

POLICYMAKER BRIEF: IMPORTANT LIMITS ON SURVEILLANCE

We hope you and your community already followed the steps in [Seeing Through Surveillance: Why Policymakers Should Look Past the Hype](#), our guide to why policymakers must ask and answer important questions about surveillance technology. If so, then you have discussed local needs with your community, defined the problem you want to address together, and thoroughly considered the full costs of surveillance, as well as alternatives that could be effective and far less intrusive. You have also reevaluated existing surveillance programs and considered how to replace them with evidence-based non-surveillance solutions.

If, after conducting these steps, your community still plans to use surveillance technology, you should use this Policymaker Brief to create a minimum set of clear and enforceable rules that need to be in place for any surveillance system in order to try to protect rights and safety.

These rules should be publicly codified into an enforceable **Surveillance Use Policy**. This policy should strictly limit how and when surveillance is conducted, and how information collected is used, shared, and retained.

The Surveillance Use Policy should also create robust rules for enforcement. There must be legal consequences for not following the policy, and the public must be able to go to court to enforce their rights. Any Surveillance Use Policy should also mandate transparency and regular evaluation of the surveillance program to assess how it is affecting the community.

Surveillance is not public safety. Further, if your community does use surveillance technology and fails to have a robust Surveillance Use Policy and clear consequences for violations, you are inviting abuse undermining vital transparency, accountability, and oversight. We hope this Policymaker Brief is useful for thinking through some basic protections if your community uses any surveillance technology.

TABLE OF CONTENTS

STRICTLY LIMIT USE OF SURVEILLANCE AND ANY COLLECTION OR USE OF INFORMATION.....	2
PREVENT THE SHARING OR MISUSE OF INFORMATION.....	3
CONTROL THE RETENTION OF INFORMATION.....	5
ENFORCE YOUR RULES AND IMPOSE CONSEQUENCES.....	6
MANDATE TRANSPARENCY AND REGULARLY REEVALUATE THE PROGRAM.....	7
CONCLUSION.....	9

Authors: Matt Cagle & Nicole Ozer

Technology & Civil Liberties Program, ACLU of Northern California

Design & Layout: Ellen Gunn

Published by the ACLU of Northern California – July 2024


1. STRICTLY LIMIT USE OF SURVEILLANCE AND ANY COLLECTION OR USE OF INFORMATION

Modern surveillance systems can collect vast amounts of sensitive information about people. Moreover, information collected for one purpose can be abused for another, opening the door to discriminatory surveillance that undermines people's rights and safety. Write a set of specific limits on how the surveillance system can be used and what information can be collected.

➤ *Do you have clear rules about uses that are permitted and prohibited?*

A surveillance system is supposed to address a particular community problem. Any use policy should specifically detail what uses are permitted and make clear that all other uses are prohibited. To determine what uses are authorized, refer back to your community's needs and the specific problem the system is designed to address.

Agencies routinely try to quietly expand their use of surveillance systems beyond what is authorized. This temptation is often very great, especially in an era where vendors may update software for existing technologies, add new features, and market new ways of using the surveillance system. If you use a surveillance system in ways not vetted or approved by the community, there is an increased chance the system will be misused and harm people's rights and safety. Your policy should prohibit any additional uses beyond what policymakers and the community have debated and approved.



“You and your communities should be free from unchecked surveillance; surveillance technologies should be subject to heightened oversight that includes at least pre-deployment assessment of their potential harms and scope limits to protect privacy and civil liberties.”

—White House Blueprint for An AI Bill of Rights¹

You should also have rules about the type and amount of information collected by surveillance technology. Stockpiling information “just in case it becomes useful” increases the risk that information will be abused. Prevent this by writing explicit rules that clearly delineate approved and prohibited uses for specific surveillance systems. For example, a fire department that is authorized to deploy drones to find hot spots at a structure fire should not record or retain video of people on nearby streets. A police department using license plate readers to locate Amber Alert vehicles should not record or retain the locations of every driver.

➤ *Do you prohibit harmful and discriminatory use of the technology?*

Your use policy should thoughtfully consider how each surveillance technology poses potential risks for community members and proactively prohibit uses that threaten their rights and safety. It should make it clear that agencies are not allowed to use the system in ways that violate privacy rights, chill free speech, or facilitate discriminatory policing and enforcement. This includes any uses that violate

statutory law or are incompatible with constitutional guarantees of privacy, freedom of speech, freedom of religion, and equal protection.

➤ *What process will be followed each time surveillance is activated or used?*

Any policy should delineate the legal process and procedures that have to be followed every time a system is used or surveillance information is accessed. This is critical to try to prevent unauthorized, outright illegal, and rogue uses of surveillance technology. You should generally require probable cause, not mere suspicion or hunches, to initiate surveillance or access databases containing surveillance information. Requiring a strict process, including a warrant requirement, is particularly essential when the technology is capable of dragnet surveillance.

STRONGER STINGRAY POLICIES IN ALAMEDA COUNTY

When Alameda County was considering cell phone surveillance technology, the Alameda District Attorney publicly released its draft use policy and solicited feedback from the community. In response to extensive community concerns, the final policy required a warrant for use of the surveillance device and strict limits on how information could be used. Such a warrant requirement is now California law pursuant to the California Electronic Communications Privacy Act (CalECPA).²

2. PREVENT THE SHARING OR MISUSE OF INFORMATION

➤ *How do you limit sharing of any information you collect?*

You should place strict limits on the sharing of any information collected via surveillance. This is important both to comply with various California laws (including the prohibition of sharing ALPR information with out-of-state entities)³ and to protect your community from harm.

If surveillance information leaves your community, your community loses control over how it is used. For example, your police department may not share information with ICE, but neighboring departments might. Or else, the private vendor you work with could share information with other departments without you even knowing.

It is not a hypothetical concern that information that leaves your community can be used to harm people. Across the U.S. we have seen agencies like Immigration and Customs Enforcement targeting and deporting immigrants by using driver location information shared by local agencies. Following the reversal of *Roe v. Wade*, information about people seeking abortion or gender-affirming care collected in your community is now vulnerable to demands by agencies in states with laws that criminalize abortion and healthcare for transgender people.

Require via written agreement that any agency that obtains access to your systems must follow your policies. If a potential recipient of your information cannot agree with your policies or conditions, or if there is any uncertainty about how that entity may use the information, you should not work with or share information with them.

At the same time, the public has a legal right to request records about your surveillance program under the California Public Records Act. Accordingly, you need to avoid any sharing limits that undermine your ability to promptly comply with public records requests sent by the public.

➤ *How will the surveillance technology and information be secured?*

It is your responsibility to secure any information collected by surveillance technology. You should

NORTHERN CALIFORNIA COMMUNITIES SUFFER AVOIDABLE DATA BREACHES OF SENSITIVE INFORMATION

After failing to heed an outside auditor’s warnings, the City of Oakland suffered a ransomware attack that resulted in the public leak of sensitive information such as social security numbers, drivers’ license numbers, home addresses and other personal details about city workers and officials. The breach, which exposed information that fraudsters could exploit to carry out identity theft, also crippled key city systems used by the public for weeks.⁴

Monterey County suffered a security breach resulting in the theft of personal information of over 140,000 local residents. A subsequent grand jury investigation of that breach concluded that the breach stemmed from “totally obsolete” data practices and a failure to follow privacy laws, warning of “serious financial consequences” if the county failed to change its practices.⁵

consult with experts and implement safeguards at multiple levels to protect information wherever it is stored, for as long as it is kept. If your community does not have expertise with information security or an official charged with overseeing it, you should seek outside assistance as soon as possible.

➤ *How do you limit access to and use of surveillance information?*

It is your responsibility to ensure that information collected with surveillance is only used to address the specific community-defined purpose for the technology and cannot be abused. Impose strict rules governing its access and use by the government or third parties. For each use case, specify the staff who can access the information and the reasons why information can be accessed. As an example, if your community uses license plate reader surveillance to locate stolen vehicles, only people working on stolen vehicle investigations should be able to access that information. In no circumstances should government employees have unfettered access to information about

community members. You should also make it clear that some uses are clearly off limits, such as immigration enforcement.

BAD INFO POLICIES LEAD TO STALKER ABUSE

Without strong policies limiting access to information, the temptation to misuse a system for personal interests can be hard to resist. The NSA even has a specific term, LOVEINT, for employees who monitor their significant others.⁶ Two officers in Fairfield, California were also caught using a statewide police database to screen women they saw on online dating sites.⁷

3. CONTROL THE RETENTION OF INFORMATION

You also need to control the retention of information, taking account of legal requirements for retention of certain records alongside the potential privacy and security risks of keeping information for longer than truly necessary. For each type of information collected by surveillance technology, an agency should specify a retention period that is not longer than necessary to address the community's identified purpose for the technology while also reasonably complying with all legal requirements. Any information that is not needed should be deleted as soon as possible. At the same time, a short retention policy should not be used as a means to thwart legal requirements to retain certain records, including records for release to defendants and in response to public records requests.

- *Does retaining information directly address a problem identified by your community?*

As a default rule, government agencies should not be using surveillance technology to generally collect information about community members. You should have well-defined uses in service of your community's specific purpose for the technology, and you should only retain the information that will directly address that problem. Specify in your policies what is required to justify retention of information. Retaining information that you really do not need or keeping it longer than necessary increases the risk that information will be used contrary to the purpose agreed upon by the community or wind up in the hands of a bad actor.

- *Do you have a written retention policy that addresses the public's right of access?*

Your policy should also publicly explain the retention policy and how agencies will implement it. Information should be regularly and automatically deleted when a retention period lapses. As part of this, your policy should articulate the circumstances that can justify exceptions to community's retention period. For instance, an agency may need to keep information because it is relevant to a specific ongoing investigation of internal misuse, relevant to civil litigation or a criminal defendant's case, or the subject of a public records act request.

4. ENFORCE YOUR RULES AND IMPOSE CONSEQUENCES

You have a responsibility to ensure that surveillance technology in your community is not used to harm people. To do this, you need a way to monitor and track how agencies use any surveillance and you need to provide the public with a legal mechanism to enforce consequences for any violations of the policy.

➤ *How are you identifying potential misuses of the technology?*

The best way to identify misuse of surveillance is to “watch the watchers” by routinely keeping thorough records each time surveillance is deployed, or surveillance information is accessed. If surveillance technology is misused, you should know what agencies and people are responsible. Designate a chain of command in your policies and require record keeping about every single use of the surveillance technology, the information it collects, any personnel involved, their stated justifications, and any known abuse. To catch what human oversight misses, ensure that technical measures including access controls and audit logs are in place. Any audit logs are a public record and

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 systems were being followed. Fresno Police Chief Jerry Dyer said he supported the audit: “I have no doubt the audit will be very helpful to our ongoing video policing operations.” The city appointed a retired federal district court judge as auditor, who then examined current use of the system and made specific policy recommendations.⁸

accordingly should be released when subject to a public records request.

➤ *What legally enforceable consequences exist to deter misuse and abuse of this technology?*

A policy without enforcement is only words on paper. Without enforcement provisions, police and other government agencies have little reason to comply, and experience shows they do not.

You should adopt your policy as a law that ensures that members of the public can impose legal consequences, including via lawsuits, for violations. This will help prevent harm and address it if it occurs. At the bare minimum, your enforcement mechanism should include:

- A private right of action allowing any person to bring a lawsuit against a government actor or agency that has not complied with rules related to surveillance technology or other auditing or oversight requirements;
- Personnel consequences for government agents that violate surveillance rules;

- The ability to seek an injunction to address the violation;
- Damages for any member of the public affected by the violation;
- Fines for each violation of the rules; and
- Costs and attorneys' fees for any prevailing plaintiff that brings a lawsuit.

➤ *Did you adopt your rules and consequences as an ordinance with the force of law?*

Once your policy and enforcement mechanism are written, your community should adopt them as a local ordinance. This is necessary to make sure that the policy has the force of law, the rules can actually be enforced, and any harms can be properly addressed.

5. MANDATE TRANSPARENCY AND REGULARLY REEVALUATE THE PROGRAM

People have a right to know how their government uses surveillance. You should adopt a plan to regularly reassess the surveillance technology and whether it has proven effective. First, impose critical and regular audits to generate information that explains how the surveillance technology has been used and how it has affected the community. Publicly release this information and create a real opportunity for the community, particularly impacted people, to have a chance to reevaluate and, if needed, dismantle existing systems.

Community oversight and feedback play two essential roles. First, transparency about any use of surveillance allows people to determine if the program is actually addressing the community problem. Second, it allows the public and policymakers to identify misuse. Once your community learns first-hand about how surveillance has been used and how it affects different individuals and groups, this information will inform a decision about whether to change course.

When you receive a request for information about your surveillance from the public, transparency should be the default. Explicitly declare that local agencies will minimize the use of exemptions for public records requests. Invoking these exemptions withholds information from the public and, under California law, they are discretionary.

➤ *Are you requiring third party audits?*

An agency cannot audit itself. You should designate an independent party to audit your systems annually, at a minimum. This helps increase the likelihood that any misuses are properly identified and made public. Anyone with oversight responsibility should be independent, be given full access to the surveillance technology and database, and be empowered to receive complaints about misuse in order to draw conclusions that can lead to legally enforceable consequences.

Here are issues that an audit should cover:

- A description of how the surveillance technology was used, and how often;
- Information, including crime statistics, that provide evidence that the surveillance was causally and directly effective at accomplishing its stated purpose;

- A summary of community complaints or concerns about the surveillance 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 information acquired through the use of the surveillance technology was shared with any outside entities;
- Statistics and information about Public Records Act requests, including responses; and
- The total annual costs of the surveillance technology, including personnel and other ongoing costs, and any external funding available to fund any or all of those costs in the coming year.

➤ *How will the community stay informed about the surveillance program?*

The community needs as much information as possible to continually evaluate any surveillance system. An independent auditor should publicly release all the information detailed above that shows how the surveillance program has operated.

➤ *How will your community reevaluate the decision to engage in surveillance or the existing policies and safeguards?*

Any surveillance program should be reconsidered on an annual basis. After all, the conditions that existed when your community approved surveillance in the first place might not hold true in light of their actual experience with the surveillance technology and its impacts. Adopt a plan for regularly reassessing the surveillance program with community input using our report, [Seeing Through Surveillance: Why Policymakers Should Look Past the Hype](#), as a guide. Demand actual evidence that shows how the program directly furthers the identified community goal and how that benefit outweighs the known and potential harms. If the evidence of benefits does not substantially outweigh the potential harms, you should dismantle the program, impose new limits or

VALLEJO CREATES SURVEILLANCE ADVISORY BOARD

After a series of surveillance and policing scandals, community members successfully advocated for the City of Vallejo to create a Surveillance Advisory Board to advise policymakers and recommend legislative solutions. The Surveillance Advisory Board consists of residents from each council district and will meet regularly to give residents a voice in decisions about surveillance. The Board is empowered to request information, create reports, and suggest policy and legal changes necessary to protect the civil liberties and civil rights of community members from surveillance.⁹

modifications to the policy, or reconsider interventions that don't involve surveillance.

CONCLUSION

Seeing Through Surveillance: Why Policymakers Should Look Past the Hype

illustrates how surveillance can be a rights, safety, and public policy nightmare masquerading as an easy solution. If your community has surveillance technology, the policy limits discussed above are the bare minimum for transparency, accountability, and oversight. As you review this document, we also urge you to work with your whole community to reconsider non-surveillance alternatives that may better fulfill your public safety needs without inflicting the harms of surveillance.

ENDNOTES

¹ The White House, *Blueprint from an AI Bill of Rights*, 6 (Oct. 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.

² Linda Lye, *ACLU Urges Alameda County to Vote No on StingRay Surveillance*, ACLU of Northern California blog, Sep. 29, 2015, available at <https://www.aclunc.org/blog/aclu-urges-alameda-county-vote-no-stingray-surveillance>; *Alameda County Board Of Supervisors Passes Most Comprehensive Cell Phone Interceptor Privacy Policy In The Country*, Media Alliance, Dec. 25, 2015, available at <https://media-alliance.org/2015/12/alameda-county-board-of-supervisors-passes-most-comprehensive-cell-phone-interceptor-privacy-policy-in-the-country/>.

³ California Department of Justice, *Information Bulletin 2023-DLE-06: California Automated License Plate Reader Data Guidance* (Oct. 27, 2023), <https://oag.ca.gov/system/files/media/2023-dle-06.pdf>.

⁴ Darwin BondGraham, *Oakland ransomware hackers dumped gigabytes of sensitive city files on the web*, the Oaklandside, Mar. 6, 2023, available at <https://oaklandside.org/2023/03/06/oakland-ransomware-hackers-leak-sensitive-city-files-data/>.

⁵ 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.

⁶ Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, Wash. Post: The Switch, 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/>.

⁷ Dave Maas, *Misuse Rampant, Oversight Lacking at California's Law Enforcement Network*, EFF: Deeplinks blog, Nov. 18, 2015, available at <https://www.eff.org/deeplinks/2015/11/misuse-rampant-oversight-lacking-californias-law-enforcement-network>.

⁸ George Hostetter, *Former Judge Wanger Writes Far-Ranging Audit on Fresno Video Policing*, Fresno Bee, Jan. 7, 2014.

⁹ John Glidden, *Vallejo's new surveillance advisory board to meet April 21*, The Vallejo Sun, Apr. 11, 2022, available at <https://www.vallejosun.com/vallejos-new-surveillance-advisory-board-to-meet-april-21/>.