance. One key question is whether your Surveillance Use Policy is actually 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.

➢ *What type of supervision exists for persons operating the technology?*

Your system of management, in addition to technical measures, facilitates 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.

➢ *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, be 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.

> "[A]ll usage is supervised. All camera and operator actions are logged and can be tracked later."
>
> Jonathan Lewin, Chicago Police Department Office of Emergency Management and Communications.[70]

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 are 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.[71]

➢ *What legally enforceable sanctions exist against 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

Your community at large 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 this 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 call 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 have a greater impact on the rights of community members than you expect. And following public outcry about NSA spying and the use of military equipment by local police, community members demand — and deserve — both a voice in any decision to deploy surveillance technology and reassurance that robust safeguards and public oversight will be in place if surveillance is going to be used. Make sure that your entire community is engaged in asking and answering the right questions about surveillance technology by adopting a Surveillance & Community Safety Ordinance and following the other recommendations in this guide.

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 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 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 purpose(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 of 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] *See* Darwin Bond Graham & Ali Winston, *The Hidden Costs of Oakland's Surveillance Center*, East Bay Express, Jan. 22, 2014, available at http://www.eastbayexpress.com/oakland/controversial-the-hidden-costs-of-oaklands-surveillance-center/Content?oid=3816398; Nancy La Vigne et al., Urban Institute, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention* (2011), available at http://www.cops.usdoj.gov/Publications/e071112381_EvalPublicSurveillance.pdf.
[2] 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.
[3] Press Release, Office of the Controller, *Butkovitz Alarmed by Police Camera Program*, June 20, 2012, http://www.philadelphiacontroller.org/page.asp?id=792.
[4] *See* Fazaga v. FBI, 844 F.Supp.2d 1022 (C.D. Cal. 2012).
[5] *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.
[6] Cal. Civil Code § 1798.29 (2014).
[7] Ponemon Inst. & Symantec, *2011 Cost of Data Breach Study: United States* (2012), available at http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf.
[8] 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.
[9] *See* 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.
[10] 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.
[11] Terrence O'Brien, *Caught Spying, FBI Asks Student to Return GPS Tracker*, SWITCHED (Oct. 8, 2010), http://www.switched.com/2010/10/08/caught-spying-fbi-asks-student-to-return-gps-tracker/.
[12] 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.
[13] 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/.
[14] Christian Watien, *5 Uses for Drones that Don't Involve Fighting Terrorists*, Epoch Times (Nov. 10, 2012), www.theepochtimes.com/n2/world/5-uses-for-drones-that-don-t-involve-fighting-terrorists-313051-print.html.
[15] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 66 (2014), available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[16] 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/.
[17] *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.
[18] *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/.
[19] Peter Nicholas, *State Tracked Protesters in the Name of Security*, L.A. Times, July 1, 2006, available at http://articles.latimes.com/2006/jul/01/local/me-security1..
[20] Camille T. Taiara, *Monitoring Malcontents: Why Do the Governor's Critics Keep Findings Themselves Targets of Strange Police Scrutiny?*, S.F .Bay Guardian, http://www.sfbg.com/39/41/news_governator.html.
[21] *See* Mike Rhodes, *Students at CSUF Are Starving for Civil Liberties*, Indybay (Apr. 27, 2005), https://www.indybay.org/newsitems/2005/04/27/17351181.php.
[22] Local 10 ILWU v. City of Oakland, No. 3:03-cv-02962 (N.D. Cal. Apr. 28, 2005) (Jordan Dep. at 24:11-24).
[23] *See* Bradley, *Santa Cruzans Speak Out Against Police Infiltration and for an Independent Investigation*, Indybay (Jan. 25, 2006), https://www.indybay.org/newsitems/2006/01/25/17981451.php.
[24] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (March 24, 2014), http://ssrn.com/abstract=2412564.
[25] Riley v. California, 134 S. Ct. 2473, 2489 (2014).

[26] United States v. Jones, 132 S.Ct. 945, 955, 56 (2012).
[27] 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.
[28] 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.
[29] European Parliament Directorate General Internal Policies, *A Review of the Increased Used of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe* 15 (2009).
[30] *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.
[31] 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).
[32] Klayman v. Obama, Civ. No. 13-0851 (D.D.C. Dec. 16, 2013).
[33] U.S. v. Jones, 132 S.Ct at 956 (quoting U.S. v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).
[34] Ballot Pamplet., Proposed Amendments to Cal. Const. with Arguments to Voters, Gen. Elec. (Nov. 7, 1972).
[35] White v. Davis, 533 P.2d (Cal. 1975).
[36] People v. Cook 41 Cal. 3d 373 (1985).
[37] 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).
[38] U.S.A. Freedom Act, H.R. 3361, 113th Cong. (2013).
[39] Email Privacy Act, H.R. 1852, 113th Cong. (2013).
[40] 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).
[41] 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).
[42] *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/.
[43] 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.
[44] PERF Report, *supra* note 2, at 35.
[45] 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.
[46] Redlands Police Department, *Citizen Privacy Council*, http://www.cityofredlands.org/police/CPC.
[47] 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.
[48] *See* Memorandum, *City Administrator's Weekly Report* (Apr. 25, 2014), http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak046804.pdf.
[49] 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.
[50] *See* ACLU, *Know Your Rights: The Government's 100-Mile "Border" Zone — Map*, https://www.aclu.org/know-your-rights-governments-100-mile-border-zone-map.
[51] *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.
[52] *See* Citris, *Cistris Study on SF Public Cameras Released* (Jan. 9, 2009), http://citris-uc.org/citris-study-on-sf-public-cameras-released/.

[53] *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.
[54] *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.
[55] PERF Report, *supra* note 2, at 44.
[56] United States v. Jones, 132 S. Ct. 945 (2012).
[57] 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/.
[58] 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/.
[59] *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.
[60] Erika Aguilar, *LAPD Body Cameras: 90-Day Test Seeks to Answer Key Questions to Create New Policy*, 89.3 KPCC (Feb. 4, 2014), http://www.scpr.org/news/2014/02/04/41855/lapd-body-cameras-90-day-test-seeks-to-answer-key/.
[61] 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.
[62] PERF Report, *supra* note 2, at 14.
[63] 18 U.S.C. § 2518(5) (2014).
[64] Ohio State Highway Patrol Policy No. OSP-103.29 (revised Dec. 23, 2008).
[65] 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.
[66] 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/.
[67] 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/.
[68] *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.
[69] PERF Report, *supra* note 5, at 36.
[70] *Id* at 14.
[71] 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.