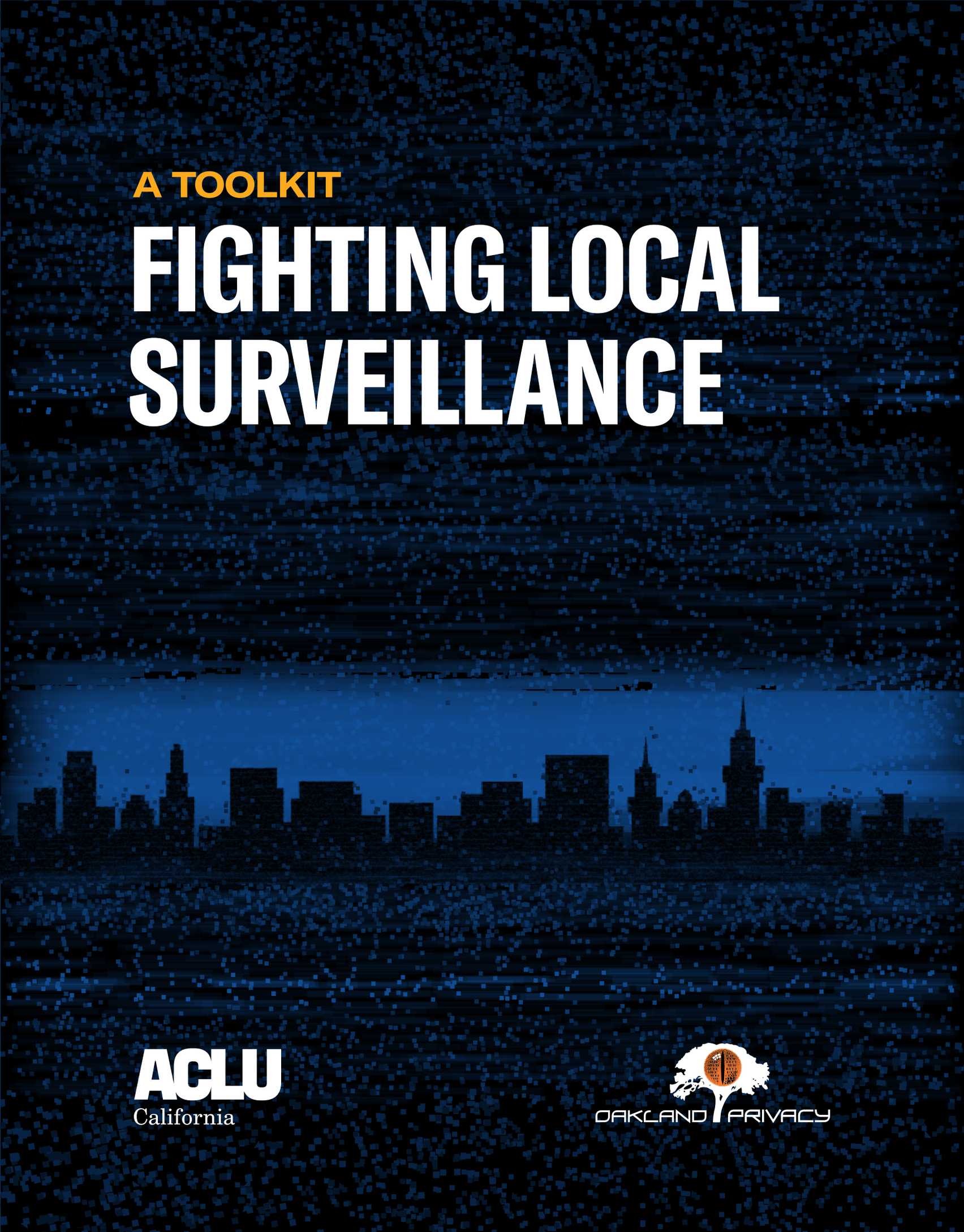
A TOOLKIT

FIGHTING LOCAL SURVEILLANCE



ACLU California

OAKLAND PRIVACY

CONTENTS

Authors: Matt Cagle, ACLU of Northern California & Tracy Rosenberg, Oakland Privacy

Contributing Writers and Editors: Tessa D'Arcangelew, Jennifer Jones, Raquel Ortega, Nomi Conway, Chris Conley

Layout & Design: Teegan Lee, Gigi Harney, Ison Design

PUBLISHED BY THE ACLU OF CALIFORNIA

APRIL 2020

You can fight government surveillance

In 2019, San Francisco passed a landmark law banning government facial recognition and requiring public oversight for local decisions related to the acquisition and use of other surveillance technologies such as cameras, drones, and more. That effort, led by the ACLU in deep partnership with civil rights partners, is part of a bigger movement afoot in the U.S. In more than a dozen cities and counties, communities have passed laws ensuring that decisions about high-tech surveillance are made by the community through the democratic process, not in secret by police and surveillance companies acting alone.

You can stop secret surveillance in your community, too.

Together, we are achieving important victories against secret and dangerous surveillance. We are raising awareness of how surveillance technology like drones, stingrays, and facial recognition exacerbate discriminatory policing, suppress dissent, and facilitate harm to immigrants and people of color. We are building the political coalitions and power essential to win surveillance reform and durable social change. We are changing the narrative by explaining why surveillance systems make us less safe and less free. We hope you'll join us.

This toolkit shows how to spark a movement and win lasting change.

This Toolkit summarizes many lessons we have learned about how to work effectively together and fight against local surveillance. It builds on the ACLU of California's report, Making Smart Decisions About Surveillance: A Guide for Community Transparency, Accountability & Oversight, which highlighted important issues about local surveillance and charted a path to reform (available online at http://www.aclunc.org/smartaboutsurveillance).

This toolkit is a resource for your surveillance reform campaign.

Change is never easy to achieve, but this Toolkit describes the methods and strategies you can use to uncover local surveillance programs, organize and build political power around issues of surveillance, and effectively push for policy and legal reforms. The accompanying **Appendix** (available online at http://www.aclunc.org/surveillancetoolkit) contains dozens of sample documents, letters, and other materials you can customize for your own surveillance reform campaign.

We hope you use this resource to fight unaccountable surveillance and protect the civil rights of everyone in your community.

FIGHTING LOCAL SURVEILLANCE

A CHECKLIST

❑ 1. FOCUS ON THE HARMS OF SURVEILLANCE

Your focus should be on the threat that surveillance technology poses, not only to our rights and liberties but also our ability to live safe lives and organize for social and political change. **Part 1** seeks to frame the harms of surveillance technology in terms of its real life impacts. For more information, please see our companion report, *Making Smart Decisions About Surveillance* (aclunc.org/smartaboutsurveillance) and the **Appendix**.

❑ 2. LEARN ABOUT SURVEILLANCE TECHNOLOGY IN YOUR COMMUNITY

There are several ways to uncover government surveillance in your neighborhood. **Part 2** summarizes steps you can take to learn about the surveillance technologies being used by local authorities. Strategies explained include monitoring public agendas posted by local government, close scrutiny of local news, questions to elected officials or government agencies, and public records requests. You can find a sample, customizable public records request in the **Appendix**.

❑ 3.BUILD A DIVERSE COALITION FOR CHANGE

A coalition helps you build political power, persuade elected leaders, and achieve durable social change. **Part 3** explains how to build an effective coalition that centers on the people most directly impacted by government surveillance. In building a coalition, seek input, inclusion, and leadership from people of color, immigrant communities, low-income or homeless individuals, people on parole, and other local activists.

❑ 4. CHOOSE A STRATEGIC GOAL TO PURSUE

There is no one-size-fits-all solution for challenging surveillance in your community. **Part 4** discusses various legislative and policy solutions you might consider, including a surveillance technology oversight ordinance, a ban on a particular technology (such as facial recognition), a privacy advisory commission, or opposition to a specific proposed purchase of surveillance technology. You can find drafts of model legislation in the **Appendix**.

❑ 5. IDENTIFY OPPORTUNITIES TO INFLUENCE LOCAL SURVEILLANCE DECISIONS

Identifying the right decisionmakers, including elected leaders and other officials, helps you to know where to focus your advocacy. **Part 5** explains how decisions about surveillance are generally made at the city and county level, including the governing bodies and stakeholders you should be aware of as you craft and execute a public campaign.

❑ 6. DEVELOP YOUR NARRATIVE AND MESSAGING

Public support is key to building consensus around your strategic goal. **Part 6** explains how to start a public conversation about the importance of your issue and create a communications strategy that will help people and policymakers understand surveillance technology, its real life impacts, and the reasons why people should support your coalition's proposed solution. Look to the **Appendix** for a guide to build a messaging strategy, as well as sample coalition letters of support and op-eds.

❑ 7. MEET WITH DECISIONMAKERS TO MAKE YOUR CASE

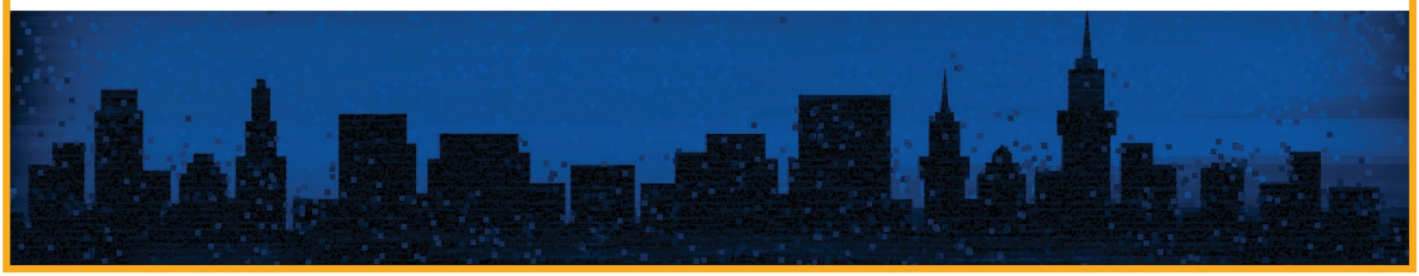
An in-person meeting with local decisionmakers gives you an opportunity to explain the issues, why they matter and their impact on community members, and to ask for support for your coalition's preferred strategic goal. To make your meeting a success, it is important to prepare and follow through. **Part 7** explains how to request and prepare for a meeting, what to bring, and how to ask for support for your solution.

❑ 8. PUBLICLY ADVOCATE FOR YOUR STRATEGIC GOAL

Public support is key to building consensus around your goal. **Part 8** explains how to start a public conversation about your coalition's strategic goal and present it to decisionmakers at a public meeting. Look to the **Appendix** for sample public comments, op-eds, and other public advocacy materials.

❑ 9. OVERCOME CHALLENGES, BUILD ON YOUR PROGRESS

You will encounter challenges, but you can overcome them. And when you win, celebrate your victory. Build on the progress you achieve, using it as an opportunity to reiterate your coalition's values and vision for social change. **Part 9** discusses how to overcome challenges, achieve your strategic goal, and build on victory for larger social change.



1. Focus on the Harms of Surveillance

Surveillance technologies can take many forms, including cameras that recognize our identifying characteristics, sensors that track our features and devices, and systems that collect and analyze our speech and activity, online and in person. Whether it is facial recognition, automated license plate readers, or social media tracking software, what matters is the impact these technologies have on people's lives.

The government's use of surveillance systems to monitor our lives and collect information about us without our consent helps fuel an unfair criminal justice system, violates core civil rights, and prevents people from living safe, fulfilling lives. Highlighting these harms and focusing your messaging on preventing or righting them is essential to winning the fight against secretive and unaccountable surveillance.

There are many ways that surveillance technology can harm your community. This section highlights some of the most common harms—but there may be others specific to your own city, county, or neighborhood. Reflect on whether the existence of one or all of these can be a compelling case for action.

THE IMPACT ON PEOPLE OF COLOR, IMMIGRANTS, AND VULNERABLE COMMUNITIES

Surveillance technology supports discriminatory policing practices and the criminalization of people of color, immigrants, and those without economic or political power. Neighborhoods and community members under constant surveillance and scrutiny are more likely to end up on a government watch list, logged into the criminal databases, and as a result, become disproportionately subject to arrest and charges for minor violations.

In some cases, these harms arise from the technology itself. For example, bias and accuracy problems have been found to exist in prominent facial recognition systems, leading people to be impacted differently based on their race, gender, or age. The data used to build surveillance systems can also fuel harm, as with predictive policing systems that rely on historical policing data, such as discriminatory arrests, to inform future patrols and enforcement actions.

Bias and discrimination isn't just the result of accuracy or bias in the technology itself, but also the reality that governments often focus the gaze of surveillance technologies on already over-policed communities. In places such as Oakland, the use of automated license plate readers has at times been concentrated in neighborhoods of color, and Immigrations and Customs Enforcement exploited data from ALPR databases to find and deport immigrants. Further, majority-minority cities, including Compton and Baltimore, have been watched using high-powered aerial surveillance cameras. Surveillance technology amplifies and fuels inequities that already exist.

THE IMPACT ON OUR ABILITY TO EXERCISE CORE CIVIL RIGHTS

Unaccountable surveillance doesn't make us more safe — but it does make us less free. We should be able to safely live our private lives without being logged into a government database. The First Amendment guarantees us the right to express ourselves online or attend a protest or place of worship being targeted simply because we exercise those rights. And our right to a fair

criminal justice system should not be undermined by government attempts to hide their surveillance practices. Yet all too often, unaccountable surveillance threatens our core rights under the U.S. and state constitutions.

Surveillance technology supercharges the government's ability to track First Amendment activity and expression. Years after the September 11th attacks, New York police used automated license plate readers to conduct suspicionless monitoring of Muslim drivers coming and going to mosques. In San Jose, officers spied on political protesters by using social media surveillance software. Surveillance of protected activities has a lasting effect: people who have to fear being monitored may hesitate to exercise these and other core constitutional rights.

The secretive use of surveillance systems also threatens our constitutional rights to a fair criminal justice system. Police in Florida withheld evidence from criminal defendants about the use of facial recognition in their cases. Other criminal defendants — and even the judges in their cases — have been denied information about the use of cell site simulators to locate them and others associated with their trials. People cannot mount an adequate criminal defense if they don't know that police used – and possibly misused – surveillance technology against them.

THE IMPACT ON MOVEMENTS FOR SOCIAL CHANGE

There is a long history of governments turning their surveillance systems against people and movements advocating for social and political change. The Federal Bureau of Investigation wiretapped Dr. Martin Luther King Jr. in an effort to generate blackmail and derail the civil rights movement. Surveillance technology, when used without public oversight, enables similar harms today.

Modern day government agencies have used digital surveillance systems to target people and groups advocating for change. San Francisco Bay Area police flew aerial drones over protesters of the Trump Administration's immigration policies and U.C. Berkeley student activists. Police across the United States have used social media surveillance and facial recognition software to track, infiltrate, and arrest activists associated with Black Lives Matter and others protesting police violence. Surveillance helps a government defend and extend existing power structures.

FOCUS ON HARMS TO STRENGTHEN YOUR CASE FOR CHANGE

We fight against unaccountable surveillance because its abuse prevents people from living safe, fulfilling lives. Highlighting these impacts is critical to building support for community efforts to rein it in. As you move forward and implement this Toolkit, focus on the reality of surveillance technology in your conversations, coalition, and strategy for change.

2. Learn About Surveillance Technology in Your Community

What surveillance technologies and systems are being used in your community? Knowing the answer to this question will help you understand which community members are impacted by surveillance and which interventions may be necessary to protect public safety and civil rights. This section outlines a few methods you can use to discover surveillance technology in your community. Explore these strategies in parallel to learn about local surveillance, changing course if your original efforts don't produce results.

MONITOR AGENDAS POSTED BY LOCAL GOVERNMENT AGENCIES

In California and other states, open meetings laws require that government bodies publicly post their agendas and related materials a few days before a public meeting is to take place. These agendas may mention plans or proposals to purchase surveillance technology. Because police departments are not the only agencies that use surveillance technology, you should also consider monitoring transit, parks and recreation, and other local departments who have their own public meetings.

Many city and county websites include a search function for local meeting materials. Discover otherwise hidden surveillance technologies by searching these sites with both general (e.g., "surveillance") and specific ("unmanned aerial vehicle") terms.

CASE STUDY: DISCOVERY OF SAN JOSE'S DRONE

The discovery of a drone in the city of San Jose shows how surveillance technology can hide in plain sight. In 2014, an intern with the ACLU of Northern California spotted a suspicious item when searching through a public agenda for the San Jose City Council meeting. Buried in hundreds of pages of agenda documents was a mention of an "Unmanned Aerial Vehicle." Neither the City Council nor the public at large were aware that San Jose's Police Department planned to purchase a drone. The publication of this purchase sparked a controversy and a discussion about surveillance reform in the city.

FOLLOW THE MONEY

For nearly twenty years, the Department of Homeland Security (DHS) has provided localities with billions of dollars in grants that local departments often use to purchase surveillance technologies. As you search public documents such as city council meeting agendas, look for references to these DHS programs, which include State Homeland Security Grant Program (HSGP), Urban Area Security Initiative (UASI), and Operation Stonegarden (OPSG).

CLOSELY READ THE LOCAL NEWS

Articles by local newspapers and press may mention surveillance proposals that may not have come up for discussion before an elected body. On occasion, government officials may reach out to local news outlets to explain and make the public case for new surveillance proposals before they acquire the technologies. Other times, law enforcement agencies will tout or reveal

their new surveillance technology in local press outlets. These technologies may not be mentioned in the headline; rather, midway through the story itself. Local news will help you find surveillance technology hiding in plain view. It will also help you understand local priorities, values, and politics once you get engaged.

CASE STUDY: FRESNO USES "THREAT LEVEL" SURVEILLANCE SOFTWARE

In 2015, a Fresno resident's discovery helped spark a public records investigation that would eventually lead to new privacy protections for people across the country and the world. A member of the ACLU of Northern California noticed that the Fresno Police were touting their use of social media surveillance software in the local press. That person alerted ACLU-NorCal, who then sent public records requests to Fresno and police around the state. The resulting documents revealed the statewide use of software to track Black Lives Matter and other activists for social change. Subsequent advocacy led Facebook, Instagram and Twitter to update their policies and take steps to protect users worldwide.

ASK AN ELECTED OFFICIAL OR GOVERNMENT AGENCY

Your local elected officials work for you, so you shouldn't hesitate to ask questions about the use of surveillance technology by local agencies. Call or e-mail your city or county's elected representative's office and politely ask about a particular surveillance technology and whether local agencies use it. If the office shares your interest, ask if they can inquire themselves. You can also contact the police, transportation, or other city departments and ask them directly. These conversations can help you build rapport, as well as give you valuable information that can inform a subsequent public records request. Be polite, and follow-up.

SEND A PUBLIC RECORDS REQUEST

California (and other states) require public agencies to provide copies of public records on request. The California Public Records Act (CPRA) gives you the right to demand the disclosure of public records from local government agencies including police, transit agencies, and other city departments. In practice, a public records request is just a letter or message that describes the records you seek – in this case, they are records relating to the acquisition or use of surveillance technology in your community.

There are no magic words or formula for writing a public records request: just do your best to describe what you're looking for in plain English, and then send it off. Try to keep your request focused: the most successful requests are focused on a particular technology (rather than a variety of technologies) and include a few straightforward inquiries for records. As with other contact with public agencies, be sure to be polite, and follow up if you don't hear back.

Check out the **Appendix** to this toolkit (http://www.aclunc.org/surveillancetoolkit) for a customizable template public records request. The **Appendix** also includes definitions of particular surveillance technologies to help you customize your requests.

3. Build a Diverse Coalition for Change

You and your neighbors are more powerful if you work together. Working within a coalition is an opportunity to create political power and connect the dots for policymakers and the public about why an issue really matters. You also increase you chances of making lasting change. A coalition can mean different things to different people, and there are many different structures. This section explains why coalitions are important to achieving durable social change and how to build one that is both inclusive and effective.

COALITIONS EXPAND NETWORKS AND ACCESS TO POWER

Coalitions create more opportunities for change. Bringing together individuals and organizations from varied backgrounds increases your chances of making connections with elected leaders and other influential stakeholders who you might need to persuade.

Coalitions expand your collective resources and knowledge of tactics. Different individuals and organizations bring different skills to the table. Expanding the talent and voices on your team will lead to a better strategy and better chances of success.

BUILDING A DIVERSE COALITION IS ESSENTIAL

Surveillance is often just one ingredient in a larger system of local injustice. Surveillance practices enable and help sustain racial profiling, mass incarceration, abusive immigration practices, criminalization of poverty, and religious discrimination. Surveillance leads to more than just harm to civil rights and civil liberties; unaccountable surveillance practices damage livelihoods and ruin people's lives.

Your coalition should reflect this intersectional reality and include people working on a variety of community issues and the people most impacted by surveillance. These diverse voices should inform your understanding of the problem and have a central voice in your coalition's strategy for addressing it.

As you begin building a coalition, make a deliberate effort to seek input, involvement, and leadership from people of color, immigrant communities, low income and unhoused individuals, people on parole, and activists or organizers, among many others. Tap into your existing networks and seek out local residents who are already fighting for justice and equality.

CASE STUDY: DIVERSE BAY AREA COALITION SAYS NO TO DANGEROUS SURVEILLANCE AFTER BART TRAGEDY

In July 2018, a Black woman named Nia Wilson was stabbed and killed in an act of racist violence on a Bay Area Rapid Transit (BART) platform in Oakland. In response, BART proposed a multi-million dollar expansion of surveillance throughout the transit network. Recognizing that surveillance technology is frequently used to police and criminalize – not protect – Black and brown people, a coalition of community organizations rose in opposition to the proposal. Hearing these concerns, BART opted against moving forward with a new surveillance infrastructure; instead, BART charted a new course, leading to a new surveillance technology ordinance that gives the public a voice in decisions about surveillance.

ENGAGE IN ONE-ON-ONE CONVERSATIONS AND LISTEN

After you reach out to potential partners, sit down to discuss mutual interests and identify shared desires for solutions or next steps. Identify your shared interests and be collaborative in identifying next steps you can take together or as individuals in pursuit of a common goal. Focus on listening and asking informed questions about their priorities and existing work. Think about your shared vision rather than making a transactional "ask." Above all, get to know your potential coalition partner.

MEET WITH COALITION PARTNERS AND DISCUSS SURVEILLANCE ISSUES

Meet with your potential coalition partners as a group to share information, build rapport, and begin identifying what course of action you want to take together. The most straightforward way to do this is to convene a coalition meeting in collaboration with key community partners. Together, develop an agenda, which might include a short presentation on surveillance issues, impacts, and a discussion of what possible collaboration could look like. Use this meeting to discuss a timeline and outcomes, and devise next steps. Consider additional strategies, such as webinars, panels, and teach-ins that provide opportunities to recruit new partners, while educating the public about surveillance issues and the findings of records requests.

DEVELOP A STRUCTURE

It is important that the individuals and organizations in the coalition feel respected. Develop norms together for not only who will do the work, but how you all want to do it together. Discuss and listen for policy positions that are non-negotiable for members of the coalition. Identify collaborative methods to make decisions, the different roles of participants, and an ongoing communication structure. Decide whether regular coalition meetings (on the phone or in person) make sense and set a schedule. And when you meet, remember to elevate the voices of people impacted by surveillance (sometimes the people who volunteer to speak are not representative of those most impacted).

LEVERAGE YOUR COALITION WITH A COALITION LETTER

A coalition letter is an opportunity to make your case – and demonstrate the political power of your coalition – in a single place for decisionmakers. A letter typically has a few key elements: it explains who is in your coalition, the surveillance technology issue in your community and why it matters, and a short explanation of your strategic goal (see **Part 4**) and why they should support it. Submit your letter to the relevant elected body at least one week prior to their meeting to discuss your surveillance issue. You can find a sample coalition letter in the **Appendix**.

COALITION WORK IS NOT EASY, BUT IT IS ESSENTIAL

It can be difficult to unite people, identify a common goal, and work toward it together. But the rewards are worth the investment. Work on coalition relationships now to prepare for future fights, both the ones you plan for and the surprises that are out of your control, and build durable political power for future fights. Diverse, unified, and effective coalitions are essential to bringing about social justice in your community.

4. Choose a Strategic Goal to Pursue

Now it's time to decide on a surveillance reform goal that your coalition will work toward together. This decision should be informed by the surveillance technologies or practices your coalition finds most concerning, the experience of impacted communities, and the political landscape and local interests that you will have to navigate. This section summarizes a few options for political or legislative change that your coalition may choose to pursue. There is no one-size-fits-all strategy. You can start with one strategy and build on success.

ENACT AN ORDINANCE TO REQUIRE OVERSIGHT OF ALL SURVEILLANCE TECHNOLOGIES

A Surveillance Technology Ordinance gives your community a seat at the table – and an opportunity to reject or to oversee any surveillance technology that your city agencies seek to acquire or use. This kind of law requires a public debate about surveillance technology proposals and a vote by elected leaders before they can be acquired. Importantly, it provides your coalition with the chance to say no to surveillance that is incompatible with civil rights, harmful to public health or safety, or at odds with your coalition's vision for the community.

As of January 2020, more than a dozen U.S. communities have adopted ordinances based on ACLU model legislation originally developed by the ACLU of California. This legislation, available in the Appendix, is part of the Community Control Over Police Surveillance (CCOPS) campaign, and designed to be customizable to meet each community's needs and local institutions. A Surveillance Technology Ordinance can also be coupled with a ban on a technology that poses a particular threat to civil rights, such as facial recognition.

ENACT A BAN OR MORATORIUM FOR A PARTICULAR SURVEILLANCE TECHNOLOGY

Your coalition may also decide to advocate for a ban or moratorium on a particular surveillance technology. This can be done through a standalone ordinance (see an example in the **Appendix**) or as one piece of a Surveillance Technology Ordinance. By supporting a ban on the government's use of a particular surveillance technology, your community makes a statement that its harms – including the likelihood it will be misused to target and criminalize community members – outweigh its theoretical benefits.

More than half a dozen U.S. communities have gone this route by passing ordinances to ban facial recognition technology. In May 2019, a coalition led by the ACLU of Northern California successfully enacted the first of these bans in San Francisco (legislation that also included a Surveillance Technology Ordinance). Since then, Oakland, Berkeley, and multiple cities in Massachuttsetts have passed similar bans, with more localities moving forward. Craft your own proposed ban using the sample language located in the **Appendix**. Bans are just one way to proactively prevent the local deployment of a specific surveillance technology.

OPPOSE A SPECIFIC SURVEILLANCE TECHNOLOGY PROPOSAL

Your coalition can also advocate against the deployment or purchase of a particular surveillance technology that is at odds with civil rights, public safety, or local values. This strategy makes sense when a local agency has decided to publicly ask the City Council or Board of Supervisors for permission to enter a contract or use taxpayer funds. Because this strategy does not require legislation and is focused on a single technology, it is a great approach if your coalition is new to surveillance issues and has not had time to start a community conversation about bigger picture reform. Explain your concerns with the proposal to the public and elected leaders to build understanding and capacity for larger, structural reforms. The **Appendix** includes a sample letter urging elected leaders to reject a proposal to expand surveillance in a community.

CASE STUDY: CALIFORNIA ACTIVISTS PUSH BACK ON LICENSE PLATE READERS

For years, many cities have used license plate readers to track the locations of local drivers, leading to the creation of large databases of residents' information. But in 2018, after news broke that Immigration and Customs Enforcement was seeking to exploit these systems to locate and deport immigrants, local activists embarked on a new strategy to oppose the growth of these systems vulnerable to such abuse. In cities across California – including Century City, Richmond, Delano, and Half Moon Bay – activists learned of proposals to expand license plate reader systems and successfully used coalition letters and public comment to persuade city councils to reject them.

CREATE AN OVERSIGHT COMMISSION

An oversight commission can help your community monitor and exercise oversight of local agencies that seek to acquire and use surveillance technology. The commission can ensure that the public learns about surveillance issues and provide a forum for experts to discuss them. A privacy commission can be staffed with community members from different regions, educational backgrounds, and with different lived experiences. Model legislation to form a standing privacy committee can be found in the **Appendix**.

CASE STUDY: HOW OAKLAND'S PRIVACY ADVISORY COMMISSION WORKS

After Oakland Privacy, the ACLU of Northern California, and many others successfully prevented Oakland from expanding a major surveillance complex named the "Domain Awareness Center," a local citizens' committee recommended that the City create an Advisory Commission. This Commission provides the City with advice on best practices to protect Oaklanders' privacy rights in connection with the City's purchase and use of surveillance technology and other privacy-impacting systems. Made up of members appointed by the City Council, the Commission regularly works with stakeholders to understand how technologies work and their impacts, and to make policy recommendations for the Oakland community.

REQUIRE LOCAL DEPARTMENTS TO REPORT THEIR USE OF SURVEILLANCE TECHNOLOGIES

You can also urge your City Council or Board of Supervisors to ask their staff to create a report that indexes and explains the surveillance technologies used by local agencies. This report is an opportunity for elected leaders to request information and conduct oversight of local departments, and it can inform which strategies your coalition decides to pursue.

5. Identify Opportunities to Influence Local Surveillance Decisions

Achieving your strategic goal will require engagement with local decisionmakers. Knowing which actors have authority and make decisions will help you target your demands, your messages, and your coalition's advocacy. In most cities and counties, this authority rests with a few key bodies and actors described in this section.

Members of your coalition should meet with these actors to discuss your coalition's strategic goal and why change is needed in your community. These meetings are an opportunity to learn how policies are implemented and generate support for your coalition's strategic goal. The **Appendix** includes a sample message you can use to request a meeting.

THE DECISIONMAKERS: CITY COUNCILS

While every state and locality is a little different, city councils are typically the municipal-level elected body that supervises the police department and the police chief, as well as various city departments (e.g., parks and recreation, waste management, etc.). City councils can demand information and reports from the police and other local departments, such as a report on what surveillance technologies city departments possess and use. City councils also control local budgets, which means they influence decisions to buy surveillance technology.

A city council is also a lawmaking body. City councils can pass laws, or ordinances, on a wide array of local concerns, including the conduct of city departments and issues related to the privacy, health, and safety of local residents. This means councils can pass a Surveillance Technology Ordinance, a ban on the government use of a particular surveillance technology, or an ordinance creating a privacy advisory commission to oversee local surveillance issues.

THE DECISIONMAKERS: BOARDS OF SUPERVISORS

In rural and unincorporated areas, county bodies and actors are typically the key decisionmakers on issues of local surveillance. In California, elected bodies known as Boards of Supervisors are responsible for the management of county affairs and supervision of county law enforcement: the sheriff and district attorney. Boards can allocate taxpayer funds, oversee contracts, set rules for county property and equipment, and request information and reports from county officials. Under their legal authority in California, Boards can also adopt the kinds of surveillance oversight legislation discussed above.

THE BEHIND-THE-SCENES PLAYERS: LOCAL DEPARTMENTS, ADMINISTRATORS, AND MANAGERS

In addition to elected leaders, cities and counties employ numerous officials charged with implementing policies and managing the day-to-day operations of departments. The heads of city departments are responsible for ensuring their teams comply with local law and policy. At a higher level, city managers and county administrators oversee the implementation of local policy, supervise departments and staff, and execute the budget determined by elected leaders.

THE KEY VOTES: A COMMITTEE AND THE FULL COUNCIL OR BOARD

If your coalition's goal is to pass an ordinance, doing so often requires at least two important votes: a vote by a committee comprised of a subset of the full city council or county board, followed by a vote by the entire elected body.

Once introduced, legislation is typically referred to a subset of the city council or board, also known as a committee. For legislation that relates to surveillance technology, that is likely to be the committee in charge of issues of public safety or policing, such as a "Public Safety Committee." Often, key decisions about the substance of legislation is made at the committee level, and so you should take it seriously. At all stages, you will need to persuade a majority of elected officials to support your cause. The next section explains how to secure their votes.

6. Develop Your Narrative and Messaging

A coalition communications strategy should guide your public advocacy. This document is informed by your coalition's core values and target audience and explains why your issue is important and worth supporting. It defines what public safety can and should mean in your community.

> *"Surveillance without oversight makes us less safe and less free. Our communities deserve a seat at the table, and the power to create safeguards and prevent abuse."*

A consistent communications strategy not only educates the public and decisionmakers, but also focuses your coalition and builds new political power. Articulate your values, the problem as you see it, and your solution.

> *"At the heart of this legislation is the basic principle that communities should know about and control what surveillance technology the police are using."*

Use your communication strategies to inform your meetings with legislators, public statements and written materials throughout your campaign. Don't hesitate to repeat your narrative and messages. The repetition of your messaging is key to building public support and consensus around your cause.

> *"This ordinance will put decisions about surveillance back where they belong: in the hands of the people. Come out to tonight's public meeting and voice your support!"*

The **Appendix** includes a communication strategy framework and example messaging for a Surveillance Technology Ordinance and ban on facial recognition.

7. Meet with Decisionmakers to Make Your Case

Whether your coalition is seeking to prevent a surveillance acquisition or pass a surveillance ordinance, it is important to meet with legislators and stakeholders who can champion your cause. If your goal is to pass legislation, you will need to identify an "author" who will introduce the legislation for consideration by the governing body. Regardless of your goal, in-person meetings give your coalition the opportunity to build support for it. This section explains how to arrange and hold meetings with the local officials who have a stake in surveillance decisions.

HOW TO REQUEST A MEETING

Making a meeting request is simple. Your elected official's contact information (email and phone) should be available on the local government's website. Your written message should identify you and your coalition, and whether you are a constituent, and a brief description of the issue or legislation you'd like to discuss. Include specific times or dates that work for you and follow up to confirm a meeting date. In the **Appendix**, you will find a few sample messages to make these requests.

You can meet with any local decisionmaker, but elected officials are understandably most responsive to their constituents, so we recommend that you prioritize inviting people to the meeting who are coalition partners and constituents of the elected official.

PREPARE FOR YOUR MEETING

You want to make sure you arrive at the meeting fully prepared and ready to make your case in a timely manner. Here are a few considerations to keep in mind as you prepare.

- **Be aware of the goal.** Remind yourself of the strategic goal your coalition decided to pursue in **Part 4** and how the decisionmaker plays a role. Can they introduce or support a Surveillance Technology Ordinance or ban on facial recognition? Can they request that city departments prepare a report on their use of surveillance? Be prepared to make a clear "ask" and to stay focused on that goal during the meeting.
- **Do your homework.** Make sure you understand and memorize your key points, including how you will explain your coalition's goal, your concerns with surveillance, and why the official should be persuaded to care. For your first meeting, you might try writing three short bullet point sentences that you and your partners can reference to stay on track.
- **Decide who will attend the meeting.** Keep it small—no more than 4 or 5 people—but try to bring people who represent diverse cross sections of the community, including those impacted by surveillance. Before the meeting, identify who will speak on each issue and who will take notes. Create space for impacted people to share their perspective and experience with surveillance technology.

Together we are more powerful. If you plan to represent the ACLU or your coalition, keep the ACLU affiliate and coalition partners in the loop about your meetings. Doing so ensures your work is coordinated and that others are available to support you.

BRING LEAVE-BEHIND MATERIALS

A meeting with a public official is both an opportunity to build rapport and to educate the official about an issue you care about. To help accomplish these goals, you should consider bringing and explaining a few relevant documents, including any model legislation you hope to pursue, news articles discussing the issues, and a coalition letter summarizing your support for legislation or your chosen strategic goal. Samples of these materials are found in the **Appendix.**

HOW TO RUN THE MEETING

As local experts on surveillance issues affecting the community, you can use your meeting as an opportunity to build rapport and be a resource for the decisionmaker. But be respectful of their time – on any given day, a decisionmaker may be working on dozens or even hundreds of issues. Here are a few tips for running a successful meeting:

- **Build rapport.** Introduce yourself as a constituent, if you are one. Politicians care about the people who can vote them in – and out – of office. Be sure to bring up any other connections, such as memberships in the same groups, common friends, or previous meetings. You can also thank the official for previous votes or actions that you supported.
- **Believe in what you say.** Say it respectfully and with conviction. Provide personal and local examples of the impact of the ordinance or issue. Explain why you are concerned about government surveillance. Be sure to demonstrate how the issue affects or will affect real people, the official, and their constituency.
- **Stay on message.** You will likely have 20 minutes or fewer to meet. Make the most out of that brief time by sticking to your message and talking points. It's okay to repeat yourself to get the message across. Don't be afraid to say, "I don't know," in response to a question or offer to follow up with a correct, informed answer after the meeting.
- **Ask for advice.** Decisionmakers know their colleagues and how to navigate their agency or governing body. If your decisionmaker is interested in being an ally, ask that person who they might recommend you meet with next, whether it is another city councilmember or decisionmaker in your community. Those might be potential supporters as well.

MAKE THE ASK

If the decisionmaker is interested in the issues and supporting your coalition's cause, ask them to support your strategic goal. That may take the form of a request that they "author" and champion legislation such as a surveillance technology ordinance or ban. After making the ask, pause and give the official time to respond. Often, if an elected official hasn't taken a position on an issue, they may not commit to one during a meeting. Be open to an alternative commitment, no commitment at all, or any strategic advice they may have.

MAKE A PLAN

After you make the ask, discuss and agree on a schedule for next steps and speaking about the issue again. Ask when you should check back and who you should contact to find out how your official intends to respond to your request. Exchange contact information so you can be in touch. Leave the materials you compiled and thank the official and their staff for taking the time to meet with you. Offer to follow up with more information if the decisionmaker has outstanding questions.

AFTER THE MEETING

A meeting is just a first step. After the meeting, debrief it with your fellow attendees and compare notes. Make sure you are all on the same page about what took place in the meeting, what the official said (and didn't say), and any next steps you need to take. Designate a group member who will gather follow up information for the decisionmaker, and who will write and deliver the follow up message.

Finally, follow up with the elected official. At a minimum, send a thank you letter on behalf of the group to summarize the visit and respond to any questions or concerns, even if the official did not ultimately share your views. If the decisionmaker does not respond to your message or take an agreed-upon action after a few days or weeks, reach out again.

Be persistent but flexible. And remember: your local government works for you. Telling elected leaders what you want them to do and why is not an imposition. It's your right as a member of your community.

8. Publicly Advocate for Your Goal

Now it's time to make the public case for surveillance reform and your strategic goal. This public advocacy should complement and reinforce your efforts directly focused on decisionmakers.

SHARE YOUR MESSAGE WITH THE PUBLIC

Your public advocacy should begin well before your city council or board of supervisors vote on your surveillance issue. In addition to submitting a coalition letter to elected leaders, publicly promoting the letter and your messages for surveillance reform using a variety of tactics (op-ed articles, guest columns, social media posts, coalition letters to elected bodies, public comment at government meetings), you are ready to publicize the results of a public records request, using what you have found to argue for the necessity of change. The **Appendix** includes samples of these materials to get you started.

PREPARING PUBLIC COMMENT

Public comment at a public meeting is your opportunity to speak to your elected representatives and be heard, frame the choice and your solution, and demonstrate the in-person political support for your coalition's strategy.

Most cities and counties provide for public comment for items on a regular meeting agenda, so if your legislation or issue is up for a vote, you should try to get as many coalition partners as possible to speak at the meeting. The public comment process can be confusing, but it isn't difficult, even if you hate public speaking. This is democracy in action and it's critically important to take part.

There a few things you should do to prepare for the public meeting. First, confirm your item or issue will be up for discussion by checking the "regular" meeting agenda on the city council or board of supervisors' website. Second, give your coalition partners a heads up, providing the time of the meeting, relevant logistical details, and a sample public comment that can be customized (check out the **Appendix** for a template). These comments should briefly summarize the issue, why it matters, and how your coalition's strategic goal will address it and affirm community values. Your coalition's messaging should be a guide to what you say and how you say it.

PROVIDING PUBLIC COMMENT

The day has finally arrived, and now it's time to speak in support of your coalition's goals. Public speakers typically get between one and three minutes for comment (a good rule of thumb is that one hundred written words is equal to one minute of speaking time). After you arrive at the meeting, find the sign-up sheet or sign-up cards and submit your name and the agenda item number you wish to discuss.

When your name is called, step up to the podium, introduce yourself and your affiliation, then deliver your outline or prepared remarks slowly and clearly. It's OK to be nervous; just try to speak at a regular pace and make eye contact with your elected leaders when possible. You've got this!

9. Overcome Challenges, Build On Progress

It is difficult, time-consuming work to build a coalition, develop messaging, and carry out a public campaign to persuade decisionmakers. You will encounter challenges, but you can overcome them. And when you win, celebrate your victory. Build on the progress you've achieve, using it as an opportunity to reiterate your coalition's values and vision for social change.

OVERCOME CHALLENGES

Fighting secretive and unaccountable government surveillance isn't easy. But your coalition is strong and has the tools to overcome any opposition. Common roadblocks include opponents seeking to create a false choice between public safety and civil rights protections, delays in the consideration of your legislation, or a lack of public facts about the state of local surveillance.

Whatever the roadblock, you can overcome it by doubling down on your plan, your coalition's core strengths, and your positive, affirmative case for social change.

SECURE VICTORY AND CHOOSE A NEW STRATEGIC GOAL

If you are victorious, be vigilant and ensure that local officials comply with the change in policy your coalition helped achieve. Don't hesitate to reengage with local officials if you identify non-compliance or other issues. The strategies outlined in this toolkit, such as public records requests, messaging, and public comment, are all useful means to achieve full compliance by officials and make your victory a durable one.

At the same time, consider pursuing another strategy outlined in **Part 4**. If you passed a ban on facial recognition, now may be the time for a privacy commission to exercise oversight of surveillance issues. If you stopped the purchase of a surveillance technology, consider championing the passage of a surveillance technology ordinance that would require a consistent process for future proposals. A victory is a chance to move forward and deepen your coalition.

CELEBRATE WHAT YOU'VE ACCOMPLISHED

Organizing and being part of a coalition that advocates for civil rights is difficult, time-consuming work. A coalition of shared interests is an impressive achievement and an important foundation for future progress. Convene with your coalition partners to discuss lessons learned and shared goals, and to explore strategies for future collaboration. That is the best way to prepare for the many fights ahead.

REMEMBER WHY WE FIGHT

It's OK if your coalition is unable to achieve victory on its first try. The power, capacity, and relationships you built together are a resource for future work. Remember: in a democracy, you have the power to take control of these important decisions that impact your life. These decisions should be made by you, not by police and surveillance vendors behind closed doors.

We hope you'll use this toolkit to continue the fight. Whether you're uncovering surveillance practices, changing the public narrative about surveillance, or passing legislation, your work on behalf of the community is valuable and essential to our democracy.

SURVEILLANCE TOOLKIT: SAMPLE PUBLIC RECORDS REQUEST

This is a draft request for records under the California Public Records Act (CPRA). For further background on public records laws, check out guides by the Reporters' Committee for Freedom of the Press (here) and the California League of Cities (here). The Appendix also includes definitions of particular surveillance technologies to help you customize your requests. The blue text should be customized.

Month ##, 2020

Sent via e-mail

City Official
City Agency
Address
State, ZIP

Re: Public Records Act request related to surveillance technology

Dear City Official,

This is a request under the California Public Records Act (California Government Code § 6250 et seq.) and Article I, § 3 of the California Constitution. This request seeks records[1] regarding software designed to access information from surveillance technology.[2]

Records Requested

Please provide copies of the following:

1. All records referencing the design or features of surveillance technology, including but not limited, to marketing materials, e-mail promotions, product brochures, product manuals, and requests for specification.
2. All records referencing the public process related to the acquisition of surveillance technology, including but not limited to meeting agendas, meeting minutes, public notice, communications between your office and elected leaders, and analyses.

[1] Throughout this request, the term "records" includes but is not limited to any paper or electronic information, reports, evaluations, memoranda, correspondence, letters, emails, charts, graphs, flyers, meeting agendas, meeting minutes, training materials, diagrams, forms, DVDs, tapes, CDs, notes, or other similar materials.

[2] Thoughout this request, the term [Here, you can insert a definition of the particular surveillance technology that you seek records about. Defintions for common surveillance technologies can be located elsewhere in the Toolkit Appendix.]

3. All records of correspondence between an employee in your office and any company or company representative regarding surveillance technology, including but not limited to e-mails, calendar invitations, and instant messages.
4. All records of correspondence between employees in the City Department regarding surveillance technology, including but not limited to e-mails, calendar invitations, and instant messages.
5. All records referencing the purchase of surveillance technology, including requests for proposal, purchase orders, invoices, grant applications, sole source letters or justifications, and budget requests.
6. Any records referencing draft or finalized agreements related to surveillance technology, including e-mail negotiations, contracts, memoranda of understanding, terms of service, and master services agreements.
7. All records referencing policies governing surveillance technology, including policies that describe authorized uses, prohibited uses, applicable legal standards, limits on sharing with third parties, data security, and training requirements.

If you determine that some but not all of the information is exempt from disclosure and that you intend to withhold it, I ask that you redact it for the time being and make the rest available as requested. In any event, please provide a signed notification citing the legal authorities on which you rely if you determine that any or all of the information is exempt and will not be disclosed. If I can provide any clarification that will help expedite your attention to our request, please contact me at (###) ###-#### or you@email.com.

Because this request is on a matter of public concern, we request a fee waiver. We are also requesting that documents be provided in electronic format if at all possible. Doing so would eliminate the need to copy the materials and provides another basis for our requested fee waiver. If, however, such a waiver is denied, we will reimburse you for the reasonable cost of copying. Please inform us in advance if the cost will be greater than $50.

According to the California Public Records Act (California Government Code § 6253(c)), a response is required within 10 days. Thank you for your prompt attention to this matter. Please furnish all applicable records to us at you@email.com if in electronic format or, if in physical form, at your street address.

Sincerely,

SURVEILLANCE TOOLKIT: SAMPLE LETTER DISCUSSING CONCERNS WITH SPECIFIC SURVEILLANCE TECHNOLOGY PROPOSALS

A letter helps you articulate concerns with surveillance technology and your strategic goal, all while communicating the political power of your coalition. These letters follow a basic, structure: first, introduce your coalition, your issue and state your main ask of the elected leaders; second, explain the issue and the surveillance technology or proposal that you're concerned about; and finally, conclude by summarizing your points, restating your ask, and offering to meet or talk to discuss your perspective. Throughout your letter and wherever possible, center the impacts of surveillance on real people and your coalition partners. The blue text should be customized.

SAMPLE 1: LETTER EXPRESSING CONCERN ABOUT AUTOMATED LICENSE PLATE READER TECHNOLOGY PROPOSAL

Month ##, 2020

Mayor
Councilmember
Councilmember
Councilmember
Councilmember
Your City Council
Street address
City, CA ZIP

Dear City Council,

We are a community civil rights coalition and write to raise significant concerns with the Police Department's proposal to expand its use of automated license plate reader (ALPR) technology in our community. We urge the City Council to consider alternatives to surveillance that will keep our community safe without the severe costs to civil rights and civil liberties invited by ALPR.

ALPR systems - whether their cameras are attached to police cars or street lights - collect and store location information about drivers whose cars pass through their cameras' fields of view, which, after being matched to dates, times, and location, can be compiled into databases that reveal sensitive information about where our community members work, live, associate, and visit. No locality should acquire or deploy license plate readers without proper safeguards that protect all residents, given the invasiveness of the technology and the breadth of revealing information it can collect about individuals.

We know that ALPR systems have been misused to harm minority communities. For example, police have used license plate readers to target Muslim Americans by spying on mosques.[1] And before the advent of license plate readers, police monitored the license plates of LGBT people for purposes of extortion.[2] ALPR systems are easily misused: blind reliance by San Francisco police on these readers led to the wrongful detention of a black woman at gunpoint, triggering a multi-year civil rights lawsuit.[3] As with other surveillance technologies, police tend to deploy license plate readers disproportionately in poor areas, regardless of crime rates.[4]

These concerns have taken on a new urgency because ICE now accesses license plate information held by one of the largest ALPR vendors, Vigilant Solutions, access that may include detailed location information collected by local law enforcement agencies. Through this arrangement, ICE can tap into Vigilant's nationwide database of license plate and associated location records to target and deport our immigrant residents.[5]

The community should always have a voice in decisions about whether to acquire surveillance systems such as ALPR and the safeguards and accountability mechanisms that need to be in place to prevent warrantless, mass surveillance. To ensure this debate and oversight occurs, we also urge the City Council to consider an ordinance that requires that decisions about surveillance technology such as ALPR are subject to rigorous democratic debate and input by community members who are impacted by the use of such technologies. More than a dozen U.S. communities – including Berkeley, Oakland, and San Francisco – have adopted ordinances based on ACLU guidance and that require transparency, oversight, and accountability for all surveillance proposals.[6] Our residents deserve a voice in decisions such as these.

---

[1] Adam Goldman and Matt Apuzzo, *With cameras, informants, NYPD eyed mosques*, Associated Press, Feb. 23, 2012, https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques;

[2] Josh Hicks, *A few reasons the public might care about license-plate tracking*, Washington Post, Feb. 19, 2014, https://www.washingtonpost.com/news/federal-eye/wp/2014/02/19/a-few-reasons-the-public-might-care-about-license-plate-tracking/.

[3] Kade Crockford, *San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error*, ACLU, May 13, 2014, https://www.aclu.org/blog/privacy-technology/location-tracking/san-francisco-woman-pulled-out-car-gunpoint-because; Matt Cagle, *San Francisco – Paying the Price of Surveillance Without Safeguards,* ACLU of Northern California, May 22, 2014, https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards.

[4] Dave Maass and Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, Electronic Frontier Foundation, Jan. 21, 2015, https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data ("If you are driving through or parking your car in a neighborhood with a higher density of white families, you are less likely to be picked up by ALPR cameras…. Overlaying Census data for Black or African-American and Latinx or Hispanic populations show the converse of the white population.")

[5] Vasudha Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU, Mar. 13, 2019, https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data.

[6] *Making Smart Decisions About Surveillance: A Guide for Community Transparency, Accountability & Oversight*, ACLU of Northern California, https://www.aclunc.org/smartaboutsurveillance; Community

The risks to civil liberties and civil rights that ALPR technology creates are well-documented. The best way to ensure that our residents are safe from unnecessary intrusion into their personal lives and the misuse of their sensitive information is to reject the use of ALPR technology altogether. We urge the City to consider a public safety solution other than ALPR, which invites the creation of databases that are vulnerable to misuse that harms civil rights and residents. At a minimum, the City should press pause on any plans to deploy ALPR while it engages community members in a discussion about whether this surveillance technology is appropriate for our city, and the kinds of safeguards that should be in place whenever surveillance technology including drones are proposed. We would be happy to meet to discuss this issue.

Sincerely,

Control Over Police Surveillance (CCOPS), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.

SAMPLE 2: LETTER EXPRESSING CONCERN WITH DRONE PROPOSAL

Month ##, 2020

Mayor
Councilmember
Councilmember
Councilmember
Councilmember
Your City Council
Street address
City, CA ZIP

Dear City Council,

We are a community civil rights coalition and write to raise significant concerns with the City's proposed acquisition of unmanned aerial vehicles ("drones"). This drone proposal invites dragnet and discriminatory surveillance, and as a result threatens the privacy and civil rights of local residents. We urge the City Council to consider alternatives to drone-based surveillance that will keep our community safe without the severe costs to civil rights and civil liberties invited by these systems.

Drones offer unprecedented surveillance power to law enforcement agencies, and intrude into the public's privacy in a far more significant and invasive fashion than most investigative tools commonly used by police. Drones are small, agile, and capable of being fitted with high-powered cameras that monitor people without their knowledge or consent.[1] Given their power, drones can—and do—monitor people in their private homes, workplaces, and places of worship, as well as in public spaces and during public events like protests.[2] When coupled with powerful sensors such as high-resolution video cameras, facial recognition software, and other forms of biometric data collection programs, drones enable police to stockpile detailed information about individuals that those agencies traditionally would not be able to access. Drone surveillance

---

[1] "Due to the heights at which drones can fly, they are often beyond the range of sight for most people. In addition, drones can also be designed to be very small and maneuverable. This means drone surveillance often occurs without the knowledge of the individual being monitored." *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, Electronic Privacy Information Center (last visited March 8, 2018), https://epic.org/privacy/drones/.

[2] Jeff Stone, *UK police may use drones to monitor protests, siege operations*, International Business Times (January 5, 2016), http://www.ibtimes.com/uk-police-may-use-drones-monitor-protests-siege-operations-2250287.

poses a direct threat to civil rights: indeed, police in Northern California have previously deployed drones to monitor student and immigrants' rights protests.[3]

In light of these concerns, people overwhelmingly reject the use of drones by local law enforcement. When the Los Angeles Police Department proposed acquiring and using drones last year, Angelinos inundated LAPD with letters, public comments, and petitions opposing the deployment of drones. Prior to a vote on the program, LAPD received over 1,675 letters in response to requests for public comment on its proposed drone program, the vast majority of which urged LAPD to halt the program in its entirety.[4] The local pushback LAPD received related to its drone program is reflective of broader public sentiment against the use of drones for domestic surveillance.[5]

The community should always have a voice in decisions about whether to acquire surveillance systems such as drones and the safeguards and accountability mechanisms that need to be in place to prevent warrantless, mass surveillance. To ensure this debate and oversight occurs, we also urge the City Council to consider an ordinance that requires that decisions about surveillance technology such as drones are subject to rigorous democratic debate and input by community members who are impacted by the use of such technologies. More than a dozen U.S. communities – including Berkeley, Oakland, and San Francisco – have adopted ordinances based on ACLU guidance and that require transparency, oversight, and accountability for all surveillance proposals.[6] Our residents deserve a voice in decisions such as these.

---

[3] *See* Dave Maass & Mike Katz-Lacabe, *Alameda and Contra Costa County Sheriffs Flew Drones Over Protests*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/deeplinks/2018/12/alameda-and-contra-costa-county-sheriffs-flew-drones-over-protests (Dec. 5, 2018).

[4] Makeda Easter and Kate Mather*, Civilian oversight panel hears guidelines for LAPD use of drones*, (October 3, 2017), *available at* http://www.latimes.com/local/lanow/la-me-ln-lapd-drones-20171002-story.html. The public also expressed its opposition to the drone program in two separate petitions, one with over 1,900 signatories and another with more than 800 signatories. See "Drone-Free LAPD. No Drones, LA!", MoveOn.org Petitions, https://petitions.moveon.org/sign/drone-free-lapd-no-drones-1 (803 signatories as of March 4, 2018).

[5] *See* Terance Miethe, Miliaikeala SJ. Heen, & Emily Trosyhnski, *Public Attitudes About Aerial Drone Activities: Results of a National Survey (Research in Brief report*), CENTER FOR CRIME AND JUSTICE POLICY, https://www.unlv.edu/sites/default/files/page_files/27/Research-PublicAttitudesaboutAerialDroneActivities.pdf (July 2014). *See also* Stephen Rice, *Eyes In The Sky: The Public Has Privacy Concerns About Drones*, FORBES, https://www.forbes.com/sites/stephenrice1/2019/02/04/eyes-in-the-sky-the-public-has-privacy-concerns-about-drones/#135ac3d66984 (Feb. 4, 2019) (citing data from a study revealing that drone use generates fears of police and that the general public opposes ongoing drone surveillance).

[6] *Making Smart Decisions About Surveillance: A Guide for Community Transparency, Accountability & Oversight*, ACLU of Northern California, https://www.aclunc.org/smartaboutsurveillance; Community Control Over Police Surveillance (CCOPS), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance.

We urge the City Council not to approve the acqusition of a drone at this time. The City should engage community members in a discussion about whether this surveillance technology is appropriate for our city, and the kinds of safeguards that should be in place whenever surveillance technology including drones are proposed. We would be happy to meet to discuss this issue.

Sincerely,

SURVEILLANCE TOOLKIT: SAMPLE E-MAIL MESSAGE SEEKING A MEETING WITH CITY OFFICIALS

Below are examples of straightforward messages you can use to request a meeting with an elected official, and to follow up after the meeting. The blue text should be customized.

MESSAGE REQUESTING A MEETING:

Hi Councilmember Name,

I am a constitutent and a member of a community civil rights coalition. I would like to request a meeting to discuss an issue related to the use of surveillance technology in our community. Specifically, I would like to discuss the city department's acquisition and use of a surveillance technology, this technology's impact on civil rights and members of our community, and the need for city council oversight prior to any decision to acquire or use this technology.

I hope we can meet soon to discuss these important issues. Some times that we are available and my contact information are below. [List 3-5 available dates and hour-long windows of time.]

We look forward to hearing from you.

Sincerely,

Name
Organizational affiliation (if any)
Email address, Phone number

MESSAGE FOLLOWING-UP AFTER MEETING:

Hi Councilmember Name,

Thank you for meeting to discuss the city department's acquisition and use of surveillance technology. I appreciate you taking the time to discuss this issue. I wanted to follow up with some materials that we discussed in the meeting.

As a next step, we would like to ask that you request additional information from the city department about this technology and to facilitate a public discussion about it at an upcoming city council meeting.

I am also attaching the ACLU's draft model surveillance technology ordinance. This ordinance ensures surveillance technology proposals are subject to our local democratic process and that residents have a seat at the table for decisions about technologies such as drones, video cameras, and license plate readers. More than a dozen U.S. localities have adopted a version of this legislation.

Please let me know if you have any additional questions. We will be in touch.

Sincerely,

Name
Organizational affiliation (if any),
Email address, Phone number

SURVEILLANCE TOOLKIT: SAMPLE AGENDA FOR A MEETING WITH AN ELECTED OFFICIAL

Below is a sample agenda for a meeting with a local elected official. This sample agenda is focused on a Surveillance Technology Ordinance, but the same basic framework applies to any meeting with a local official. As explained by Part 7 of the Toolkit, an in-person meeting is an opportunity to explain the issues, why they matter and their impact on community members, and to ask for support for your coalition's preferred strategic goal. This sample agenda is designed to help you accomplish those goals. Remember: there is no one right way to run a meeting with an elected official.

Meeting with Councilmember

Date:

Coalition facilitator:

Introductions

1. Thank you, introductions, and note any connections to the elected leader's district, such as number of members within district and whether constituents are present.
2. State the goal of the meeting: To urge the elected leader to support your strategic goal (here, a Surveillance Technology Ordinance), and to answer any questions.

Key MESSAGES

1. Surveillance without oversight makes us less safe and less free. Our communities deserve a seat at the table, and the power to create safeguards and prevent abuse.
2. All of us should feel at home in our own neighborhoods. That's why public safety in the digital era must include transparency and accountability.
3. Decisions about our public safety should be made by the community acting through the local democratic process, not by police and surveillance vendors behind closed doors.

Key FACTS

1. At the heart of this legislation is the basic principle that communities should know about and control what surveillance technology the police are using. It requires a public debate and elected leader oversight over decisions to acquire or use surveillance technology.
2. This legislation makes sure the right questions are asked and answered about surveillance technology from the beginning. It will help us make smart decisions that keep communities safe and their rights intact.
3. This ordinance will build trust and protect our rights by bringing common sense oversight to surveillance in our city.

CLOSING

1. Ask the elected official (or staff) for their thoughts and questions on Ordinance.
2. Ask the elected official (or staff) if they will vote YES on Ordinance. If yes, thank them for their support and ask if they would co-sponsor the Ordinance. If the elected official doesn't commit, ask them if they have additional questions that you can answer and when a good time to follow up with them will be.
3. (Write down any follow-ups you promise in the meeting).

FAQ (try to think of your best answers to questions you expect to be asked)

Who is the legislator sponsoring this ordinance?

When do you expect this to be up for a vote?

Who is in your coalition and supporting this?

What does this legislation cover?

- This Ordinance covers the acquisition and use of surveillance technology by city departments, including the police. It ensures that the community has a seat at the table for these important decisions.
- The Ordinance covers all types of surveillance technologies commonly used in communities, including drones, video cameras, cell phone trackers, social media monitoring software, and predictive policing software.

SURVEILLANCE TOOLKIT: SAMPLE LETTER ASKING ELECTED LEADER TO INTRODUCE A SURVEILLANCE TECHNOLOGY ORDINANCE

This is an example of a letter to a local elected official explaining your coalition's support for a particular strategic goal, a Surveillance Technology Ordinance, and urging the official to sponsor (i.e., introduce and support) legislation related to that goal. You can send this meeting before or after you have met with that elected official in person. This letter can also be customized for outreach to potential coalition partners. The blue text should be customized.

Dear elected official,

We are a local coalition dedicated to protecting civil rights and civil liberties, including the right to be free from intrusive, discriminatory, and dangerous government surveillance. We write to urge you to sponsor an ordinance for our community that would institute basic transparency and oversight when decisions are made about technologies such as drones, automated license plate readers, and social media monitoring.

We know that when the city makes decisions about surveillance technology in the dark, it doesn't lead to the best outcomes for our City. [Here, provide an example of a time when surveillance technology was purchased in your community (or a neighboring one) without public knowledge or elected leader involvement.] For example, several years ago, our police department obtained a drone without notifying the public—and most City Councilmembers were unaware that they had approved the purchase.

A Surveillance Technology Ordinance would ensure that the public and elected leaders have a voice in decisions about surveillance. To ensure this, the ordinance requires:

- **Informed Public Debate & Council Approval at Earliest Stage of the Process** – Public notice, production and distribution of an easy-to-understand Surveillance Impact Report and opportunity for meaningful public input prior to seeking funding or otherwise moving forward with surveillance technology proposals;
- **Determination by Board That Benefits Outweigh Cost and Concerns** – The Board expressly considers costs (fiscal and civil rights) and determines whether surveillance technology is appropriate before moving forward.
- **Robust Surveillance Use Policy Approved by Board** – Board approval of a Surveillance Use Policy with robust civil rights, civil liberties, and security safeguards for all existing and new surveillance technology; and
- **Ongoing Oversight & Accountability** – Proper oversight of surveillance technology use and accountability through annual reporting and public review by the Board.

This ordinance has proven to be a workable model in more than a dozen US cities and counties, including San Francisco, Oakland, Berkeley, Davis, Palo Alto, and in Santa Clara County. Using the ordinance, residents and elected leaders are now able to have an informed public debate about new technology using the democratic process and to decide together whether, or how, to acquire or use new surveillance systems.

We would appreciate the opportunity to sit down to discuss our concerns and the need for this legislation here in our City. Please let us if you are available to further discuss this ordinance.

Sincerely,

SURVEILLANCE TOOLKIT: SAMPLE E-MAIL MESSAGE SEEKING A MEETING WITH CITY OFFICIALS

Below are examples of straightforward messages you can use to request a meeting with an elected official, and to follow up after the meeting. The blue text should be customized.

MESSAGE REQUESTING A MEETING:

Hi Councilmember Name,

I am a constitutent and a member of a community civil rights coalition. I would like to request a meeting to discuss an issue related to the use of surveillance technology in our community. Specifically, I would like to discuss the city department's acquisition and use of a surveillance technology, this technology's impact on civil rights and members of our community, and the need for city council oversight prior to any decision to acquire or use this technology.

I hope we can meet soon to discuss these important issues. Some times that we are available and my contact information are below. [List 3-5 available dates and hour-long windows of time.]

We look forward to hearing from you.

Sincerely,

Name
Organizational affiliation (if any)
Email address, Phone number

MESSAGE FOLLOWING-UP AFTER MEETING:

Hi Councilmember Name,

Thank you for meeting to discuss the city department's acquisition and use of surveillance technology. I appreciate you taking the time to discuss this issue. I wanted to follow up with some materials that we discussed in the meeting.

As a next step, we would like to ask that you request additional information from the city department about this technology and to facilitate a public discussion about it at an upcoming city council meeting.

I am also attaching the ACLU's draft model surveillance technology ordinance. This ordinance ensures surveillance technology proposals are subject to our local democratic process and that residents have a seat at the table for decisions about technologies such as drones, video cameras, and license plate readers. More than a dozen U.S. localities have adopted a version of this legislation.

Please let me know if you have any additional questions. We will be in touch.

Sincerely,

Name
Organizational affiliation (if any),
Email address, Phone number

SURVEILLANCE TOOLKIT: SAMPLE COALITION LETTER SUPPORTING SURVEILLANCE TECHNOLOGY ORDINANCE

As explained in Part 3 of the Surveillance Toolkit, a coalition letter is an opportunity to state your case – and demonstrate the political power of your coalition – in a single place for decisionmakers. A coalition support letter contains a few key elements: it explains who is in your coalition (you can include partner organizations' logos in the header of the letter), the surveillance technology issue in your community and why it matters, and a short explanation of your strategic goal and why they should support it. Submit your letter to the relevant elected body at least one week prior to the meeting where they will discuss your surveillance issue. The blue text should be customized.

Month ##, 2020

Mayor
Councilmember
Councilmember
Councilmember
Councilmember
Your City Council
Street address
City, CA ZIP

Dear City Council,

Re: Support for the Surveillance and Community Safety Ordinance

Dear Honorable Members of the City Council:

We are a local coalition dedicated to protecting civil rights and civil liberties, including the right to be free from intrusive, discriminatory, and dangerous government surveillance. We write to urge the City Council to adopt the proposed Surveillance and Community Safety Ordinance ("Surveillance Ordinance"). This legislation gives residents and elected leaders an important voice in decisions about surveillance technology, and its adoption would make our City a leader in protecting local residents from unaccountable and secretive police surveillance.

This Surveillance Ordinance is the result of a robust and open debate among the City's residents, civic organizations, and government stakeholders. The Ordinance is straightforward: it requires essential transparency, accountability, and oversight for all surveillance technology proposals, and it ensures that the public is informed of the civil rights and civil liberties impact before such tools are acquired and after they are used.

As the federal government turns its surveillance and enforcement powers on immigrants and Muslim Americans, and as a health crisis impacts the most vulnerable members of our society, this elected body has a special responsibility to enact strong measures that protect those very residents from harmful suspicionless monitoring, secretive technologies, and information-collection that can be exploited for discriminatory ends. This Ordinance is needed now to help protect the civil liberties and civil rights of all residents.

We urge this Committee to recommend that the City Council adopt it without delay.

Sincerely,

SURVEILLANCE TOOLKIT: SAMPLE COALITION LETTER SUPPORTING A BAN ON GOVERNMENT FACIAL RECOGNITION TECHNOLOGY

The following is a draft coalition letter in support of a ban on a particular surveillance technology. A coalition support letter contains a few key elements: it explains who is in your coalition (you can include partner organizations' logos in the header of the letter), the surveillance technology issue in your community and why it matters, and a short explanation of your strategic goal and why they should support it. Submit your letter to the relevant elected body at least one week prior to the meeting where they will discuss your surveillance issue. The blue text should be customized.

Month ##, 2020

Mayor
Councilmember
Councilmember
Councilmember
Councilmember
Your City Council
Street address
City, CA ZIP

Re: Support for Proposed Ordinance to Prohibit the Acquisition and/or Use of Face Recognition Technology

Dear Honorable Members of the City Council,

We are a local coalition dedicated to protecting civil rights and civil liberties, including the right to be free from intrusive, discriminatory, and dangerous government surveillance. We write to express strong support for the proposed prohibition on the City's acquisition and use of face recognition technology.

The legislation will safeguard residents against dangerous, invasive, and biased systems that endanger their civil rights and safety. We urge you to adopt the ordinance and position our city at the cutting-edge of municipal technology oversight, joining the ranks of cities from California to Massachusetts that have decided to ensure decisions about advanced surveillance technology are firmly under democratic control. This letter explains several reasons the Council should adopt the prohibition.

1. Face recognition technology grants City departments unprecedented power to identify and continuously monitor residents, amplifying historical bias against communities of color, immigrants, and other vulnerable residents.

Face recognition technology enables the government to automatically track residents' identities, whereabouts, associations, and even facial expressions. Using existing video cameras and officer-worn body cameras promised as a way to keep us safe, government agencies can create unfettered citywide networks that place our communities under continuous

surveillance. The powerful and automated nature of face recognition incentivizes the needless expansion of surveillance in our communities. People should not have to fear having their movements and private lives logged in a database simply for walking down the street. Face surveillance will make residents of our city less free. It will also lead to new violations of civil rights.

The harms from face recognition will disproportionately impact communities of color and immigrants. This is because face recognition systems connect to existing surveillance infrastructure and amplify biased policing and enforcement practices already present in these communities. Members of these groups are more likely to be tracked – and subject to government interventions – because they attended a political rally, visited an abortion clinic, or attended a religious service. Face recognition systems risk further criminalizing the lives of people of color and immigrants subject to their surveillance.

Face recognition databases also place the personal information and safety of residents at risk. In the absence of a prohibition, implementing a face recognition system in our City may lead to the creation of a sensitive database featuring the face prints of local residents or the use of a secretive private database, created without the consent of community members. Databases containing the face prints of residents may prove an attractive target for exploitation efforts and demands from agencies like ICE, which has already begun mining state databases using this technology. These sensitive biometric databases are vulnerable not only to such misuse, but also to data breaches. Yet unlike a password or a credit card number, a local resident cannot "reset" his or her face if it is compromised due to a breach of a City database.

2. Face recognition technology's demonstrated inaccuracies and biases threaten the civil rights and safety of residents—especially immigrant communities, communities of color, and women.

Multiple studies of facial recognition technology have concluded that it suffers from significant flaws and bias. In December 2019, the National Institute of Standards and Technology (NIST) released a landmark study of prominent facial recognition algorithms that found Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search. According to a peer-reviewed study by researchers at MIT, face recognition technology products perform poorly for people with darker skin and women. When ACLU ran photos of members of Congress through Amazon's "Rekognition" product last year, we found that 28 members of Congress incorrectly "matched" with mugshot booking photos of arrestees. Of the false matches, 39 percent were people of color, even though people of color make up only 20 percent of lawmakers in Congress.

Our City should refuse to test a technology that even has the potential to arbitrarily treat some local residents differently because of their skin color, sex, or other characteristic. The use of inequitable technology will invite unnecessary encounters with law enforcement, and misinformed decisions about the use of force.

But even when a face recognition algorithm is perfectly accurate, it is still vulnerable to other types of bias that pervade the databases and realities that underlie these systems. For example, since face recognition systems often use mugshot photos for matching purposes—and these

mugshot databases reflect the historical over-policing of communities of color—the matching databases used by these systems will frequently overrepresent people of color. Communities of color may be unfairly targeted by the gaze of these systems simply because they appeared in a database and were arrested or subjected to discriminatory policing in the past.

3. Voters overwhelmingly oppose government surveillance based on biometrics.

The proposed prohibition aligns with the will of local constituents. In a poll of likely 2020 California voters, 79 percent of Bay Area respondents opposed the government being able to monitor and track a person using biometric information. This view is held widely across generations, ethnic groups, and political parties, according to the poll.

4. Conclusion

The civil rights and civil liberties cost of facial recognition technology substantially outweigh this technology's theoretical benefits. In summary, we recommend the Council adopt the proposed legislation to protect residents from a technology that is primed for abuse, regardless of its accuracy or rules governing its use.

Sincerely,

SURVEILLANCE TOOLKIT: SAMPLE NARRATIVE & MESSAGING FRAMEWORK

A consistent communications strategy not only educates the public and decisionmakers, but also focuses your coalition and builds new political power. Articulate your values, the problem as you see it, and your solution. Use this narrative and your messages to inform how you talk about the Ordinance, whether you're writing a letter, making public comment, or holding an in-person meeting.The below sample messaging is from the campaign to pass San Francisco's historic legislation banning facial recognition and requiring oversight of surveillance technology.

Set out your core theme. This introduces the big idea and shows what you are fighting for. Start by writing a two or three sentence summary – this will be your topline messaging. Clearly frame the problem and how your solution will fix it. Think about what's at stake, and how each word you choose to use conveys the reason you're in this fight.

> *"Without public oversight of what surveillance technologies are introduced into our neighborhoods, invasive high-tech systems proliferate, jeopardizing our rights and our safety. Time and again, the harms of these technologies fall hardest on immigrants, activists, and people of color. The responsible and ethical answer is to create an open and inclusive process that prevents discriminatory surveillance and protects everyone."*

Describe your values. Connect to the audience and define the conversation in terms they care about. Remind your audience that surveillance is not synonymous with real safety.

> *"Surveillance without oversight makes us less safe and less free. Our communities deserve a seat at the table, and the power to create safeguards and prevent abuse."*

> *"All of us should feel at home in our own neighborhoods. That's why public safety in the digital era must include transparency and accountability. We can't allow technologies that let police track and control us run wild."*

> *"We shouldn't be test subjects for facial recognition, an invasive and dangerous technology that undermines our most fundamental civil liberties and freedoms."*

State the problem.

> *"Technologies like drones, social media surveillance, and facial recognition invade our private lives and create databases vulnerable to exploitation by the federal government."*

> *"Face surveillance has no place in this community. It gives police an unprecedented power to track and record who we are, where we go, and who we meet with."*

> *"The secret growth of ineffective, unaccountable, and discriminatory surveillance technologies is dangerous. It discourages activism, and can put people's lives and freedom at risk.*

Explain your solution. Demonstrate how the values of your audience are realized through engagement with your coalition.

> *"At the heart of this legislation is the basic principle that communities should know about and control what surveillance technology the police are using."*

> *"This legislation makes sure the right questions are asked and answered about surveillance technology from the beginning. It will help us make smart decisions that keep communities safe and their rights intact."*

> *"This ordinance will build trust and protect our rights by banning face recognition and bringing common sense oversight to surveillance in our city."*

Anticipate resistance. These are never easy conversations. Think about what is making people hesitate, or what arguments your opponents will use. Anticipating opposing views can help you overcome them.

> *"Real public safety requires communication, trust, and accountability. Decisions about surveillance technology should be made by community members acting through the democratic process, not by police or surveillance vendors behind closed doors.*

> *"Surveillance technologies that are bought and used in secret create systems that further fuel racist police violence, push people into the hands of ICE, and distract public resources that should be used to keep us healthy and safe."*

> *"It's unacceptable for police to hide their practices from the public. When surveillance is forced into the light, communities have the power to call out racist policing practices and stop discriminatory surveillance in its tracks."*

Call to action. This helps clarify the ask for your audience and members of the coalition.

> *"Our City is at the forefront of civic innovation. By passing this law, the city's elected leaders can redefine what tech leadership means."*

> *"This ordinance will put decisions about surveillance back where they belong: in the hands of the people. Come out to tonight's public meeting and voice your support!"*

With a shared narrative and messages in hand, your coalition is ready to start the next steps of your public advocacy.

Why Santa Clara County needs a surveillance transparency ordinance

By George Cammarotal, San Jose Resident & Community Organizer

Stingrays, Hailstorms, Triggerfishes, FLIRs, Amberjacks, NGI, Harpoons and ALPRS are not exactly household names to most Santa Clara County residents. The names sound like something out of “Moby Dick” meets a science fiction novel. But these pieces of high-tech surveillance equipment and more like them are being used now by local law enforcement, often without public knowledge, input or consent.

That is why Santa Clara County’s Board of Supervisors is considering a global surveillance equipment transparency ordinance. The proposed legislation covers all surveillance technology from cellphone interceptors to license plate readers to facial recognition software to those not invented yet. It dictates a cost-benefit analysis prior to purchase and a proposed usage policy — vetted in a public forum — and after purchase, an annual use audit to provide real data in real time.

High-tech gadgets can be useful tools in the investigation of crimes. But they can also be expensive boondoggles that rarely get used. Or worse, they can be used inappropriately and generate costly lawsuits and unjust outcomes.

This isn’t just a theoretical worry. A 2012 audit of National Security Agency intelligence operations documented 2,776 privacy violations in just one year, including a dozen incidents dubbed “LOVEINT” — meaning the use of the agency’s formidable surveillance apparatus to stalk current or former love interests of NSA staffers.

Policing is not exempt from the racial divides that cross this country. Profiling and targeting can and have been applied disproportionately to certain groups including African-Americans, Latinos, religious groups, young people and those marching in the street for redress of grievances.

As people become aware of the billions in federal funding and the extensive equipment provided directly to law enforcement for surveillance, they want to know when and why it is being considered, what it is intended to do, and what are the real costs before being deployed. They also want rules to ensure proper use, oversight, accountability and safeguards for individual rights.

Gov. Jerry Brown heeded that call in 2015, signing into law three bills that increased surveillance transparency: SB 178 (email privacy), SB 741 (cellphone interceptors) and SB 34 (license plate data usage). But new innovations in technology race ahead faster than equipment-specific legislation can possibly keep up with.

It’s understandable that some sectors of law enforcement have hesitated to embrace the ordinance wholeheartedly. They want to use every tool they can to do their job. But communities increasingly understand the need to ensure that time, energy and resources are not spent on systems that cost more and do less.

The county Finance and Government Operations Committee will review the surveillance transparency ordinance on April 14 at 3 p.m. at 70 West Hedding St. in San Jose. The meeting is open to the public and will have a comment period.

A lack of defined policies opens the door for mistakes, overreaches and even abuses, which thrive in the lack of established use policies. These mistakes create mistrust between law enforcement and residents, especially in communities where crime rates are higher — that are often most surveilled. Such mistrust makes community policing harder, as beat cops must depend on relationships within neighborhoods to get information and investigate and prevent crimes.

Following the public outcry about NSA warrant-less spying and the use of paramilitary equipment by local police, community members deserve reassurance that safeguards and public oversight will be in place if surveillance equipment is going to be used.

It's plain good government.

Why facial recognition is a threat to civil liberties

By Christie Hill, Deputy Advocacy Director, ACLU of San Diego and Imperial Counties

Protecting the freedoms that define America means making smart choices about surveillance and public safety in the 21st century. We're living in an age when machines can collect information about nearly everything we do — from the places we go to the emotions we feel to the people we hang out with — and have the capability to transmit this data to each other and to our government.

When nearly any device can be turned into a hyper-powerful surveillance tool, it's up to us to ensure technology makes us more, not less, safe. That's why we're gravely concerned about the invasive use of facial recognition software in police body cameras.

California state senators will soon vote on a bill to halt this practice. Assembly Bill 1215, the Body Camera Accountability Act, is a sensible public safety measure that will ensure you can walk down the street, attend a protest or ask police for help without having your face automatically scanned and recorded by the government.

In a free country, you don't have to identify yourself to every officer you pass on the street. Face-scanning body cameras would force you to do just that. Facial recognition software is now capable of analyzing live streaming video and identifying, tracking and cataloguing hundreds of people at once. If even a fraction of the estimated 67,200 local law enforcement officers in California were equipped with face-scanning body cameras, it will create a vast, roaming surveillance network that poses an immediate threat to our civil liberties and most fundamental freedoms.

When it comes to facial recognition software, the stakes couldn't be higher. Body cameras and facial recognition simply should not mix.

Top corporate players agree: Facial recognition is incompatible with police body cameras. Axon, the largest maker of police body cameras, recently announced that police should not use its cameras with facial recognition technology after examining the ethical issues such use would raise. Microsoft, a leading purveyor of facial recognition software, has also refused to provide facial recognition for police body cameras in California, recognizing the radical threat to civil rights such systems would pose.

When companies that stand to make huge profits off the marriage of these technologies can't bring themselves to do it, you know it's a bad idea.

As if the threat to our civil liberties isn't enough, facial recognition is inaccurate and racially biased. Study after study has proven that facial recognition software is dangerously likely to misidentify people with darker skin, especially black women. A widely publicized face recognition test recently misidentified 26 California legislators as arrestees in a mugshot database. More than half of them were legislators of color.

In the real world, misidentifications lead to wrongful stops, arrests and deadly use of force. We can't risk these kinds of mistakes. Instead of placing our faith in flawed technology, we must explore and adopt more humane approaches to public safety.

Even if facial recognition was perfectly accurate, if we allow body cameras to be used to track the public, other law enforcement agencies could begin mining the data. California is home to millions of immigrants and refugees from all over the world. And we already know the U.S. Immigration and Customs Enforcement has sought to use facial recognition to identify immigrants.

Those opposed to Assembly Bill 1215 call facial recognition a tool, but this description couldn't be less true when it comes to body cameras. It is reckless to use the public as test subjects with facial recognition-enabled police body cameras — and even to arrest people — when experts have concluded the technology is inaccurate and biased, when the largest body camera maker has announced it has no place on body cameras, and when we know ICE may demand access to body camera databases to target and deport Californians.

Adding facial recognition to body cameras will not only threaten our civil rights, it will undermine the public safety benefits of body cameras, which were only to be used to ensure police accountability. Indeed, 62 percent of likely 2020 California voters — across political parties and regions — strongly agree that body cameras should be used solely for oversight and accountability and not to track and identify people.

We shouldn't allow police to use technology that will make us less safe. Will body cameras that promised to increase public trust in police now be turned against our communities and used to violate our privacy and fundamental freedoms? It's up to us.

In a free country, you don't have to identify yourself to every officer you pass on the street. Face-scanning body cameras would force you to do just that.

New surveillance oversight law keeps communities safe and redefines tech leadership

Technology should work for the public good, not against it.

By Matt Cagle and Brian Hofer

Technology should work for the public good, not against it. Yet, San Francisco's city departments are currently permitted to use invasive, high-tech surveillance systems without consulting with residents or setting up basic rules to keep us safe. The harms that technologies like drones, automatic license plate readers, and face recognition can inflict are real and will fall hardest on our already-marginalized community members.

Next week, San Francisco's Board of Supervisors will vote on a law, authored by Supervisor Aaron Peskin, that ensures surveillance technology is considered and used responsibly by requiring public debate, clear use policies and a final Board vote. The ordinance also specifically prevents the city from deploying face surveillance technology.

The legislation is supported by the ACLU and a broad coalition representing immigrants, people of color, the homeless, the LGBTQ community, and others who are most subject to abusive surveillance. San Franciscans should ask their supervisors to pass this law.

Opponents of the legislation say that democratic oversight is impractical and would stop residents from sharing information with the city. But this process works – six other Northern California localities have adopted similar laws. And the ordinance explicitly allows city departments to accept and use tips from the community.

San Franciscans have experienced the danger of hastily deployed surveillance firsthand.

For instance, SFPD pulled over Denise Green, a Black woman, when a patrol car's automated license plate reader mistakenly indicated that her car was stolen. License plate readers are known to have a 10 percent error rate, but there were no policies requiring officers to verify automated readings. The police forced Ms. Green out of her car, to her knees, and held her at gunpoint.

Ms. Green's story demonstrates that unaccountable surveillance makes us less safe and less free. We know that surveillance technology is used most often against people of color and immigrants, who are, in turn, most in danger of racially biased violence.

This ordinance also recognizes the unprecedented dangers of face surveillance— a new technology that, as a New York Times experiment showed, exploits public camera feeds to secretly track people by scanning their faces against photo databases.

Experts have warned face recognition is inaccurate for people of color and women. But even if it were completely accurate, the city should still reject it.

Face surveillance is incompatible with a healthy democracy. In China, it's already being used to profile and control a largely Muslim ethnic minority. In one Chinese city, a once-bustling public square became desolate after this technology was installed.

If unleashed, face surveillance would suppress civic engagement, compound discriminatory policing, and fundamentally change how we exist in public spaces.

A young adult should have confidence that the city isn't logging their first visit to a gay bar. A Muslim resident should not worry their visit to a mosque will place them on a watchlist. And an immigrant should be able to show their face in public without fear of deportation.

Modern technology gives the government unprecedented surveillance powers. To put things in perspective: in 1973, the SFPD possessed intelligence files on over 100,000 people, including civil rights demonstrators, union members, and anti-war activists. These records took decades to amass.

Today, city police can stockpile information on 100,000 residents in a few hours.

The legislation before the Board brings these systems out of the shadows with a simple process of public accountability that also ensures that San Francisco lives up to its sanctuary promise. Indeed, a recent ACLU report found that the Trump administration is trying to use data from local surveillance systems to locate and deport immigrants.

An overwhelming majority of Bay Area voters support laws requiring oversight and transparency of government surveillance and oppose the government's use of face recognition.

San Francisco sits at the center of innovation; by passing this law, the Board of Supervisors can redefine what tech leadership means.

SPEAK UP Ask your supervisor to support the "Stop Secret Surveillance" ordinance by emailing Board.of.Supervisors@sfgov.org

Matt Cagle is a Technology and Civil Liberties Attorney at the ACLU of Northern California. Brian Hofer is the Executive Director of Secure Justice.

SURVEILLANCE TOOLKIT: SAMPLE COMMENTS FOR A PUBLIC MEETING

This is a sample public comment that you can customize for remarks at a City Council or Board of Supervisors meeting in support of your strategic goal. This is based on remarks presented by the ACLU of Northern California at an Oakland City Council meeting during the consideration of that City's Surveillance Technology Ordinance. The blue text should be customized.

As you draft your own remarks, keep in mind that speakers are often given a limited amount of time to present, usually between 1 to 3 minutes (generally, 125 words = 1 minute of speaking time).

Good evening,

My name is NAME and I represent a community coalition dedicated to protecting civil rights and civil liberties, including the right to be free from intrusive, discriminatory, and dangerous government surveillance.

Our coalition strongly encourages the City Council to vote **YES** on the Surveillance Technology Ordinance before you today. This ordinance is the result of conversations and input from community and city stakeholders, and will ensure that decisions about advanced surveillance technology are firmly under democratic control.

There is an urgent need for this legislation. We know surveillance technologies—particularly when acquired or used in secret, without the input from a diversity of community members and robust oversight—are disproportionately used to harm people of color, immigrants, and political activists.

This ordinance will help ensure that residents get a voice in key surveillance decisions that affect their neighborhoods, lives, and families. Real public safety requires that residents be part of decisions about whether to acquire technologies such as drones or cameras.

Finally, the ordinance will help ensure that our City's precious resources are not spent on costly, ineffective and invasive surveillance that creates more problems than it solves.

We strongly urge the committee to vote YES for transparency, democracy, and basic fairness by approving this surveillance ordinance.

Thank you.

SURVEILLANCE TOOLKIT: LEGAL DEFINITIONS FOR COMMON SURVEILLANCE TECHNOLOGIES

The following definitions describe various common surveillance technologies. You can use these definitions as part of legislation (e.g., a surveillance technology ordinance or ban on a particular technology) and in your public records requests.

Automated license plate readers (ALPR)

"Automated license plate recognition system" or "ALPR system" means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras, combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

Body cameras

"Officer camera" means a body-worn camera or similar device that records or transmits images or sounds and is attached to the body or clothing of, or carried by, a law enforcement officer.

Cell site simulators (e.g., Stingrays)

"Cellular communications interception technology" means any device that intercepts mobile telephony calling information or content, including an international mobile subscriber identity catcher or other virtual base transceiver station that masquerades as a cellular station and logs information about a mobile device.

Drones, or unmanned aerial vehicles (UAVs)

"Drone" or "Unmanned aerial vehicle" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.

Facial recognition

"Facial recognition technology" means an automated or semi-automated process that assists in identifying or verifying an individual, or captures information about them, based on the physical characteristics of an individual's face.

Predictive policing

"Predictive Policing Technology" means software that is used to predict information or trends about crime or criminality in the past or future, including but not limited to the characteristics or profile of any person(s) likely to commit a crime, the identity of any person(s) likely to commit crime, the locations or frequency of crime, or the person(s) impacted by predicted crime.

Location tracker

"Location tracker" is any device or service designed to seek or obtain location information. "Location information" means any information that helps to ascertain the location of an individual or particular electronic device that, in whole or in part, is generated or derived from the operation of an electronic device, including but not limited to a cell phone, smartphone, cell site, global positioning system, cell-site simulator, digital analyzer, stingray, triggerfish, amberjack,

kingfish loggerhead, or other electronic device, including both historical and real-time information.

Networked surveillance doorbell system

“Networked surveillance doorbell system” means any software that provides access to a network consisting of cameras or other recording devices mounted on private property and capable of monitoring, analyzing, or recording private property, the area around private property, and areas accessible to the public, including but not limited to public streets, sidewalks or common areas of public housing complexes.

Social media surveillance software

“Social media surveillance software” means any service or software that enables the monitoring, searching, collection, or analysis of user-generated content located on social media services. Examples of such social media services include, but are not limited to, Facebook, Instagram, Twitter, TikTok, Pinterest, Reddit, and SnapChat. “Social media surveillance software” does not include a mobile application or website operated by a social media service.

Radio frequency identification (RFID)

"Identification device" means any item, application, or product that is passively or actively capable of transmitting personal information, including, but not limited to, devices using radio frequency technology.

Video surveillance

“Video surveillance” means a digital recording surveillance system capable of monitoring, analyzing, or recording areas accessible to the public, including but not limited to, public streets, sidewalks or common areas of public housing complexes.

SURVEILLANCE TOOLKIT: MODEL LEGISLATION FOR A SURVEILLANCE TECHNOLOGY & COMMUNITY SAFETY ORDINANCE

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, reviewed by policymakers, and enforcement mechanisms.

MODEL ORDINANCE TEXT

ORDINANCE NO. _____

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF ######## ADDING ARTICLE ####

OF THE ######## MUNICIPAL CODE REGARDING OVERSIGHT OF THE CITY'S ACQUISITION AND/OR USE OF SURVEILLANCE TECHNOLOGY

WHEREAS, the City Council finds it essential to have an informed public debate as early as possible about decisions related to surveillance technology.

WHEREAS, the City Council finds that no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution, as well as Sections 1, 2, and 13 of Article I of the California Constitution.

WHEREAS, the City Council finds that, while surveillance technology may threaten the privacy of all of us, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.

WHEREAS, the City Council finds that decisions regarding if and how surveillance technologies should be funded, acquired, or used, and whether data from such technologies should be shared, should not be made until meaningful public input has been solicited and given significant weight.

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any surveillance technology is deployed; and

WHEREAS, the City Council finds that, if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF ######## DOES HEREBY ORDAIN AS FOLLOWS:

SECTION 1. Article #### is hereby added to ######## Municipal Code to read as follows:

1.1 Title.

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

1.2 City Council Review Mandatory for Surveillance Technology Decisions

(a) A City department must obtain City Council approval by ordinance of a Surveillance Use Policy following a public hearing conducted at a regular City Council meeting, prior to engaging in any of the following:

(1) Seeking funds for a 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 for the purpose of acquiring surveillance technology;
(2) Acquiring or borrowing a new surveillance technology, including, but not limited to, acquiring such technology without the exchange of monies or consideration;
(3) Using new or existing a surveillance technology for a purpose, in a manner or in a location not previously approved by the City Council in accordance with this Act; or
(4) Entering into an agreement, including a written and oral agreement, with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data-sharing agreements.

1.3 Surveillance Impact Report and Surveillance Use Policy Submission

(a) The City department seeking approval under Section 1.2(a) shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy via an informational staff report on a regular City Council meeting consent calendar at least forty-five (45) days prior to the public hearing, required under Section 1.2(a). The informational staff report shall be posted on the City website with the relevant City Council agenda at least thirty (30) days prior to the public hearing.
(b) The City Council may request revisions to the Surveillance Impact Report or Surveillance Use Policy submitted by the City department.

1.4 Standard for Approval

(a) The City Council shall only approve a request to fund, acquire, or use a surveillance technology under Section 1.2(a) of this Act if it determines the benefits of the proposed surveillance technology outweigh its costs, that the Surveillance Use Policy will safeguard

civil liberties and civil rights, that no alternative with lesser economic cost or impact on civil rights or liberties would be as effective, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or group.

1.5 Compliance for Existing Surveillance Technology

(a) A City department or departments possessing or using surveillance technology prior to the effective date of this Article shall submit or jointly submit a proposed Surveillance Use Policy no later than one hundred twenty (120) days following the effective date of this Article for review and approval by the City Council pursuant to Sections 1.2.
(b) If a City department is unable to meet this 120-day timeline, the Department may notify the Board in writing of the department's request to extend this period and the reasons for that request. The City Council may grant City departments extensions of up to 90 days beyond the 120-day timeline to prepare and submit a proposed Surveillance Use Policy.
(c) If the City Council has not approved the continuing use of surveillance technology, including the Surveillance Impact Report and Surveillance Use Policy, within one hundred eighty (180) days of their submission to the City Council, the City department shall cease its use of the surveillance technology and the sharing of surveillance data therefrom until such time as City Council approval is obtained in accordance with this Act.

1.6 Oversight Following Council Approval

(a) A City department that obtains approval under Section 1.2 of this Act must submit to the City Council, and make available on its website, an Annual Surveillance Report for each surveillance technology used by the City department within twelve (12) months of Board approval, and annually thereafter on or before November 1. If the City department is unable to meet the deadline, the department head shall notify the City Council in writing of staff's request to extend this period, and the reasons for that request. The City Council may grant reasonable extensions for good cause.
(b) Based upon information in the Annual Surveillance Report, the City Council will, at a public hearing during a regular City Council meeting, reassess whether that surveillance technology as used continues to meet the standard of approval set forth in Section 1.4. If it does not, the City Council shall consider (1) directing that the use of the surveillance technology cease; (2) requiring modifications to the Surveillance Use Policy that are designed to address the Board's concerns; and/or (3) directing a report-back from the department regarding steps taken to address the Board's concerns.

1.7 Prevention of Secret Surveillance Technology Contracts and Agreements

(a) It shall be unlawful for the City or any City department to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such future contracts or agreements, including, but not limited to, non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Act shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Act.

(b) To the extent permitted by law, the City shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

1.8 Enforcement

(a) Any violation of this Article 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 Article. An action instituted under this paragraph shall be brought against the City of ########, and if necessary to effectuate compliance with this Article or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third party, except a city employee, with possession, custody, or control of data subject to this Article.

(1) Prior to the initiation of any legal proceeding under subsection (a), the City of ######## shall be given written notice of the violation(s) and an opportunity to correct such alleged violation(s) within 30 days of receipt of the notice.
(2) If the alleged violation is substantiated and subsequently cured, a notice shall be posted in a conspicuous space on the City's website that generally describes the corrective measure(s) taken to address the violation(s).

(b) A court shall award costs to the prevailing plaintiff in any action brought to enforce this Article and any reasonable attorney's fees as may be awarded pursuant to State law.
(c) Nothing in this Article is intended to, or shall be interpreted to, conflict with the Constitution of the United States, the Constitution of the State of California, or with any State or federal law.

1.9 Definitions

For purposes of this Article, the following words, terms and phrases shall have these definitions:

(a) "Annual Surveillance Report" means an annual written report concerning a specific surveillance technology. The Annual Surveillance Report will include all of the following:

(1) A general description of how the surveillance technology was used;
(2) A general description of whether and how often data acquired through the use of the surveillance technology item 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);
(3) A summary of community complaints or concerns about the surveillance technology item;
(4) The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;
(5) Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;
(6) Statistics and information about any related Public Records Act requests;

(7) 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;
(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;
(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.
(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.

(b) The Annual Surveillance report will not contain the specific records that a surveillance technology item collects, stores, exchanges, or analyzes and/or information protected, restricted and/or sealed pursuant to State and/or federal laws, including information not required to be released by the Public Records Act.
(c) “City Department” means any City department and its officers and employees.
(d) “Personal Communication Device” means a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet-accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.
(e) “Surveillance Impact Report” means a written report including at a minimum the following:

(1) Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
(2) Information on the proposed purpose(s) for the surveillance technology;
(3) If applicable, the location(s) it may be deployed and crime statistics for any location(s);
(4) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;
(5) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
(6) An assessment identifying with specificity (1) Any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and (2) what specific, affirmative measures will be implemented to safeguard the public from those potential adverse impacts.
(7) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis; and
(8) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights, or civil liberties abuses.

(f) “Surveillance Technology” means any software, 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, biometric, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group.

(1) “Surveillance technology” includes, but is not limited to: international mobile subscriber identity (IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers; closed-circuit television cameras; gunshot detection hardware and services; video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; mobile DNA capture technology; biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; software designed to monitor social media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network.

(2) “Surveillance technology” does not include the following devices, hardware or software:

i. Office hardware, such as televisions, computers, credit card machines, copy machines, telephones, and printers that are in widespread use by City departments and used for routine City business and transactions;

ii. City databases and enterprise systems that contain information kept in the ordinary course of City business, including, but not limited to, human resources, permits, licenses, and business records;

iii. City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases;

iv. Information technology security systems, including firewalls and other cybersecurity systems;

v. Physical access control systems, employee identification management systems, and other physical control systems;

vi. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

vii. Manually-operated technological devices used primarily for internal City and department communications and are not designed to surreptitiously collect surveillance data, such as radios, personal communication devices, and email systems;

viii. Manually-operated, non-wearable, handheld cameras, audio recorders and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;

ix. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment;

x. Computers, software, hardware, or devices used in monitoring the work and work-related activities involving city employees, contractors and volunteers or used in conducting internal investigations involving city employees, contractors and volunteers;
xi. Parking Ticket Devices;
xii. Police department interview room, holding cell, and police department internal security audio/video recording systems;
xiii. Police department computer-aided dispatch (CAD), records/case management, Live Scan, booking, Department of Motor Vehicles, California Law Enforcement Telecommunications Systems (CLETS), 9-1-1, and related dispatch and operation or emergency services systems;
xiv. Police department early warning systems.

(g) "Surveillance Use Policy" means a publicly-released, legally enforceable written policy governing the City department's use of a specific surveillance technology that, at a minimum, includes all of the following:

(1) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.
(2) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use and uses of the surveillance technology that will be expressly prohibited.
(3) Data Collection: What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology, what types of data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize and delete such data.
(4) Data Access: The category of individuals who can access or use the collected information, how and what circumstances data collected with surveillance technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.
(5) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.
(6) Data Retention: The limited time period, if any, that information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Use Policy, 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.
(7) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.
(8) Third Party Data Sharing: Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the surveillance technology operated by the City department, including any required justification or legal standard necessary to share that data, and how it will ensure that any entity sharing or receiving such data complies with the Surveillance Use Policy.
(9) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

(10) 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 record keeping 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.

(11) Complaints: What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and how the municipal entity will ensure each question and complaint is responded to in a timely manner.

1.11 Severability

The provisions of this Article are declared to be separate and severable. The invalidity of any clause, phrase, sentence, paragraph, subdivision, section or portion of this Article, or the invalidity of the application thereof to any person or circumstance, shall not affect the validity of the remainder of this Article, or the validity of its application to other persons or circumstances.

SECTION 2. The City Clerk shall certify to the adoption of this Ordinance and shall cause the same or a summary thereof to be published as required by law.

SECTION 3. This Ordinance shall take effect and be in full force and effect thirty (30) days from and after the date of its final passage and adoption.

INTRODUCED on the ___ day of _____, 2020, and PASSED AND ADOPTED by the City

Council of the City of ####### on this _____ day of _____, 2020, by the following vote:

SURVEILLANCE TOOLKIT: MODEL LEGISLATION FOR A BAN ON FACIAL RECOGNITION (OR OTHER SURVEILLANCE TECHNOLOGY)

This is an example of language that your City Council can adopt as an ordinance to prohibit (ban) the acquisition or use of facial recognition or surveillance technology by city departments. Your community can adopt this as a standalone ordinance, or as part of a Surveillance Technology & Community Safety Ordinance. Your coalition will need to update the legislation findings (e.g., "Whereas…") if you customize this model to pursue a ban on a different technology.

ORDINANCE NO. _____

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF ######## ADDING ARTICLE ####

OF THE ######## MUNICIPAL CODE REGARDING A PROHIBITION ON THE CITY'S ACQUISITION AND USE OF FACIAL RECOGNITION TECHNOLOGY

WHEREAS, the City Council finds that the propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring; and

WHEREAS, the City Council finds that facial recognition have the potential to grant government entities the unprecedented power to secretly identify, monitor, and locate people simply going about their daily lives, threatening Californians' privacy, liberty, safety and freedom as guaranteed by the California Constitution.

WHEREAS, the City Council that the use of biometric surveillance systems to watch, categorize, monitor and record the activities and movements of all Californians disproportionately impacts people of color, women, immigrants, LGBTQ people, and political activists of all backgrounds. Bias, accuracy issues, and stereotypes built into biometric surveillance systems pose a threat to Californians.

WHEREAS, the City Council recognizes the emerging need to protect the public safety, privacy and civil rights of their residents, a growing number of local governments have adopted laws that prohibit the use of facial recognition and other biometric surveillance technology. More than half a dozen U.S. cities, including Oakland, Berkeley, and San Francisco have passed bans on the government use of facial recognition.

SECTION 1. Article #### is hereby added to ######## Municipal Code to read as follows:

(a) It shall be unlawful for any City Department to obtain, retain, access, or use:

(1) facial recognition technology; or

(2) any information obtained from facial recognition technology.

(b) A City Department's inadvertent or unintentional receipt, retention access to, or use of any information obtained from facial recognition technology shall not be a violation of this subsection, provided that:

(1) The City Department does not request or solicit its receipt, access to, or use of such information; and

(2) The City Department creates a log of such receipt, access to, or use and within seven days of the event, submits that log to the City Council for inclusion in the City Council's subsequent Regular Meeting Agenda.

(b) "Facial recognition technology" means an automated or semi-automated process that assists in identifying or verifying an individual, or captures information about them, based on the physical characteristics of an individual's face.

(c) "City Department" means any City department and its officers and employees.

(d) Any violation of this Article 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 Article. An action instituted under this paragraph shall be brought against the City of #######.

(e) No data collected or derived from any use of facial recognition in violation of this Article, and no evidence derived therefrom, may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority subject to the jurisdiction of [name of government unit]. Data collected or derived in violation of this law shall be considered unlawfully obtained, and shall be deleted upon discovery.

(f) A court shall award costs to the prevailing plaintiff in any action brought to enforce this Article and any reasonable attorney's fees as may be awarded pursuant to State law.

SURVEILLANCE TOOLKIT: MODEL LEGISLATION TO FORM A PRIVACY ADVISORY COMMISSION

This is model legislation that your community can customize and that your local City Council could adopt to form a Privacy Advisory Commission, based on the legislation that formed Oakland's own Commission of this type. This is just a model and a starting point: you should decide on a set of duties and a Commission composition that matches your City's needs.

ORDINANCE NO. _____

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF ######## ADDING ARTICLE ####

OF THE ######## MUNICIPAL CODE ESTABLISHING A COMMUNITY PRIVACY ADVISORY COMMISSION, PROVIDING FOR THE APPOINTMENT OF MEMBERS THEREOF, AND DEFINING THE DUTIES AND FUNCTIONS OF SAID COMMISSION

SECTION 1. ESTABLISHMENT

Pursuant to the Charter of the City of YOUR CITY, there is hereby created an YOUR CITY Privacy Advisory Commission (hereinafter referred to as the "Privacy Commission" or "Commission").

SECTION 2. DUTIES AND FUNCTIONS

It shall be the duty and function of the Privacy Commission to:

(a) Provide advice and technical assistance to the City of YOUR CITY on best practices to protect the privacy and civil rights of residents in connection with the City's purchase and use of surveillance equipment and other technology that collects, analyzes, processes, or stores information about the residents of YOUR CITY.

(b) Conduct meetings and use other public forums to collect and receive public input on the above subject matter.

(c) Draft for City Council consideration, model legislation relevant to the above subject matter, including, but not limited to, a Surveillance Technology Ordinance.

(d) Submit annual reports and recommendations to the City Council regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.

(e) Provide analyses to the City Council of pending federal, state and local legislation relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles or processes the information of residents.

(f) The Privacy Commission shall make reports, findings and recommendations either to the City Administrator or the City Council, as appropriate. An annual report will be presented in writing to the City Council. The Commission may submit recommendations to the City Council following submission to the City Administrator.

SECTION 3. MEMBERSHIP AND QUORUM

(a) The Commission shall consist of nine (9) members, at least six (6) of whom are YOUR CITY residents. Pursuant to Section 601 of the Charter, members of the Commission shall be appointed by the Mayor subject to confirmation by the affirmative vote of five members of the Council. Each Councilperson may recommend, shall nominate for the Mayor's consideration, his/her own recommendation or selection for Commission member.

(b) Five (5) members shall constitute a quorum.

(c) Each commission member shall serve as a volunteer without pay.

(d) The members shall be appointed to overlapping terms of three (3) years beginning on March 15th of each year and ending on March 15th three years later, or until a successor is appointed and confirmed, pursuant to Section 601 of the City Charter. An appointment to fill a vacancy shall be for the unexpired term only. To assure that terms overlap, appointments shall be as follows: three (3) initial members will serve a three-year initial term, three (3) initial members will serve a two-year initial term, and the other three (3) initial members will serve a one-year initial term.

(e) In the event an appointment to fill a vacancy has not occurred by the expiration of a member's term, that member may remain in a holdover capacity for up to one year, only following the expiration of his or her term or until a replacement is appointed, whichever is earlier.

(f) No member of the Privacy Commission shall serve more than three (3) consecutive terms.

(g) All members of the Privacy Commission shall be persons who have an interest in privacy rights as demonstrated by work experience, being a member of a group impacted by historical surveillance, civic participation, and/or political advocacy. No member may be an elected official.

(h) No member may have a financial interest, employment, or policy-making position in any commercial or for-profit facility, research center, or other organization that sells surveillance equipment or profits from decisions made by the Commission.

SECTION 4. VACANCY AND REMOVAL

(a) A vacancy on the Privacy Commission will exist whenever a member dies, resigns, or is removed, or whenever an appointee fails to be confirmed by the Council within 60 days of appointment. Vacancies shall be filled for any unexpired term provided, however, that if the Mayor does not submit for confirmation a candidate to fill the vacancy within 90 days of the date the vacancy first occurred, the Council may fill the vacancy. If the Mayor does submit for confirmation a candidate to fill a vacancy within the 90-day time frame and the Council does not confirm the candidate, the 90- day period shall commence anew. For purposes of this Section, a seat filled by a holdover appointment will be considered vacant as of the expiration of the holdover's prior term of office.

(b) A member may be removed for cause, after a hearing, by the affirmative vote of at least six (6) Council members.

SECTION 5. COMMISSION GOVERNANCE

a. OFFICERS AND ELECTIONS

At the first regular meeting, and subsequently at the first regular meeting of each year, members of the Privacy Commission shall elect a chairperson and a vice chairperson.

b. MEETINGS AND VOTING

The Privacy Commission shall meet at an established regular interval, day of the week, time, and location suitable for its purpose. Such meetings shall be designated regular meetings. Other meetings scheduled for a time or place other than the regular day, time and location shall be designated special meetings. Written notice of special meetings shall be provided to the Privacy Commission members, and all meetings of the Commission shall comport with any City or State open meetings laws, policies, or obligations. The Privacy Commission shall, in consultation with the City Administrator, establish bylaws, rules and procedures for the conduct of its business by a majority vote of the members present. Voting shall be required for the adoption of any motion or resolution. Any action by the Commission shall be approved by a majority of members present, provided a quorum exists.

c. STAFF

Staff assistance may be provided to the Privacy Commission as determined by the City Administrator, pursuant to his or her authority under the Charter to administer all affairs of the City under his or her jurisdiction.

SECTION 6. SEVERABILITY

If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause or phrase thereof, irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

SECTION 7. CODIFICATION

The City Clerk shall codify this ordinance upon approval of the code numbering as to formby the City Attorney.

SECTION 8. EFFECTIVE DATE

This ordinance shall become effective immediately on final adoption if it receives six or more affirmative votes; otherwise it shall be effective upon the seventh day after final adoption.

SURVEILLANCE TOOLKIT: ONE-PAGER SUMMARY OF SURVEILLANCE TECHNOLOGY AND COMMUNITY SAFETY ORDINANCE

FACT SHEET

Surveillance Technology & Community Safety Ordinance

(Councilmember _____)

The Problem

Modern surveillance technologies can collect sensitive information about our private lives without our knowledge or consent. Technologies such as drones, license plate readers, video cameras, and online monitoring software can easily be misused to discriminate, invade privacy, and chill First Amendment freedoms.

And surveillance technology is quickly growing more powerful - new face recognition surveillance systems give the government the unprecedented ability to automatically track who we are, where we go, and even our facial expressions.

The deployment of surveillance technology, which often occurs in secret, disproportionately harms immigrants, Muslim-Americans, political protesters, and the LGBTQ community, resulting in the collection of sensitive information about their lives that is ripe for misuse. Databases generated by these technologies are vulnerable to breach and other exploitation efforts, including by agencies like ICE.

Smart public safety decisions and the protection of all community members require that the City ensure public debate and community involvement in decisions about whether to acquire or use surveillance technology. Real public safety requires that residents have a voice in these decisions.

The Solution

The **Surveillance Technology & Community Safety Ordinance** ensures that residents and the local democratic process are in control of local surveillance decisions made in the City.

- The **Ordinance** creates a transparent process for considering surveillance technology proposals and gives local elected officials and residents a central role in decisions about whether to acquire or use it.
- The **Ordinance** ensures that there are strong rules to prevent misuse and harm for any surveillance technology acquired or used by City Departments.
- Finally, the **Ordinance** requires periodic assessments of surveillance technologies being used by the City to ensure that their costs – both to civil rights and to taxpayers – do not outweigh any potential benefits.

This Ordinance is based on a workable model: Seven California communities and thirteen localities nationwide have passed legislation of this type ensuring community members have a seat at the table for important decisions about surveillance

SURVEILLANCE TOOLKIT: CHECKLIST FOR ASSESSING A SURVEILLANCE USE POLICY

There should be enforceable written rules for every type of surveillance technology used by a government agency. The following checklist is designed to help you assess whether a written surveillance use policy meets the bare minimum requirements for protection of civil rights and civil liberties. As you review a written policy, look for shortcomings, omissions, or vague language that you can highlight for decisionmakers and in other advocacy.

SURVEILLANCE USE POLICY CHECKLIST		
Purpose of the technology	Does the policy list the specific purpose(s) of that type of surveillance technology?	**YES/NO**
Specific authorized & prohibited uses	Does the policy specifically explain the scenarios or circumstances when the agency may use the surveillance technology?	**YES/NO**
Data that can be collected	Does the policy specifically say what information the technology can be used to collect?	**YES/NO**
Data access instructions/ restrictions	Does the policy specifically say who can access or use any collected information, and under what conditions?	**YES/NO**
Data protection	Does the policy describe safeguards that protect information from unauthorized access, such as encryption, user login controls, or employee access limits?	**YES/NO**
Data Retention	If data is collected and recorded/retained, does the policy state how long collected data may be retained?	**YES/NO**
Public Access	Does the policy describe how members of the public, including criminal defendants, can access information about the technology and its use?	**YES/NO**
Third party data sharing	Does the policy specifically say whether and/or how non-City/County entities may get access to information collected with this technology? If yes, are there restrictions on that access?	**YES/NO**
Training	Does the policy describe what training is required for officers or employees who will use the technology or access the data?	**YES/NO**
Auditing and oversight	Does the policy describe how use of the technology and data will be audited, such as internal recordkeeping, automated process, or third party oversight?	**YES/NO**
Legally enforceable	Does the policy set forth consequences for misuse? Are they enforceable in a court or via a lawsuit?	**YES/NO**