

COMPLAINT DEADLINES REPORT

INVESTIGATIONS										
NO.	Complainant	Filed Date	Incident Date	Notice of Allegations Due (20 Bus. Day)	Notice of Allegations Issued	BOI Packet (80 days)	BOI Packet Issued	BOI Findings Report Goal (105 days)	120 Days	STATUS
2391		01/25/16		02/22/16	02/01/16	04/14/16	04/20/16	05/09/16	05/24/16	BOI continued*
2395		03/09/16		04/06/16	03/16/16	05/28/16	05/13/16	06/22/16	07/07/16	BOI continued**
2400		06/06/16		07/01/16	06/30/16	08/25/16	08/24/16	09/19/16	10/04/16	BOI 9/12
2402		08/17/16		tbd		tbd		tbd	n/a	LATE/pending approval

*tolled from 5/5 at officer's request

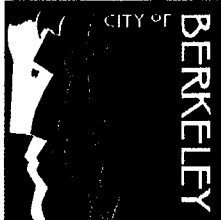
**officer unavailability

MEDIATION										
NO.	Complainant	Filed Date	Date of Election	Notice of Election to Officer Due (5 bus day)	Notice of Election Issued	Officer Agreed to Mediation	SEEDS Referral Date	Date of Mediation	Notice of Closure to Comm.	STATUS
2396		03/10/16	03/10/16	03/17/16	03/14/16	Y	03/31/16	09-06-2016		initially delayed*
2401		07/07/16	07/07/16	07/14/16	07/08/16	Y	07/14/16	08-29-2016	9-14-16	initially delayed*
2403		08/23/16	08/23/16	08/30/16	08/23/16	1 of 2				pending ofc. agreement
2404		08/17/16	08/17/16							LATE/pending approval
2407		08/30/16	09/09/16	09/16/16	09/09/16					pending ofc. agreement

*officer unavailability

POLICY REVIEWS								
NO.	Complainant	Filed Date	Notice of Complaint to BPD	Due to Comm (30 days or next mtg.)	Initial Commission Meeting Date	Commission Resolved Y/N	Admin. Closure Due	STATUS
2377	DENNEY, CAROL	06/22/15	07/10/14	07/22/15	07/08/15	n		Investigation
2384	PITCHER, STEPHEN	09/21/15	09/23/15	10/21/15	10/14/15	n		Investigation
2406	KEENLEY, JAMES	08/30/16	08/30/16	09/14/16	09/14/16			pending approval





Office of the City Manager

MEMORANDUM

Date: September 12, 2016
To: Katherine J. Lee, Police Review Commission Officer
CC: George Perezvelez, Chair, Police Review Commission
From: *DWR* Dee Williams-Ridley, City Manager
Subject: **Standard of Proof**

I received a letter from the Police Review Commission (PRC) Chair George Perezvelez requesting that I explain my reasons for not implementing the change to the burden of proof proposed by the PRC. Mr. Perezvelez stated that the PRC had decided to amend the standard of proof from the "clear and convincing evidence" standard to a lower "preponderance of the evidence" standard. He noted that on two occasions, the PRC unanimously approved the shift to the preponderance standard, after careful consideration of the policy issues and an investigation of the established best practices. He further stated that the PRC's enabling ordinance specifically empowers the PRC to "adopt rules and regulations and develop such procedures for its own activities and investigations as may be necessary." (BMC 3.32.090.E)

On August 1, 2016, I met with you, Mr. Perezvelez and Terry Roberts, along with the Police Chief and Assistant City Attorney, to discuss this letter amongst with other topics. While the issue of meet and confer was not mentioned in Mr. Perezvelez's letter, we discussed this requirement during our meeting, and the group expressed that it would be helpful for me to share with the PRC an explanation of the meet and confer process and how it impacted the proposal to change the standard of proof.

It is important to recognize the long-established role that the meet and confer process has in the adoption of changes to the PRC's Regulations. The City Manager is obligated, consistent with state law and the provisions of the Memorandum of Agreement with the Berkeley Police Association (BPA), upon request of the union, to meet and confer with representatives of the BPA and endeavor to reach agreement on the practical consequences "**of any changes** in wages, hours and **other terms and conditions** of employees represented by the Association." Meet and confer continues until management and labor either reach an agreement or reach impasse. "Impasse"

means that the City and the BPA have a dispute over matters within the scope of representation and have reached a point in meeting and negotiating over the dispute at which their differences in positions are **so substantial or prolonged** that future meetings would be futile. Impasse is only reached after multiple meetings and extensive effort on both sides to reach an agreement.

To choose to go down this path on a matter likely to lead to impasse, I need to weigh and balance the benefit to the City in pushing forward an attempt to implement a change against the impact reaching impasse would have on the City, including staff morale and the ongoing relationship with the represented employees and association leadership. I do not take these matters lightly and recognize the thought and deliberation that the PRC has put into making this proposal. However, I ultimately must make the decision that is in the overall best interests of the City.

The change proposed to the standard of proof in the PRC's Regulations was identified as a change that required engaging in the meet and confer process. The standard of proof, clear and convincing evidence, has been the standard used by the PRC for more than 30 years. I cannot discuss the specific details of the meet and confer discussions in this or any other matter as the process is confidential. I can confirm that it was clear going into negotiations that the BPA was not in agreement with the proposed change to the standard of proof. It is also my understanding that this is not the first time the topic of changing the standard of proof has come up as a topic of meet and confer, and has been identified as a non-negotiable issue.

As I am ultimately responsible for ensuring that the City has a productive working relationship with all of our represented employees, I need to make critical decisions about which issues I will pursue further and which I will take off the table for that particular meet and confer process. Considering that 44 policy changes to the PRC Regulations were ultimately agreed to at the conclusion of the meet and confer process and have now been implemented, I believe that the process was an overall success.

City of Berkeley

Surveillance and Community Safety Ordinance

BE IT HEREBY ORDAINED that the City Council of Berkeley adopts the following ordinance:

Section 1. Title

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

Section 2. Findings

The City Council finds as follows:

- 1) Transparency is essential when the City is considering procurement and use of surveillance technology.
- 2) Such technology is often proposed as beneficial to public order and safety, but have the potential to put both privacy and civil liberties at risk. In U.S. history, government surveillance has had a disproportionately repressive effect on marginalized racial, ethnic, religious, and LGBT communities and social change movements.
- 3) No decisions relating to surveillance technology should occur without strong consideration of the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions.
- 4) Decisions regarding whether and how surveillance technologies should be funded, acquired, or used should give significant weight to public input.
- 5) 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 acquired or deployed.
- 6) 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 observed.

Section 3. City Council Approval Requirement

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

Section 4. Information Required

- 1) The City entity seeking approval under Section 2 shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy at least forty-five (45) days prior to the public hearing. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.
 - a) Prior to seeking City Council approval under Section 2, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the Police Review Commission for its review at a regularly noticed meeting.
 - b) The Police Review Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy.
- 2) After receiving the recommendation of the Police Review Commission, the City Council shall publicly release in print and online the Surveillance Impact Report, proposed Surveillance Use Policy, and Police Review Commission recommendation at least thirty (30) days prior to the public hearing.
- 3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(1).

Section 5. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 2, subsection (1) or Section 5 of this ordinance after first considering the recommendation of the Police Review Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Section 6. Compliance for Existing Surveillance Technology

Each City entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy in compliance with Section 3 (1) (a-b), and no later than one hundred eighty (180) days following the effective date of this ordinance for review and approval by the City Council pursuant to Section 4. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 7. Oversight Following City Council Approval

- 1) A City entity which obtained approval for the use of surveillance technology must submit a written Surveillance Report for each such surveillance technology to the City Council within twelve (12) months of City Council approval and annually thereafter on or before November 1.
 - a) Prior to submission of the Surveillance Report to the City Council, the City entity shall submit the Surveillance Report to the Police Review Commission for its review.
 - b) The Police Review Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the Surveillance Use Policy that will resolve the concerns.
- 2) Based upon information provided in the Surveillance Report and after considering the recommendation of the Police Review Commission, the City Council shall determine whether the requirements of Section 4 are still satisfied. If the requirements of Section 4 are not satisfied, the

City Council shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve any deficiencies.

- 3) No later than January 15 of each year, the City Council shall hold a public meeting and publicly release in print and online a report that includes, for the prior year:
 - a) A summary of all requests for City Council approval pursuant to Section 2 or Section 5 and the pertinent Police Review Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval; and
 - b) All Surveillance Reports submitted.

Section 8. Definitions

The following definitions apply to this Ordinance:

- 1) "Surveillance Report" means a written report concerning a specific surveillance technology that includes all of the following:
 - a) A description of how the surveillance technology was used, including the quantity of data gathered or analyzed by the technology;
 - b) Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
 - c) Where applicable, a breakdown of what physical objects the surveillance technology software was installed upon; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
 - d) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau;
 - e) A summary of community complaints or concerns about the surveillance technology, and an analysis of any discriminatory uses of the technology and effects on the public's civil rights and civil liberties, including but not limited to those guaranteed by the California and Federal Constitutions;
 - f) The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response;
 - g) Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
 - h) Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - i) Statistics and information about public records act requests, including response rates;
 - j) 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; and
 - k) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
- 2) "City entity" means any department, bureau, division, or unit of the City of Berkeley.
- 3) "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, process, or share audio, electronic,

visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group.

- a) "Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 7(3): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital 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; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems; (f) municipal agency databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.
- 4) "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:
 - a) **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - b) **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
 - c) **Location:** The location(s) it may be deployed and crime statistics for any location(s);
 - d) **Impact:** An assessment identifying any potential impact on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm. In addition, identify specific, affirmative measures that will be implemented to safeguard the public from each such impacts;
 - e) **Data Sources:** A list of all sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data;
 - f) **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
 - g) **Fiscal Cost:** The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
 - h) **Third Party Dependence:** 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;
 - i) **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
 - j) **Track Record:** A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

- 5) "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of the surveillance technology that at a minimum specifies the following:
- a) **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
 - b) **Authorized Use:** The uses that are authorized, the rules and processes required prior to such use, and the uses that are prohibited;
 - c) **Data Collection:** The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;
 - d) **Data Access:** The individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
 - e) **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
 - f) **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;
 - g) **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;
 - h) **Third Party Data Sharing:** If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
 - i) **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, including any training materials;
 - j) **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
 - k) **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

Section 9. Enforcement

- 1) Any violation of this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective city agency, the City of Berkeley, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any third-party with possession, custody, or control of data subject to this Ordinance.
- 2) Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy, may institute proceedings in any court of competent jurisdiction against any person who committed such violation and shall be entitled to recover

actual damages (but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater) and punitive damages.

- 3) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (1) or (2).
- 4) In addition, for a willful, intentional, or reckless violation of this Ordinance or of a Surveillance Use Policy, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding \$1,000 per violation.

Section 10. Secrecy of Surveillance Technology

It shall be unlawful for the City of Berkeley or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such 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 Ordinance 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 Ordinance.

Section 11. Whistleblower Protections.

1) No municipal entity or anyone acting on behalf of a municipal entity may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms, conditions, access to information, restrictions on due process rights, privileges of employment, or civil or criminal liability, because:

a) The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council Member, based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or

b) The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Ordinance.

2) It shall be grounds for disciplinary action for a municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Ordinance.

3) Any employee or applicant who is injured by a violation of Section 10 may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

Section 12. Severability

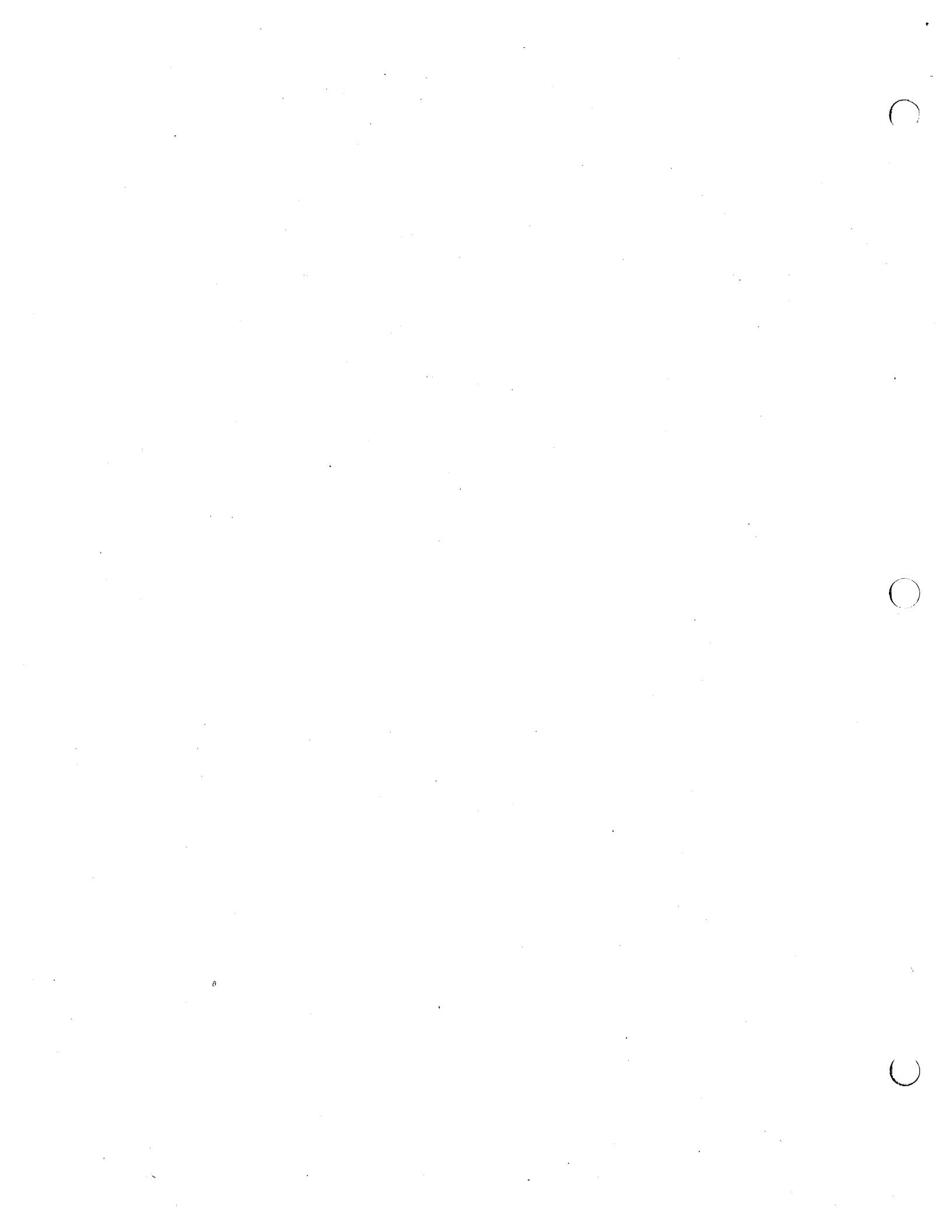
The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such part or provisions to other persons or circumstances, shall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

Section 13. Construction

The provisions of this Ordinance, including the terms defined in Section 7, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 13. Effective Date

This Ordinance shall take effect on [DATE].



Recommendations to be included in the Commander's Guide to Crowd Management & Crowd Control

Pre-Planned Events

If requesting mutual aid for 1st Amendment events, request that if possible, they not bring obviously armored vehicles or that if they do, that they be willing to keep them in the staging area until use required.

For large scale crowd management events, increase staffing of bicycle officers, motorcycle officers and parking enforcement officers, dispatchers and jailer positions.

Contact Crowd Leadership if possible

If DOC used, have IT and Public Works staff on hand
Ensure Tactical Channel is recorded
Tactical Dispatcher
If staffing allows, use social media to communicate with the crowd

Inventory munitions and ensure that sign in/out sheets are utilized

Conduct Briefing for all LE participants

Convey community concerns such as reasonable use of force, use of armored vehicles, use of chemical agents, to all personnel.

Review no baton strike areas on the human body.

Brief media policy.

If issued, outline use of body worn cameras.

Review rules of engagement with Less Lethal operators prior to deployment.

Consider deploying joint police and fire scout teams to manage small fires and scout medical calls.

The IC in charge when event ends has 72 hrs. to submit the AAR. If due to the length of the incident, i.e. multiple operational periods, the IC shall write a summary report. Use of less lethal and chemical munitions should be recorded in the after action report.

Spontaneous Events-Watch Commander is the IC

Use BPD forces to contact the crowd whenever possible.

Time permitting, review rules of engagement with Less Lethal operators

Utilize munitions sign in/out sheet

IC may command from field or have Squad Leader(s) designated as Field Commander

Broadcast initial objectives and update as the situation progresses

At the conclusion of the operation, have Squad Leaders submit use of force reports and munitions sign in/out sheets to the IC for the AAR.

The IC in charge when event ends has 72 hrs. to submit the AAR. If due to the length of the incident, i.e. multiple operational periods, the IC shall write a summary report.

Mission

The Mission of the Berkeley Police Department in crowd situations is to facilitate free expression, de-escalate violence, and resolve conflict peacefully with the overall goal of ensuring public safety and protecting First Amendment rights of free speech and assembly.

Communication

To enhance two-way communication and facilitate peaceful demonstrations, BPD will, whenever practical, communicate with crowd leadership before and during the event. BPD negotiators, crisis intervention trained officers, or others with a similar skill set should be considered for this role first.

Look for opportunities to give directions to the crowd. Directions should include acceptable and unacceptable behavior that can potentially lead to a dispersal order. Record and document these public addresses.

Directions may also include a medical admonishment describing what to do if exposed to gas ("Get to fresh air and flush the skin and eyes with water") as well as the location of a first aid station or eye wash station (in the event one is established). Social media can also be used to accomplish this goal.

Consider using the mini-PA on the Polaris Ranger to communicate with the crowd (i.e. directions, Dispersal Orders). Caution- Giving prolonged dispersal orders

Tactical Command

Tactical command decision making should be made in the field (responsibility for squad movements).

The Chief's intent via the IC will be captured in the Operations Plan and briefed. Based on the needs of an incident, the IC has the discretion to delegate overall tactical control of an incident to one or more field commanders. That person(s) will be responsible for communicating with the Operations Section Chief to coordinate squad taskings that will fulfill that intent.

Command should provide clear and specific taskings to Field Commanders. Field Commanders should make redeployment decisions proactively based on known situational awareness. (If task is accomplished or not needed by the time the Commander and his/her squad arrives, go 10-8. Look for work).

Opportunities for the police to deescalate from crowd control to crowd management tactics needs to be recognized and seized.

Deployment

Deploy resources at the beginning of an event in preventative crowd management roles designed to keep events peaceful. Examples: Bikes monitoring from the front, sides and rear of crowd. Officers walking with crowd. Motors and PEOs to facilitate traffic control.

Maneuver

Have a contingent of officers to move with the crowd, so that violent elements in the crowd will see a continuous police presence.

Deploy squads with dedicated drivers who remain in/with the vehicles to increase squad mobility and facilitate vehicle security.

Media

Review pertinent parts of BPD General Order P-29 – Public/Media Relations during the briefings with officers, reminding them to attempt to identify members of the press in the crowd.

Social Media

When practical BPD will use social media proactively before and during the event to communicate with participants, clearly identifying all communications as coming from BPD.

Dispersal Orders

Issue fewer dispersal orders and record evidence that the crowd was able to hear the orders.

Give plain English explanations to make sure the message is understood. As dispersal orders are given over the loud speaker, social media will be used when practical to communicate more detailed information to the crowd.

If a crowd forms but their composition may have changed reissue dispersal orders before making arrests for failure to disperse per California Penal Code Section 409.

Skirmish Lines

Skirmish lines should be deployed only in situations where the use of force that may be necessary to enforce the line is warranted by the objective of deploying the line.

Have enough officers in place to support isolated arrests.

Officers or Squad Leaders on a skirmish line should not get into a debate or argument with crowd members but may answer reasonable questions.

CS Gas

Only to be used as a last resort when all other means have failed or are not possible.

If possible, give preparatory orders warning officers of the impending use of chemical agents over the radio prior to their use.

Prior to the planned deployment of CS Gas, medical aid should be on scene and available to respond to treat people who might be affected by CS Gas.

Have a Gas Plan for every volley of gas. The Commander's Gas Plan should include clear direction regarding the type of gas to be used, the quantity of gas to be used, and the intended location for release. For instance, two canisters of gas and two canisters of smoke released at the southwest corner of MLK and Addison. The commander may consider starting with one canister of gas and/or smoke to ascertain the wind direction and effect on the crowd. After each use of chemical agent and/or gas, the commander shall re-evaluate to determine if additional chemical agents and/or smoke are necessary. If he or she determines that additional chemical agents and/or smoke are needed, the commander should articulate a new Gas Plan.

If a determination is made that the use of hand thrown chemical agents is necessary, the preferred method of delivery is to roll the canister.

Arrests

When possible make targeted arrests of law breakers before they coopt event.



Use of Automated License Plate Readers Expanding in Northern California, and Data is Shared with Feds

July 22, 2013

Issues : [Privacy and Government Surveillance](#), [Technology and Civil Liberties](#)

By: Matt Cagle [follow @Matt_Cagle](#)

The feeling of freedom that comes from driving down California's sunny open roads is at risk—and rising gas prices are not to blame. Our investigations show that at least twenty Northern California law enforcement entities as well as the California Highway Patrol track the whereabouts of millions of Californians using automated license plate readers (ALPR), and some apparently even share records with a "fusion center" connected to the federal intelligence community.

Scanning thousands of plates per minute, ALPR cameras create records of innocent people's movements that can be held for years. Unfortunately, as the [ACLU's recent report shows](#), many agencies use ALPR without clear privacy protections for the collected data. Without proper safeguards, license plate readers can be used to identify every car parked near a protest or event, or to collect data about your visits to a doctor's office, local bar, religious services, and more. We need clear, strong rules to prevent the misuse of ALPRs and the data they collect.

The massive amounts of data collected by a few Northern California police departments show how ALPR data makes it easy to track residents' whereabouts. In Piedmont, a tiny city east of Oakland with about 11,000 residents, the local police department captured 1,641,841 plate scans with one ALPR unit in just one year. South Bay city Milpitas, with only 67,000 residents, collected 4.7 million plate images in slightly more time. On the state's highways, the California Highway Patrol operates at least 200 cameras, but we don't even know how much data they have collected. To bring into focus how these large quantities of scans can be used to track cars within a given area, take a [look at these maps](#) produced by Berkeley's ALPR parking enforcement system.

Unfortunately, there are no statewide privacy protections for these records, and many individual law enforcement agencies have no such protections either. In fact, only about half of the 20 agencies we learned use ALPR had a written policy manual at all. Of those agencies with written policies, many allowed the data to be used for all "[legitimate law enforcement business](#)." Some cities, [including Milpitas](#) in the South Bay, do not even keep records of who accesses the ALPR information. In addition, agencies vary wildly in how long they retain ALPR records. Although the Marin County town of Tiburon deletes records after 30 days if not associated with a criminal investigation, cities such as Concord, Elk Grove, and East Palo Alto allow the data to be held for [upwards of two years](#)—and [Berkeley did not even have](#) a retention policy.

We also found that sensitive ALPR data is shared with other counties and potentially the federal intelligence community through a "[fusion center](#)." A [Memorandum of Understanding \(MOU\) signed by Daly City](#) describes an ALPR database shared by a [Bay Area fusion center](#) and fifteen Northern California counties. Under the plan, participating counties get continuous access to each other's data with no clear limits on what it can be used for. By combining records from

multiple jurisdictions, this database has the potential to contain extensive records of motorists' travels throughout Northern California. The U.S. Senate concluded in 2012 that fusion centers fail to make us safer, tend to be mismanaged, and needlessly intrude on Americans' privacy, so the suggestion that counties are sharing Californians' data en masse is particularly concerning.

ALPR technology should be used to accomplish specific law enforcement goals, not deployed as a tool for dragnet surveillance. As it stands, lax safeguards on the use of ALPR and the availability of collected data to the federal intelligence system raise substantial privacy concerns. Real safeguards formed through democratic debate can shed light on the technology's use, and prevent future misuse. The starting point for establishing these safeguards is to have an open discussion with local government and citizens about the risks and benefits of ALPRs. Driving may be a privilege, but privacy is a right.

Model Surveillance & Community Safety Ordinance

A. KEY PRINCIPLES OF THE MODEL ORDINANCE

- o **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.
- o **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.
- o **Thorough Surveillance Use Policy:** Legally enforceable Surveillance Use Policy with robust civil liberties, civil rights, and security safeguards approved by policymakers.
- o **Ongoing Oversight & Accountability:** Proper oversight of surveillance technology use and accountability through annual reporting, review by policymakers and enforcement mechanisms.

B. MODEL ORDINANCE TEXT

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

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

Section 1. Title

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

Section 2. [Council/Board] Approval Requirement

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

Section 3. Information Required

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

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

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

Section 5. Compliance for Existing Surveillance Technology

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

Section 6. Oversight Following [Council/Board] Approval

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

Section 7. Definitions

The following definitions apply to this Ordinance:

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

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

Section 8. Enforcement

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

Section 9. Severability

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

Section 10. Effective Date

This Ordinance shall take effect on [DATE].