

11. Approval of the following: 1) Contract with Flock Safety (S23187316) for Automated License Plate Recognition (ALPR) Implementation for a three-year term in an amount not to exceed \$174,400; 2) ALPR Surveillance Use Policy; and 3) Budget amendment in the Supplemental Law Enforcement Services fund; CEQA status – categorically exempt (Section 15321 enforcement actions) *Public Comments, Presentation*



CITY OF  
**PALO  
ALTO**

## City Council Staff Report

**From: City Manager**  
**Report Type: ACTION ITEMS**  
**Lead Department: Police**

**Meeting Date: April 3, 2023**  
Report #: 2301-0741

### **TITLE**

Approval of the following: 1) Contract with Flock Safety (S23187316) for Automated License Plate Recognition (ALPR) Implementation for a three-year term in an amount not to exceed \$174,400; 2) ALPR Surveillance Use Policy; and 3) Budget amendment in the Supplemental Law Enforcement Services fund; CEQA status – categorically exempt (Section 15321 enforcement actions);

### **RECOMMENDATION**

Staff recommend that the City Council:

1. Approve Contract No. S23187316 (Attachment A) with Flock Safety, for 3 years, not to exceed \$174,400 to implement fixed Automated License Plate Recognition (ALPR) technology; and
2. Approve the fixed Automated License Plate Recognition (ALPR) surveillance use policy and use of ALPR technology to deter and investigate criminal activity (Attachment B); and
3. Amend the Fiscal Year 2023 Budget Appropriation (requires 2/3 approval) for the Supplemental Law Enforcement Services Fund (SLESF) by
  - a. Increasing SLESF Contract Services expense appropriation by \$61,900, and
  - b. Decreasing the ending fund balance by \$61,900.

### **EXECUTIVE SUMMARY**

This report contains a surveillance evaluation of Automated License Plate Recognition (ALPR), as required by municipal ordinance, describing the uses and benefits of fixed ALPR technology,

associated privacy considerations and applicable law. Staff is recommending Council approve a three-year contract for the installation of fixed ALPR cameras at strategic locations in the City, as well as an ALPR surveillance use policy. ALPR technology uses a combination of cameras and computer software to scan the license plates of passing vehicles. The use of ALPR technology provides several potential benefits, including crime deterrence, real-time alerts to police when stolen or wanted vehicles enter an area, and enhanced investigative capabilities when a crime has already occurred. The initial year is recommended to be funded from COPS grant funds.

## **BACKGROUND**

The City Council discussed the prospective use of fixed ALPR technology on October 24, 2022<sup>1</sup>. This staff report brings forward a contract with Flock Safety for the deployment of fixed ALPR, as well as the associated Surveillance Use Policy.

Automated License Plate Recognition (ALPR) technology uses a combination of cameras and computer software to scan the license plates of passing vehicles. The cameras, which can be fixed (e.g., mounted on road signs or traffic lights) or mobile (i.e., mounted on a vehicle), capture computer-readable images that allow law enforcement to compare plate numbers against plates of known stolen vehicles or vehicles associated with individuals wanted on criminal charges. When a match is found, a real-time alert is generated, notifying police of the location where the image of the stolen or wanted vehicle was captured. ALPR data can also be used by investigators, after a crime has been committed, to identify and locate associated vehicles.

The Palo Alto Police Department has utilized a single mobile ALPR unit for over ten years. The limitation of a single mobile ALPR is that alerts and data collection only occur when that vehicle is being operated by an officer and data is also limited to the route and distance traveled by the patrol vehicle.

## **ANALYSIS**

The addition of fixed ALPR cameras provides the City with a cost-effective force multiplier that helps direct officers to where crimes are occurring and provides invaluable investigative leads following a crime. Fixed ALPR technology is being used widely by many local police agencies to locate stolen vehicles and solve crimes where a vehicle has been used. Over time, the quality and accuracy of ALPR technology has continued to evolve, while also becoming more affordable.

This report recommends the Council approve the following:

- A three-year contract with Flock Safety (S23187316) for ALPR Implementation, and
- Automated License Plate Recognition (ALPR) Surveillance Use Policy and Surveillance Evaluation

---

<sup>1</sup> <https://www.cityofpaloalto.org/City-Hall/City-Council/Council-Agendas-Minutes>

- Budget adjustment in the Supplemental Law Enforcement Services fund (grant funding) to provide for this investment.

#### Three Year Contract with Flock Safety

The proposed three-year contract calls for Flock Safety to install and maintain twenty ALPR cameras at locations identified by the Police Department. It also calls for Flock Safety to provide the Department with searchable access to its ALPR data, and to store the data for 30 days.

Staff proposes a follow-on contract procurement process as permitted under Palo Alto Municipal Code section 2.30.360(k), allowing the use of another governmental agency's contract or substantially the same contract terms and exempting the competitive solicitation requirements to acquire the fixed ALPR equipment. The contract is based upon the City of Alameda's recent procurement process that selected Flock Safety. The City's Procurement Officer has determined that the City of Alameda's solicitation process is substantially similar to the City's. City staff reviewed the marketplace for this technology and received uniformly positive feedback from numerous other local government agencies regarding their experiences with the quality and reliability of the ALPR systems supplied by Flock Safety. Therefore, staff recommend moving forward with Flock Safety. Use of the City of Alameda's contract terms provides a more timely and efficient deployment of this technology than if the City performed its own solicitation process.

#### Automated License Plate Recognition Surveillance Use Policy

Palo Alto's Surveillance Technology ordinance (No. 5420) modified PAMC §2.30.620, et seq. to establish criteria and procedures to protect personal privacy in the acquisition and use of surveillance technology, and provide for ongoing oversight. Fixed ALPR is "surveillance technology" as defined by the ordinance. The ordinance requires Council approval of the acquisition of new surveillance technology and of a Surveillance Use Policy for each new approved technology. In approving new surveillance technology, the Council must determine that its benefits outweigh the associated costs and concerns.

The ordinance sets forth specific elements that must be present in a Surveillance Use Policy, including proposed access, use, and retention, as well as a description of compliance procedures. The Department has prepared and attached a Surveillance Use Policy, which addresses each of these elements (Attachment B).

In addition, prior to the approval by the Council of a new surveillance activity, the ordinance requires the completion of a Surveillance Evaluation, consisting of five specific elements.

#### Surveillance Evaluation

*(1) A description of the surveillance technology, including how it works and what information it captures;*

A fixed ALPR system captures the date, time, location, license plate (state, partial, paper, and no plate), and vehicle characteristics (make, model, type, and color) of passing vehicles. ALPR cameras are positioned to capture rear license plates only and are not designed to capture images of vehicle occupants or use facial recognition technology. ALPR data is transmitted in an encrypted format to, and stored by, Flock Safety, consistent with Criminal Justice Information System (CJIS) protocols. The Department will access the data via a web-based platform.

*(2) Information on the proposed purpose, use and benefits of the surveillance technology;*

Purpose & Use: Recent years have seen regional increases in catalytic converter thefts, auto burglaries, vehicle thefts and organized retail thefts. The community has also experienced several brazen robberies and residential burglaries. Those responsible for such crimes commonly use a vehicle to travel to and flee from the crime scene. Moreover, they often engage in criminal offenses involving multiple jurisdictions, and commonly arrive in a stolen vehicle, a vehicle bearing stolen plates, or a vehicle that law enforcement has previously connected to verified criminal activity. Identifying such vehicles, via fixed ALPR, as they enter a target area provides law enforcement an opportunity to intervene before additional crimes are committed, and potentially apprehend wanted persons or recover stolen property. ALPR data also provides investigators with an additional technique to identify and apprehend offenders once a crime has already occurred.

Other local communities are currently using fixed ALPR technology, including Menlo Park, Atherton, Los Altos Hills, Saratoga, Campbell, San Jose, Los Gatos, Gilroy, Morgan Hill, Milpitas, and Santa Clara, with others in the process of implementing the technology. Anecdotally, these jurisdictions report that since the deployment of fixed ALPR, they have experienced a marked increase in the recovery of stolen vehicles and report investigative success stories attributable to ALPR data.

Benefits of Usage: The use of ALPR technology provides several potential benefits:

- *Real-Time Alerts:* When a real-time ALPR alert occurs, notifying police of the presence of a wanted or stolen vehicle, officers can respond to the area to search for the vehicle. If officers locate the vehicle, prior to making an enforcement stop, they visually confirm the plate number and manually check it against law enforcement databases to confirm the accuracy of the ALPR information and the legal justification for the stop.
- *Deterrence:* Even if officers are unable to locate and stop the vehicle in question, suspects may see the police response and be deterred from further criminal activity. Indeed the mere presence of the fixed ALPR cameras may act as a deterrent. Police personnel have reported to staff that some criminals will intentionally target jurisdictions without ALPR technology and avoid those where it is in use.

- *Solving Crimes Already Committed:* Commonly, by the time a crime is reported to police, the suspects have already fled the area, and it is the job of police to identify and locate the suspects at a later time. While victims and witnesses can often provide a description of the vehicle used by a suspect, those descriptions are frequently incomplete (e.g., a partial license plate number, vehicle type and color only) or consist of a license plate number that corresponds to a stolen vehicle or a stolen plate. Investigators can turn that imperfect information into actionable leads by querying the ALPR database. Existing DMV databases do not offer this capability.
- *Regional Coordination:* ALPR data sharing among local law enforcement partners allows agencies to collaboratively investigate, identify and apprehend multi-jurisdictional offenders, or those who commit crimes in one jurisdiction but reside in another. For example, in the case of organized retail thieves, ALPR data sharing may allow investigators to connect multiple cases across disparate jurisdictions, share evidence, and obtain the best prosecutorial outcomes.
- *Expanded Searchable Data Set:* Private entities (e.g., shopping centers, individual retailers) utilizing ALPR cameras can share their data with local law enforcement, to include real-time alerts. This is a one-way share. In other words, an entity that shares its ALPR data with law enforcement does not gain access to law enforcement data in return. The investigative usefulness of an ALPR system is greatly enhanced as its searchable data set increases, whether from other law enforcement contributors or private entities.

One of the City Council's four priorities this calendar year is Community Health and Safety. While the implementation of ALPR for policing was not previously identified as an objective, based on prior Council discussion and subject to approval staff will recommend adding this as an objective. Further, the 2030 Comprehensive Plan includes policies S-1.6 and S-1.7, which supports a balanced approach of utilizing safety technology with policy-driven safeguards. The Department believes that the deployment of a fixed ALPR system, with sound policies and training, would support crime prevention, criminal apprehension, stolen vehicle recovery, and criminal investigation.

*(3) The location or locations where the surveillance technology may be used;*

To derive maximum benefit with the fewest cameras needed, cameras will be placed at strategically selected locations based on several factors: crime statistics, common vehicular ingress and egress points, and traffic volume. Accounting for these factors provides the greatest likelihood of capturing images of suspects' vehicles and their license plates. While the Department has no intention of permanently installing ALPR cameras in residential neighborhoods, cameras could be temporarily repositioned in response to a specific crime in a specific neighborhood. If placed in a residential neighborhood, cameras would not be positioned to capture images of homes, front yards, or pedestrians.

*(4) Existing federal, state and local laws and regulations applicable to the surveillance technology and the information it captures; the potential impacts on civil liberties and privacy; and proposals to mitigate and manage any impacts;*

Some organizations, such as the American Civil Liberties Union (ACLU), have generally expressed concerns about the use of ALPR, specifically on the aspects of data access, storage, retention, sharing, and reporting. The Department's proposed Surveillance Use Policy is responsive, in whole or in part, to each of these concerns and the ACLU's LPR guidelines<sup>2</sup>. For example, while many local law enforcement agencies retain ALPR data for one year and often longer, the Department believes that a retention period of 30 days will adequately support its investigative needs. Only data which has been identified as relevant to a specific criminal investigation will be retained longer.

In addition to the City Surveillance Technology Ordinance, California Civil Code §1798.90.5, et seq. governs the collection of license plate information by government agencies. It spells out the policies and training that an agency must implement when collecting ALPR data. These policies, largely, address the same concerns set forth above. The Department will ensure that its policies and training satisfy the requirements of this statute. Flock Safety has adopted a usage and privacy policy consistent with California Civil Code §1798.90.5, et seq. Moreover, by the terms of the proposed contract with the City, Flock Safety is required to observe specific data security protocols, including restricting data access only to that which is necessary for system maintenance, logging all access by its employees, conducting quarterly compliance audits, and permitting the City to review these audits logs.

Internally, data will only be accessible to trained staff with a legitimate law enforcement need, and all queries will be logged and subject to audit. Whereas some local law enforcement agencies share data with federal and out of state law enforcement agencies, the Department will only share its data with other local law enforcement agencies with whom an MOU is in place, and those queries would likewise be logged. Neither the Department, nor Flock Safety, will share the Department's data with any non-law enforcement entities. The Department will make accessible to the public, via its ALPR webpage<sup>3</sup>, relevant policies as well as information concerning the number of cameras deployed, the data retention period, and the names of law enforcement agencies with whom it shares data. Flock Safety will also maintain a publicly-accessible Transparency Portal containing much of the same information.

*(5) The costs for the surveillance technology, including acquisition, maintenance, personnel and other costs, and current or potential sources of funding.*

---

<sup>2</sup> <https://www.aclunc.org/publications/making-smart-decisions-about-surveillance-guide-community-transparency-accountability>

<sup>3</sup> <https://www.cityofpaloalto.org/Departments/Police/Public-Information-Portal/Automated-License-Plate-Recognition-ALPR>

In year one, the initial deployment of this ALPR technology would come at a total cost of \$61,900, including the initial installation and setup. In years two and three, the on-going annual cost is \$52,500. This includes access to the cameras, data storage, and access to the ALPR database. The Department anticipates no more \$2,500 will be needed annually to repair any damaged equipment. The Department intends to use existing COPS funds to fund the initial deployment.

#### **TIMELINE**

The Department is informed that, following Council approval, Flock Safety can complete the installation and setup process within 8 weeks. Associated Department personnel training and policy implementation can also be accomplished during this timeframe.

#### **FISCAL/RESOURCE IMPACT**

The Department is contracting for the installation and use – not the purchase – of ALPR cameras. Flock Safety will complete the installation and setup of the cameras and will be the owner of the equipment. The cameras are solar-powered and transmit data via a wireless cell signal, requiring no utility connection. Flock Safety will maintain or replace the cameras as needed. Data storage - other than specific images identified as evidence in a criminal investigation - will be the responsibility of Flock Safety who will be responsible for maintaining CJIS data protocols, and the data will be accessed via a web platform, requiring no new software.

The implementation of this ALPR technology will come at a total cost of \$61,900, including the initial installation and setup, which should encompass the remainder of FY 2023 and FY 2024. For subsequent years (FY2025 and FY 2026), costs are projected to be \$52,500 annually. This includes access to the cameras, data storage, and access to the ALPR database. Damaged cameras will be replaced by Flock Safety at a cost of \$500 per camera, with an annual cost not expected to exceed \$2,500. Funding for years one and two of contract will come from the SLES Fund balance for FY 2023 and FY 2024. Subsequent years of the contract are subject to appropriation of funds through the annual budget process. Staff will seek to continue use of grant funds for future funding, however, if unsuccessful, this would be an ongoing General Fund cost.

#### **STAKEHOLDER ENGAGEMENT**

The Department participated in a Council ALPR study session on October 24, 2022. Prior to that, the Department consulted with several other agencies to gather best practices for the deployment, and oversight of a fixed ALPR program.

In November 2022, the Department met with a representative of the Peninsula Chapter of the ACLU to better understand the ACLU's concerns about the use of ALPR technology, and to discuss the Department's efforts to be responsive to those concerns in drafting a surveillance use policy.



Additionally, in December 2022, the Department accepted invitations to address the topic with the Palo Alto Chamber of Commerce and a neighborhood group.

On February 13, 2023, the Department launched an informational webpage, including an opportunity for community input. This yielded 7 total submissions: 1 solicitation from an ALPR vendor, 1 comment questioning the need for ALPR, and 5 supportive comments.

On March 9, 2023, the Department presented a virtual information session on ALPR technology. A recording was subsequently posted to the Department's dedicated ALPR webpage, and has been viewed 30 times.

#### **ENVIRONMENTAL REVIEW**

Approval of this agreement and surveillance policy are categorically exempt under CEQA regulation 15321 for enforcement actions.

#### **ATTACHMENTS**

Attachment A – Flock Safety, Contract No. S23187316

Attachment B – Palo Alto Police Fixed ALPR Surveillance Use Policy

Attachment C – ACLU Guidelines

#### **APPROVED BY:**

Andrew Binder, Police Chief

**CITY OF PALO ALTO CONTRACT NO. S23187316**

**AGREEMENT FOR PROFESSIONAL SERVICES**

**BETWEEN THE CITY OF PALO ALTO AND FLOCK GROUP INC. dba FLOCK SAFETY**

This Agreement for Professional Services (this “Agreement”) is entered into as of the 1<sup>st</sup> day of April, 2023 (the “Effective Date”), by and between the CITY OF PALO ALTO, a California chartered municipal corporation (“CITY”), and FLOCK GROUP INC. dba FLOCK SAFETY, a Delaware corporation, Department of Industrial Registration No. PW-LR-1000674310 located at 1170 Howell Mill Road NW, Suite 210, Atlanta, Georgia, 30318 (“CONSULTANT”).

The following recitals are a substantive portion of this Agreement and are fully incorporated herein by this reference:

**RECITALS**

A. CITY intends to implement an Automated License Plate Reader System (ALPR) (the “Project”) and desires to engage a consultant to furnish all equipment, equipment maintenance, installation, materials, tools, and software services to implement ALPR across City of Palo Alto’s key areas in connection with the Project (the “Services”, as detailed more fully in Exhibit A).

B. CONSULTANT represents that it, its employees and subconsultants, if any, possess the necessary professional expertise, qualifications, and capability, and all required licenses and/or certifications to provide the Services.

C. CITY, in reliance on these representations, desires to engage CONSULTANT to provide the Services as more fully described in Exhibit A, entitled “SCOPE OF SERVICES”.

NOW, THEREFORE, in consideration of the recitals, covenants, terms, and conditions, in this Agreement, the parties agree as follows:

**SECTION 1. SCOPE OF SERVICES.** CONSULTANT shall perform the Services described in Exhibit A in accordance with the terms and conditions contained in this Agreement. The performance of all Services shall be to the reasonable satisfaction of CITY.

**SECTION 2. TERM.**

The term of this Agreement shall be from the date of its full execution through June 30, 2026 unless terminated earlier pursuant to Section 19 (Termination) of this Agreement. CITY shall have the option to extend the term of this Agreement for one additional renewal term of 24 months, through June 30, 2028.

**SECTION 3. SCHEDULE OF PERFORMANCE.** Time is of the essence in the performance of Services under this Agreement. CONSULTANT shall complete the Services within the term of

this Agreement and in accordance with the schedule set forth in Exhibit B, entitled “SCHEDULE OF PERFORMANCE”. Any Services for which times for performance are not specified in this Agreement shall be commenced and completed by CONSULTANT in a reasonably prompt and timely manner based upon the circumstances and direction communicated to the CONSULTANT. CITY’s agreement to extend the term or the schedule for performance shall not preclude recovery of damages for delay if the extension is required due to the fault of CONSULTANT.

**SECTION 4. NOT TO EXCEED COMPENSATION.** The compensation to be paid to CONSULTANT for performance of the Services shall be based on the compensation structure detailed in Exhibit C, entitled “COMPENSATION,” including any reimbursable expenses specified therein, and the maximum total compensation shall not exceed **One Hundred Sixty Six Thousand Nine Hundred Dollars (\$166,900)**. The hourly schedule of rates, if applicable, is set out in Exhibit C-1, entitled “SCHEDULE OF RATES.” Any work performed or expenses incurred for which payment would result in a total exceeding the maximum compensation set forth in this Section 4 shall be at no cost to the CITY.

☒ Optional Additional Services Provision (This provision applies only if checked and a not-to-exceed compensation amount for Additional Services is allocated below under this Section 4.)

In addition to the not-to-exceed compensation specified above, CITY has set aside an annual amount of **Two Thousand Five Hundred Dollars (\$2,500)**; the total not-to-exceed compensation amount of **Seven Thousand Five Hundred Dollars (\$7,500)** for the performance of Additional Services (as defined below). The total compensation for performance of the Services, Additional Services and any reimbursable expenses specified in Exhibit C, shall not exceed **One Hundred Seventy Four Thousand Four Hundred Dollars (\$174,400)**, as detailed in Exhibit C.

“Additional Services” means any work that is determined by CITY to be necessary for the proper completion of the Project, but which is not included within the Scope of Services described at Exhibit A. CITY may elect to, but is not required to, authorize Additional Services up to the maximum amount of compensation set forth for Additional Services in this Section 4. CONSULTANT shall provide Additional Services only by advanced, written authorization from CITY as detailed in this Section. Additional Services, if any, shall be authorized by CITY with a Task Order assigned and authorized by CITY’s Project Manager, as identified in Section 13 (Project Management). Each Task Order shall be in substantially the same form as Exhibit A-1, entitled “PROFESSIONAL SERVICES TASK ORDER”. Each Task Order shall contain a specific scope of services, schedule of performance and maximum compensation amount, in accordance with the provisions of this Agreement. Compensation for Additional Services shall be specified by CITY in the Task Order, based on whichever is lowest: the compensation structure set forth in Exhibit C, the hourly rates set forth in Exhibit C-1, or a negotiated lump sum.

To accept a Task Order, CONSULTANT shall sign the Task Order and return it to CITY’s Project Manager within the time specified by the Project Manager, and upon authorization by CITY (defined as counter-signature by the CITY Project Manager), the fully executed Task Order shall become part of this Agreement. The cumulative total compensation to CONSULTANT for all Task Orders authorized under this Agreement shall not exceed the

amount of compensation set forth for Additional Services in this Section 4. CONSULTANT shall only be compensated for Additional Services performed under an authorized Task Order and only up to the maximum amount of compensation set forth for Additional Services in this Section 4. Performance of and payment for any Additional Services are subject to all requirements and restrictions in this Agreement.

**SECTION 5. INVOICES.** In order to request payment, CONSULTANT shall submit monthly invoices to the CITY describing the Services performed and the applicable charges (including, if applicable, an identification of personnel who performed the Services, hours worked, hourly rates, and reimbursable expenses), based upon Exhibit C or, as applicable, CONSULTANT's schedule of rates set forth in Exhibit C-1. If applicable, the invoice shall also describe the percentage of completion of each task. The information in CONSULTANT's invoices shall be subject to verification by CITY. CONSULTANT shall send all invoices to CITY's Project Manager at the address specified in Section 13 (Project Management) below. CITY will generally process and pay invoices within thirty (30) days of receipt of an acceptable invoice.

**SECTION 6. QUALIFICATIONS/STANDARD OF CARE.** All Services shall be performed by CONSULTANT or under CONSULTANT's supervision. CONSULTANT represents that it, its employees and subcontractors, if any, possess the professional and technical personnel necessary to perform the Services required by this Agreement and that the personnel have sufficient skill and experience to perform the Services assigned to them. CONSULTANT represents that it, its employees and subcontractors, if any, have and shall maintain during the term of this Agreement all licenses, permits, qualifications, insurance and approvals of whatever nature that are legally required to perform the Services. All Services to be furnished by CONSULTANT under this Agreement shall meet the professional standard and quality that prevail among professionals in the same discipline and of similar knowledge and skill engaged in related work throughout California under the same or similar circumstances.

**SECTION 7. COMPLIANCE WITH LAWS.** CONSULTANT shall keep itself informed of and in compliance with all federal, state and local laws, ordinances, regulations, and orders that may affect in any manner the Project or the performance of the Services or those engaged to perform Services under this Agreement, as amended from time to time. CONSULTANT shall procure all permits and licenses, pay all charges and fees, and give all notices required by law in the performance of the Services.

**SECTION 8. ERRORS/OMISSIONS.** CONSULTANT is solely responsible for costs, including, but not limited to, increases in the cost of Services, arising from or caused by CONSULTANT's errors and omissions, including, but not limited to, the costs of corrections such errors and omissions, any change order markup costs, or costs arising from delay caused by the errors and omissions or unreasonable delay in correcting the errors and omissions.

**SECTION 9. COST ESTIMATES.** If this Agreement pertains to the design of a public works project, CONSULTANT shall submit estimates of probable construction costs at each phase of design submittal. If the total estimated construction cost at any submittal exceeds the CITY's stated construction budget by ten percent (10%) or more, CONSULTANT shall make recommendations to CITY for aligning the Project design with the budget, incorporate CITY approved recommendations, and revise the design to meet the Project budget, at no additional cost to CITY.

**SECTION 10. INDEPENDENT CONTRACTOR.** CONSULTANT acknowledges and agrees that CONSULTANT and any agent or employee of CONSULTANT will act as and shall be deemed at all times to be an independent contractor and shall be wholly responsible for the manner in which CONSULTANT performs the Services requested by CITY under this Agreement. CONSULTANT and any agent or employee of CONSULTANT will not have employee status with CITY, nor be entitled to participate in any plans, arrangements, or distributions by CITY pertaining to or in connection with any retirement, health or other benefits that CITY may offer its employees. CONSULTANT will be responsible for all obligations and payments, whether imposed by federal, state or local law, including, but not limited to, FICA, income tax withholdings, workers' compensation, unemployment compensation, insurance, and other similar responsibilities related to CONSULTANT's performance of the Services, or any agent or employee of CONSULTANT providing same. Nothing in this Agreement shall be construed as creating an employment or agency relationship between CITY and CONSULTANT or any agent or employee of CONSULTANT. Any terms in this Agreement referring to direction from CITY shall be construed as providing for direction as to policy and the result of CONSULTANT's provision of the Services only, and not as to the means by which such a result is obtained.

**SECTION 11. ASSIGNMENT.** The parties agree that the expertise and experience of CONSULTANT are material considerations for this Agreement. CONSULTANT shall not assign or transfer any interest in this Agreement nor the performance of any of CONSULTANT's obligations hereunder without the prior written approval of the City Manager. Any purported assignment made without the prior written approval of the City Manager will be void and without effect. Subject to the foregoing, the covenants, terms, conditions and provisions of this Agreement will apply to, and will bind, the heirs, successors, executors, administrators and assignees of the parties.

**SECTION 12. SUBCONTRACTING.**

☒ **Option A: No Subcontractor:** CONSULTANT shall not subcontract any portion of the Services to be performed under this Agreement without the prior written authorization of the City Manager or designee. In the event CONSULTANT does subcontract any portion of the work to be performed under this Agreement, CONSULTANT shall be fully responsible for all acts and omissions of subcontractors.

☐ **Option B: Subcontracts Authorized:** Notwithstanding Section 11 (Assignment) above, CITY agrees that subcontractors may be used to complete the Services. The subcontractors authorized by CITY to perform work on this Project are: None

CONSULTANT shall be responsible for directing the work of any subcontractors and for any compensation due to subcontractors. CITY assumes no responsibility whatsoever concerning compensation of subcontractors. CONSULTANT shall be fully responsible to CITY for all acts and omissions of subcontractors. CONSULTANT shall change or add subcontractors only with the prior written approval of the City Manager or designee.

**SECTION 13. PROJECT MANAGEMENT.** CONSULTANT will assign Kyle Egkan, Telephone: (714) 469-0389, Email: [kyle.egkan@flocksafety.com](mailto:kyle.egkan@flocksafety.com) as the CONSULTANT's Project

Manager to have supervisory responsibility for the performance, progress, and execution of the Services and represent CONSULTANT during the day-to-day performance of the Services. If circumstances cause the substitution of the CONSULTANT's Project Manager or any other of CONSULTANT's key personnel for any reason, the appointment of a substitute Project Manager and the assignment of any key new or replacement personnel will be subject to the prior written approval of the CITY's Project Manager. CONSULTANT, at CITY's request, shall promptly remove CONSULTANT personnel who CITY finds do not perform the Services in an acceptable manner, are uncooperative, or present a threat to the adequate or timely completion of the Services or a threat to the safety of persons or property.

CITY's Project Manager is Cpt. James Reifschneider, Police Department, Investigative Services Division, 275 Forest Avenue, Palo Alto, CA, 94301, Telephone: (650) 838-2778. CITY's Project Manager will be CONSULTANT's point of contact with respect to performance, progress and execution of the Services. CITY may designate an alternate Project Manager from time to time.

**SECTION 14. OWNERSHIP OF MATERIALS.** All work product, including without limitation, all writings, drawings, studies, sketches, photographs, plans, reports, specifications, computations, models, recordings, data, documents, and other materials and copyright interests developed under this Agreement, in any form or media, shall be and remain the exclusive property of CITY without restriction or limitation upon their use. CONSULTANT agrees that all copyrights which arise from creation of the work product pursuant to this Agreement are vested in CITY, and CONSULTANT hereby waives and relinquishes all claims to copyright or other intellectual property rights in favor of CITY. Neither CONSULTANT nor its subcontractors, if any, shall make any of such work product available to any individual or organization without the prior written approval of the City Manager or designee. CONSULTANT makes no representation of the suitability of the work product for use in or application to circumstances not contemplated by the Scope of Services.

**SECTION 15. AUDITS.** CONSULTANT agrees to permit CITY and its authorized representatives to audit, at any reasonable time during the term of this Agreement and for four (4) years from the date of final payment, CONSULTANT's records pertaining to matters covered by this Agreement, including without limitation records demonstrating compliance with the requirements of Section 10 (Independent Contractor). CONSULTANT further agrees to maintain and retain accurate books and records in accordance with generally accepted accounting principles for at least four (4) years after the expiration or earlier termination of this Agreement or the completion of any audit hereunder, whichever is later.

**SECTION 16. INDEMNITY.**

☒ 16.1. To the fullest extent permitted by law, CONSULTANT shall indemnify, defend and hold harmless CITY, its Council members, officers, employees and agents (each an "Indemnified Party") from and against any and all demands, claims, or liability of any nature, including death or injury to any person, property damage or any other loss, including all costs and expenses of whatever nature including attorney's fees, experts fees, court costs and disbursements ("Claims") resulting from, arising out of or in any manner related to performance or nonperformance by CONSULTANT, its officers, employees, agents or contractors under this Agreement, regardless of whether or not it is caused in part by an Indemnified Party.

16.2. Notwithstanding the above, nothing in this Section 16 shall be construed to require CONSULTANT to indemnify an Indemnified Party from a Claim arising from the active negligence or willful misconduct of an Indemnified Party that is not contributed to by any act of, or by any omission to perform a duty imposed by law or agreement by, CONSULTANT, its officers, employees, agents or contractors under this Agreement.

16.3. The acceptance of CONSULTANT's Services and duties by CITY shall not operate as a waiver of the right of indemnification. The provisions of this Section 16 shall survive the expiration or early termination of this Agreement.

**SECTION 17. WAIVERS.** No waiver of a condition or nonperformance of an obligation under this Agreement is effective unless it is in writing in accordance with Section 29.4 of this Agreement. No delay or failure to require performance of any provision of this Agreement shall constitute a waiver of that provision as to that or any other instance. Any waiver granted shall apply solely to the specific instance expressly stated. No single or partial exercise of any right or remedy will preclude any other or further exercise of any right or remedy.

**SECTION 18. INSURANCE.**

18.1. CONSULTANT, at its sole cost and expense, shall obtain and maintain, in full force and effect during the term of this Agreement, the insurance coverage described in Exhibit D, entitled "INSURANCE REQUIREMENTS". CONSULTANT and its contractors, if any, shall obtain a policy endorsement naming CITY as an additional insured under any general liability or automobile policy or policies.

18.2. All insurance coverage required hereunder shall be provided through carriers with AM Best's Key Rating Guide ratings of A:-VII or higher which are licensed or authorized to transact insurance business in the State of California. Any and all contractors of CONSULTANT retained to perform Services under this Agreement will obtain and maintain, in full force and effect during the term of this Agreement, identical insurance coverage, naming CITY as an additional insured under such policies as required above.

18.3. Certificates evidencing such insurance shall be filed with CITY concurrently with the execution of this Agreement. The certificates will be subject to the approval of CITY's Risk Manager and will contain an endorsement stating that the insurance is primary coverage and will not be canceled, or materially reduced in coverage or limits, by the insurer except after filing with the Purchasing Manager thirty (30) days' prior written notice of the cancellation or modification. If the insurer cancels or modifies the insurance and provides less than thirty (30) days' notice to CONSULTANT, CONSULTANT shall provide the Purchasing Manager written notice of the cancellation or modification within two (2) business days of the CONSULTANT's receipt of such notice. CONSULTANT shall be responsible for ensuring that current certificates evidencing the insurance are provided to CITY's Chief Procurement Officer during the entire term of this Agreement.

18.4. The procuring of such required policy or policies of insurance will not be construed to limit CONSULTANT's liability hereunder nor to fulfill the indemnification provisions of this Agreement. Notwithstanding the policy or policies of insurance, CONSULTANT will be obligated for the full and total amount of any damage, injury, or loss

caused by or directly arising as a result of the Services performed under this Agreement, including such damage, injury, or loss arising after the Agreement is terminated or the term has expired.

## **SECTION 19. TERMINATION OR SUSPENSION OF AGREEMENT OR SERVICES.**

19.1. Reserved.

19.2. Reserved.

19.3. In event of suspension or termination, CONSULTANT will be paid for the Services rendered and work products delivered to CITY in accordance with the Scope of Services up to the effective date in the notice of suspension or termination; provided, however, if this Agreement is suspended or terminated on account of a default by CONSULTANT, CITY will be obligated to compensate CONSULTANT only for that portion of CONSULTANT's Services provided in material conformity with this Agreement as such determination is made by the City Manager acting in the reasonable exercise of his/her discretion. The following Sections will survive any expiration or termination of this Agreement: 14, 15, 16, 17, 19.2, 19.3, 19.4, 20, 25, 27, 28, 29 and 30.

19.4. No payment, partial payment, acceptance, or partial acceptance by CITY will operate as a waiver on the part of CITY of any of its rights under this Agreement, unless made in accordance with Section 17 (Waivers).

## **SECTION 20. NOTICES.**

All notices hereunder will be given in writing and mailed, postage prepaid, by certified mail, addressed as follows:

To CITY:                      Office of the City Clerk  
                                    City of Palo Alto  
                                    Post Office Box 10250  
                                    Palo Alto, CA 94303

With a copy to the Purchasing Manager

To CONSULTANT: Attention of the Project Manager at the address of  
                                    CONSULTANT recited on the first page of this Agreement.

CONSULTANT shall provide written notice to CITY of any change of address.

## **SECTION 21. CONFLICT OF INTEREST.**

21.1. In executing this Agreement, CONSULTANT covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of the Services.

21.2. CONSULTANT further covenants that, in the performance of this Agreement, it will not employ subcontractors or other persons or parties having such an interest.



CONSULTANT certifies that no person who has or will have any financial interest under this Agreement is an officer or employee of CITY; this provision will be interpreted in accordance with the applicable provisions of the Palo Alto Municipal Code and the Government Code of the State of California, as amended from time to time. CONSULTANT agrees to notify CITY if any conflict arises.

21.3. If the CONSULTANT meets the definition of a “Consultant” as defined by the Regulations of the Fair Political Practices Commission, CONSULTANT will file the appropriate financial disclosure documents required by the Palo Alto Municipal Code and the Political Reform Act of 1974, as amended from time to time.

## **SECTION 22. NONDISCRIMINATION; COMPLIANCE WITH ADA.**

22.1. As set forth in Palo Alto Municipal Code Section 2.30.510, as amended from time to time, CONSULTANT certifies that in the performance of this Agreement, it shall not discriminate in the employment of any person due to that person’s race, skin color, gender, gender identity, age, religion, disability, national origin, ancestry, sexual orientation, pregnancy, genetic information or condition, housing status, marital status, familial status, weight or height of such person. CONSULTANT acknowledges that it has read and understands the provisions of Section 2.30.510 of the Palo Alto Municipal Code relating to Nondiscrimination Requirements and the penalties for violation thereof, and agrees to meet all requirements of Section 2.30.510 pertaining to nondiscrimination in employment.

22.2. CONSULTANT understands and agrees that pursuant to the Americans Disabilities Act (“ADA”), programs, services and other activities provided by a public entity to the public, whether directly or through a contractor or subcontractor, are required to be accessible to the disabled public. CONSULTANT will provide the Services specified in this Agreement in a manner that complies with the ADA and any other applicable federal, state and local disability rights laws and regulations, as amended from time to time. CONSULTANT will not discriminate against persons with disabilities in the provision of services, benefits or activities provided under this Agreement.

## **SECTION 23. ENVIRONMENTALLY PREFERRED PURCHASING AND ZERO WASTE REQUIREMENTS.**

CONSULTANT shall comply with the CITY’s Environmentally Preferred Purchasing policies which are available at CITY’s Purchasing Department, hereby incorporated by reference and as amended from time to time. CONSULTANT shall comply with waste reduction, reuse, recycling and disposal requirements of CITY’s Zero Waste Program. Zero Waste best practices include, first, minimizing and reducing waste; second, reusing waste; and, third, recycling or composting waste. In particular, CONSULTANT shall comply with the following Zero Waste requirements:

(a) All printed materials provided by CONSULTANT to CITY generated from a personal computer and printer including but not limited to, proposals, quotes, invoices, reports, and public education materials, shall be double-sided and printed on a minimum of 30% or greater post-consumer content paper, unless otherwise approved by CITY’s Project Manager. Any submitted materials printed by a professional printing company shall be a minimum of 30% or greater post-consumer material and printed with vegetable-based inks.

(b) Goods purchased by CONSULTANT on behalf of CITY shall be purchased in accordance with CITY’s Environmental Purchasing Policy including but not limited to Extended

Producer Responsibility requirements for products and packaging. A copy of this policy is on file at the Purchasing Department's office.

(c) Reusable/returnable pallets shall be taken back by CONSULTANT, at no additional cost to CITY, for reuse or recycling. CONSULTANT shall provide documentation from the facility accepting the pallets to verify that pallets are not being disposed.

#### **SECTION 24. COMPLIANCE WITH PALO ALTO MINIMUM WAGE ORDINANCE.**

CONSULTANT shall comply with all requirements of the Palo Alto Municipal Code Chapter 4.62 (Citywide Minimum Wage), as amended from time to time. In particular, for any employee otherwise entitled to the State minimum wage, who performs at least two (2) hours of work in a calendar week within the geographic boundaries of the City, CONSULTANT shall pay such employees no less than the minimum wage set forth in Palo Alto Municipal Code Section 4.62.030 for each hour worked within the geographic boundaries of the City of Palo Alto. In addition, CONSULTANT shall post notices regarding the Palo Alto Minimum Wage Ordinance in accordance with Palo Alto Municipal Code Section 4.62.060.

**SECTION 25. NON-APPROPRIATION.** This Agreement is subject to the fiscal provisions of the Charter of the City of Palo Alto and the Palo Alto Municipal Code, as amended from time to time. This Agreement will terminate without any penalty (a) at the end of any fiscal year in the event that funds are not appropriated for the following fiscal year, or (b) at any time within a fiscal year in the event that funds are only appropriated for a portion of the fiscal year and funds for this Agreement are no longer available. This Section shall take precedence in the event of a conflict with any other covenant, term, condition, or provision of this Agreement.

#### **SECTION 26. PREVAILING WAGES AND DIR REGISTRATION FOR PUBLIC WORKS CONTRACTS.**

☒ 26.1. This Project is subject to prevailing wages and related requirements as a "public works" under California Labor Code Sections 1720 et seq. and related regulations. CONSULTANT is required to pay general prevailing wages as defined in California Labor Code Section 1773.1 and Subchapter 3, Title 8 of the California Code of Regulations Section 16000 et seq., as amended from time to time. Pursuant to Labor Code Section 1773, the CITY has obtained the general prevailing rate of per diem wages and the general rate for holiday and overtime work in this locality for each craft, classification, or type of worker needed to execute the contract for this Project from the State of California Department of Industrial Relations ("DIR"). Copies of these rates may be obtained at the CITY's Purchasing Department office. The general prevailing wage rates are also available at the DIR, Division of Labor Statistics and Research, web site (see e.g. <http://www.dir.ca.gov/DLSR/PWD/index.htm>) as amended from time to time. CONSULTANT shall post a copy of the general prevailing wage rates at all Project job sites and shall pay the adopted prevailing wage rates as a minimum. CONSULTANT shall comply with all applicable provisions of Division 2, Part 7, Chapter 1 of the California Labor Code (Labor Code Section 1720 et seq.), including but not limited to Sections 1725.5, 1771, 1771.1, 1771.4, 1773.2, 1774, 1775, 1776, 1777.5, 1782, 1810, 1813 and 1815, and all applicable implementing regulations, including but not limited to Subchapter 3, Title 8 of the California Code of Regulations Section 16000 et seq. (8 CCR Section 16000 et seq.), as amended from time to time. CONSULTANT shall comply with the requirements of Exhibit E, entitled "DIR REGISTRATION FOR PUBLIC WORKS CONTRACTS", for any contract for public works construction, alteration, demolition, repair or maintenance, including but not limited to the

obligations to register with, and furnish certified payroll records directly to, DIR.

**SECTION 27. CLAIMS PROCEDURE FOR “9204 PUBLIC WORKS PROJECTS”.** For purposes of this Section 27, a “9204 Public Works Project” means the erection, construction, alteration, repair, or improvement of any public structure, building, road, or other public improvement of any kind. (Cal. Pub. Cont. Code § 9204.) Per California Public Contract Code Section 9204, for Public Works Projects, certain claims procedures shall apply, as set forth in Exhibit F, entitled “Claims for Public Contract Code Section 9204 Public Works Projects”.

☒ **This Project is a 9204 Public Works Project** and is required to comply with the claims procedures set forth in Exhibit F, entitled “Claims for Public Contract Code Section 9204 Public Works Projects”.

**SECTION 28. CONFIDENTIAL INFORMATION.**

28.1. In the performance of this Agreement, CONSULTANT may have access to CITY’s Confidential Information (defined below). CONSULTANT will hold Confidential Information in strict confidence, not disclose it to any third party, and will use it only for the performance of its obligations to CITY under this Agreement and for no other purpose. CONSULTANT will maintain reasonable and appropriate administrative, technical and physical safeguards to ensure the security, confidentiality and integrity of the Confidential Information. Notwithstanding the foregoing, CONSULTANT may disclose Confidential Information to its employees, agents and subcontractors, if any, to the extent they have a need to know in order to perform CONSULTANT’s obligations to CITY under this Agreement and for no other purpose, provided that the CONSULTANT informs them of, and requires them to follow, the confidentiality and security obligations of this Agreement.

28.2. “Confidential Information” means all data, information (including without limitation “Personal Information” about a California resident as defined in Civil Code Section 1798 et seq., as amended from time to time) and materials, in any form or media, tangible or intangible, provided or otherwise made available to CONSULTANT by CITY, directly or indirectly, pursuant to this Agreement. Confidential Information excludes information that CONSULTANT can show by appropriate documentation: (i) was publicly known at the time it was provided or has subsequently become publicly known other than by a breach of this Agreement; (ii) was rightfully in CONSULTANT’s possession free of any obligation of confidence prior to receipt of Confidential Information; (iii) is rightfully obtained by CONSULTANT from a third party without breach of any confidentiality obligation; (iv) is independently developed by employees of CONSULTANT without any use of or access to the Confidential Information; or (v) CONSULTANT has written consent to disclose signed by an authorized representative of CITY.

28.3. Notwithstanding the foregoing, CONSULTANT may disclose Confidential Information to the extent required by order of a court of competent jurisdiction or governmental body, provided that CONSULTANT will notify CITY in writing of such order immediately upon receipt and prior to any such disclosure (unless CONSULTANT is prohibited by law from doing so), to give CITY an opportunity to oppose or otherwise respond to such order.

28.4. CONSULTANT will notify City promptly upon learning of any breach in

the security of its systems or unauthorized disclosure of, or access to, Confidential Information in its possession or control, and if such Confidential Information consists of Personal Information, CONSULTANT will provide information to CITY sufficient to meet the notice requirements of Civil Code Section 1798 et seq., as applicable, as amended from time to time.

28.5. Prior to or upon termination or expiration of this Agreement, CONSULTANT will honor any request from the CITY to return or securely destroy all copies of Confidential Information. All Confidential Information is and will remain the property of the CITY and nothing contained in this Agreement grants or confers any rights to such Confidential Information on CONSULTANT.

28.6. If selected in Section 30 (Exhibits), this Agreement is also subject to the terms and conditions of the Information Privacy Policy and Cybersecurity Terms and Conditions.

## **SECTION 29. MISCELLANEOUS PROVISIONS.**

29.1. This Agreement will be governed by California law, without regard to its conflict of law provisions.

29.2. In the event that an action is brought, the parties agree that trial of such action will be vested exclusively in the state courts of California in the County of Santa Clara, State of California.

29.3. The prevailing party in any action brought to enforce the provisions of this Agreement may recover its reasonable costs and attorneys' fees expended in connection with that action. The prevailing party shall be entitled to recover an amount equal to the fair market value of legal services provided by attorneys employed by it as well as any attorneys' fees paid to third parties.

29.4. This Agreement, including all exhibits, constitutes the entire and integrated agreement between the parties with respect to the subject matter of this Agreement, and supersedes all prior agreements, negotiations, representations, statements and undertakings, either oral or written. This Agreement may be amended only by a written instrument, which is signed by the authorized representatives of the parties and approved as required under Palo Alto Municipal Code, as amended from time to time.

29.5. If a court of competent jurisdiction finds or rules that any provision of this Agreement is void or unenforceable, the unaffected provisions of this Agreement will remain in full force and effect.

29.6. In the event of a conflict between the terms of this Agreement and the exhibits hereto (per Section 30) or CONSULTANT's proposal (if any), the Agreement shall control. In the event of a conflict between the exhibits hereto and CONSULTANT's proposal (if any), the exhibits shall control.

29.7. The provisions of all checked boxes in this Agreement shall apply to this Agreement; the provisions of any unchecked boxes shall not apply to this Agreement.

29.8. All section headings contained in this Agreement are for convenience and reference only and are not intended to define or limit the scope of any provision of this Agreement.

29.9. This Agreement may be signed in multiple counterparts, which, when executed by the authorized representatives of the parties, shall together constitute a single binding agreement.

**SECTION 30. EXHIBITS.** Each of the following exhibits, if the check box for such exhibit is selected below, is hereby attached and incorporated into this Agreement by reference as though fully set forth herein:

- ☒ EXHIBIT A: SCOPE OF SERVICES
- ☒ ATTACHMENT A-1: FALCON CAMERAS SPECIFICATIONS
- ☒ ATTACHMENT B-1: STANDARD IMPLEMENTATION
- ☒ ATTACHMENT C-1: ADVANCED IMPLEMENTATION
- ☒ ATTACHMENT D-1: ELECTRICIAN INSTALLATION STEPS
- ☒ EXHIBIT A-1: PROFESSIONAL SERVICES TASK ORDER
- ☒ EXHIBIT B: SCHEDULE OF PERFORMANCE
- ☒ EXHIBIT C: COMPENSATION
- ☒ EXHIBIT C-1: SCHEDULE OF RATES
- ☒ EXHIBIT D: INSURANCE REQUIREMENTS
- ☒ EXHIBIT E: DIR REGISTRATION FOR PUBLIC WORKS CONTRACTS
- ☒ EXHIBIT F: CLAIMS FOR PUBLIC CONTRACT CODE SECTION 9204  
PUBLIC WORKS PROJECTS
- ☒ EXHIBIT G: SURVEILLANCE ORDINANCE
- ☒ EXHIBIT H: INFORMATION PRIVACY POLICY
- ☒ EXHIBIT I: CYBERSECURITY TERMS AND CONDITIONS
- ☒ EXHIBIT J: FLOCK GROUP SERVICES ADDITIONAL TERMS OF  
SERVICE

For the purposes of construing, interpreting and resolving inconsistencies between and among the Exhibits of this Agreement, the Exhibits shall have the order of precedence as set forth in the preceding section. (Sections 1 through 30 of this Agreement shall have precedence over all of the Exhibits.) If a claimed inconsistency cannot be resolved through the order of precedence, the City shall have the sole power to decide which document or provision shall govern as may be in the best interests of the City.

***THIS AGREEMENT IS NOT COMPLETE UNLESS ALL SELECTED EXHIBITS ARE ATTACHED.***

**CONTRACT No. S23187316 SIGNATURE PAGE**

IN WITNESS WHEREOF, the parties hereto have by their duly authorized representatives executed this Agreement as of the date first above written.

**CITY OF PALO ALTO**

\_\_\_\_\_  
City Manager

APPROVED AS TO FORM:

\_\_\_\_\_  
City Attorney or Designee

(Required on Contracts over \$25,000)

**FLOCK GROUP INC. dba FLOCK  
SAFETY**

**Officer 1**

By: DocuSigned by:

*Mark Smith*

Name: AC5C931454C24E31 Mark Smith

Title: General Counsel

**Officer 2 (Required for Corp. or LLC)**

By: DocuSigned by:

*James LaCamp*

Name: BE87BDF876394B6 James LaCamp

Title: CFO

## **EXHIBIT A SCOPE OF SERVICES**

CONSULTANT shall provide the Services detailed in this Exhibit A, entitled “SCOPE OF SERVICES”.

### **I. AUTOMATIC LICENSE PLATE READER SYSTEM SERVICES**

- a) CONSULTANT’s surveillance devices shall function as vehicular motion-activated sensors to detect capturing sight and sound to decode images by narrowing down visual criteria related searches. CONSULTANT’s Automated License Plate Reader Systems (ALPR or LPR) includes vehicle fingerprint technology, which will develop machine learning and computer vision analyses to break down captured evidence into searchable queries. The ALPR will provide the following:

Visual Evidence by:

- vehicle make, type, and color;
- license plate (missing plate, covered plate, paper plate, state of the license plate); and
- unique features (roof rack, bumper stickers, and window stickers)

Contextual Evidence by:

- timestamp;
- number of times vehicle has been captured in the last 30 days; and
- associated vehicles.

- b) CONSULTANT’s database video footage on visual and contextual evidences are downloadable data deliverables to provide CITY users.

### **Survey Locations**

CONSULTANT shall furnish leasing all equipment, equipment maintenance, installation, materials, tools, and software services to implement ALPR devices across City of Palo Alto’s designated key areas that shall include but not limited to the following tasks:

- a) CONSULTANT shall coordinate with CITY Project Manager and Public Works department to present several viable options for solar or AC power camera install feasibility for of up to forty (40) locations to present a deployment plan for the CITY to review and approve camera locations. CONSULTANT’s deployment plan shall include a technician to conduct site survey to:
- evaluate/reconfirm feasibility of a location per camera (location assessment, solar assessment, visibility review, etc.;
  - check line of sight to the road, safety plans and methods required to perform camera installation; and
  - evaluate/reconfirm adequate AT&T or T-Mobile cellular services in the area that is suitable by placing a white flag per location.
- b) CITY shall provide support (if needed) to provide permits, special equipment or vehicles, custom engineering drawings or traffic plans, concrete cutting and AC-powered installation source;
- c) CONSULTANT shall coordinate with State’s PG&E “811” call service and CITY Utilities

department for safe underground digging to mark each camera approved marking location for underground utilities within a 10-foot radius.

- d) In preparation of scheduling camera installation date, CONSULTANT shall ship any site-specific material(s) that CONSULTANT's technician does not have on site and coordinate with CITY staff on scheduling process of any permits required, special equipment, safety assessment and traffic control safety plans.

**Installation** (one-time service per camera location)

- a) On scheduled start date, CONSULTANT shall mount twenty (20) Falcon Camera devices (specifications are in detail reference as *Attachment A-1*) that meet standard installation procedures for Safety Performance Evaluation of Highway and Assessing Safety Hardware ([NCHRP350/MASH](#)), while adhering to standard procedural plans from the Manual of Uniform Traffic Control Devices ([MUTCD](#)).
- b) Of the 20 camera locations, fourteen (14) cameras shall require Standard Implementation service, which CONSULTANT shall perform camera mount(s) onto CITY's existing traffic pole infrastructure to meet CITY's/County of Santa Clara's Right of Way (ROW) for public use of existing property or future streets, curbs, planting strips or sidewalks. Standard Implementation is detailed therein in *Attachment B-1*.
- c) The remaining six (6) cameras shall require Advance Implementation service using required Department of Transportation (DOT) approved standard 12' CONSULTANT's above grade breakaway pole to meet DOT's "Right of Way and Land Survey" activity requirements within Caltrans' Interstate of Highway System geographic boundaries. Advanced Implementation is detailed therein in *Attachment C-1*.
- d) Upon camera mount installation of each cameras, CONSULTANT shall collaborate with CITY Utilities department for CITY electrician(s) to install AC power source and connectivity to the cameras (per Electrician Installation Steps specified in *Attachment D-1*). CONSULTANT shall inspect camera to verify device and visual line of sight meets mount/placement specification.

**Maintenance**

CONSULTANT's Field Operation team is responsible for physical installation and maintenance of leased cameras and associated equipment provided by CONSULTANT during term of this Agreement. This includes CONSULTANT's team of technicians and maintenance schedulers to coordinate maintenance service with CITY staff.

**Subscription/Software**

Post-Camera-Installation, CONSULTANT shall set up a software licensing subscription account training for CITY Project Manager to designate authorized CITY staff to access CONSULTANT's permission web-based portal and provide the CITY with training on best practices to search for relevant data.

**II. ADVANCED SEARCH**

CONSULTANT shall collaborate with CITY police staff upon request to perform via the CONSULTANT'S software web interface to utilize advanced evidence search capabilities to operate convoy analysis; multi-geo search, visual search queries; and common plate analysis in



which the ALPR shall perform:

- Visual Search to upload any digital image (i.e.) Ring doorbell footage, closed-circuit television stills or mobile phone pictures) to conduct vehicle search.
- Multi-Geo Search to connect crimes across different locations to a common suspect vehicle to expedite case clearance and prevent repeat offenses.
- Convoy Analysis on identifying vehicles frequently traveling together to identify accomplices in organized crimes (i.e. Motor Vehicle theft & drug trafficking).

### **III. ADDITIONAL SERVICES (Optional)**

CITY can request for additional surveillance relocation(s), which shall be mutually written in Agreement as detailed therein within a Task Order (Exhibit A-1 form) per Section 4 of the Agreement. CONSULTANT shall perform the following optional Additional Services for:

- a) camera relocations; and
- b) camera and/or pole replacement to reinstall damage, theft or vandalism of ALPR equipment.

## **ATTACHMENT A-1 FALCON CAMERAS SPECIFICATIONS**

### **Falcon Cameras**

#### Use Cases:

- CONSULTANT’S SAFETY LICENSE PLATE READERS (LPRs) are designed to capture images of near license plates, aimed in the direction of traffic.
- CONSULTANT’S LPRs are not designed to capture pedestrians, sidewalks, dumpsters, gates, other areas of non-vehicle traffic, or intersections.

#### Placement:

- It captures vehicles driving away from an intersection.
- It cannot point into the middle of an intersection.
- It should be placed after the intersection, to prevent “stop and go” motion activation, or “stop and go” traffic.

#### Mounting:

- It can be mounted on existing utility, light, or traffic signal poles, or 12 foot CONSULTANT’s poles. **\*\*NOTE\*\*** Permitting (or permission from pole owner) may be required in order to use existing infrastructure or install in specific areas, depending on local regulations & policies.
- It should be mounted one per pole\*. If using AC power, they can be mounted 2 per pole.
  - \*Cameras need sufficient power. Since a solar panel is required per camera, it can prevent sufficient solar power if 2 cameras and 2 solar panels were on a single pole (by blocking visibility). Therefore, if relying on solar power, only one camera can be installed per pole.
- They can be powered with solar panels or direct wire-in AC Power (no outlets). **\*\*NOTE\*\*** CONSULTANT does not provide Electrical services. Once installed, the agency or community must work with an electrician to wire the cameras. Electrician services should be completed within two days of installation to prevent the camera from dying.
- They will require adequate cellular service using AT&T or T-Mobile to be able to process & send images

### **Solar Panels**

- Solar panels need unobstructed southern -facing views

### **Pole**

- If a location requires “DOT” approved pole (i.e., not CONSULTANT’s standard pole), the “advanced implementation” cost will apply per Exhibit C-1, Schedule of Rates

## ATTACHMENT B-1 STANDARD IMPLEMENTATION

Once designated camera locations are confirmed, as part of the Standard Implementation Service, CONSULTANT shall perform the following:

- a) An in-person site survey to confirm the installation feasibility of a location (location assessment, solar assessment, visibility review, etc.)
- b) Confirm that a location is safe for work by following State utility locating procedures. Work with local utilities to prevent service interruptions during the installation.
  - Engage 811 'Call-before-you-Dig' system to receive legal dig date; and
  - Apply approved markings Coordinate with 811 regarding any necessary high-risk dig clearances or required vendor meets.
- c) Each installation may include the following:
  - Installation of camera and solar panel with **standard, 12' above grade CONSULTANT's break away pole.**
  - Installation of camera and AC adapter that a qualified electrician can connect to AC power.
    - CONSULTANT shall provide and mount an AC adapter that a qualified electrician can connect to AC power following their electrical wiring requirements per *Exhibit D-1*. CONSULTANT cannot make any AC connections or boreholes in any material other than dirt, grass, loose gravel (or other non-diggable material). Electrical work requiring a licensed electrician and associated costs, not included in the scope of work. CITY staff will conduct the electrical tasks.
  - Access requiring up to a 14' A-frame ladder
  - Standard MUTCD traffic control procedures performed by a CONSULTANT's technician
- d) Obtain a business license to operate in the City and State of camera location.

### OUT OF SCOPE ITEMS

By default, CONSULTANT does not include the following as part of the Advanced Implementation Service but can optionally provide a quote for sourcing (additional cost):

- Installation on Standard, 12' above grade Flock breakaway pole or existing infrastructure;
- A Bucket Truck for accessing horizontal/cross-beams and/or height above 14';
- Special equipment rentals for site access;
- Site-specific engineered traffic plans;
- Third-party provided traffic control;
- State or City-specific specialty contractor licenses;
- Custom engineered drawings;
- Electrical work requires a licensed electrician. CONSULTANT will provide and mount an AC; adapter that a qualified electrician can connect to AC power but cannot make any AC; connections or boreholes in any material other than dirt, grass, loose gravel (or other non-diggable material)
- Concrete cutting;
- Private utility search for privately owned items not included in standard 811 procedures (communication, networking, sprinklers, etc.);
- Upgrades to power sources to ready them for Flock power (additional fuses, switches, breakers, etc.)
- Fees or costs associated with filing for required CITY, County, or State permits

## ATTACHMENT C-1 ADVANCED IMPLEMENTATION

Once designated camera locations are confirmed, as part of the Advanced Implementation Service, CONSULTANT shall perform the following:

- a) An in-person site survey to confirm the installation feasibility of a location (location assessment, solar assessment, visibility review, etc.)
- b) Confirm that a location is safe for work by following State utility locating procedures. Work with local utilities to prevent service interruptions during the installation.
  - Engage 811 ‘Call-before-you-Dig’ system to receive legal dig date; and
  - Apply approved markings Coordinate with 811 regarding any necessary high-risk dig clearances or required vendor meets.
- c) Each installation may include the following:
  - Installation of camera and solar panel on a suitable **NCHRP 350 or MASH approved pole**.
  - Installation of camera and AC adapter that a qualified electrician can connect to AC power.
    - CONSULTANT shall provide and mount an AC adapter that a qualified electrician can connect to AC power following their electrical wiring requirements per *Exhibit D-1*. CONSULTANT cannot make any AC connections or boreholes in any material other than dirt, grass, loose gravel (or other non-diggable material). Electrical work requiring a licensed electrician and associated costs, not included in the scope of work. CITY staff will conduct the electrical tasks.
  - Access requiring up to a 14’ A-frame ladder
  - Standard MUTCD traffic control procedures performed by a CONSULTANT’s technician
- d) Obtain a business license to operate in the City and State of camera location.

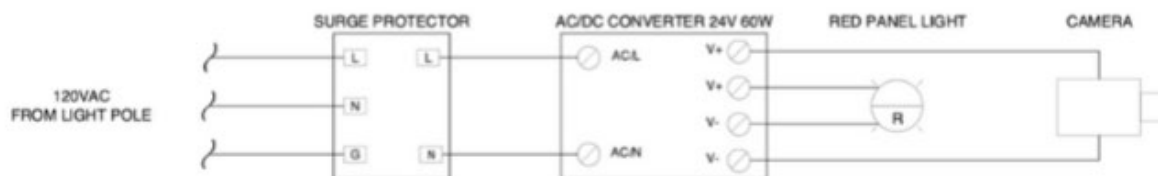
### OUT OF SCOPE ITEMS

By default, CONSULTANT does not include the following as part of the Advanced Implementation Service but can optionally provide a quote for sourcing (additional cost):

- Installation on Standard, 12’ above grade Flock breakaway pole or existing infrastructure;
- A Bucket Truck for accessing horizontal/cross-beams and/or height above 14’;
- Special equipment rentals for site access;
- Site-specific engineered traffic plans;
- Third-party provided traffic control;
- State or City-specific specialty contractor licenses;
- Custom engineered drawings;
- Electrical work requires a licensed electrician. CONSULTANT will provide and mount an AC; adapter that a qualified electrician can connect to AC power but cannot make any AC; connections or boreholes in any material other than dirt, grass, loose gravel (or other non-diggable material)
- Concrete cutting;
- Private utility search for privately owned items not included in standard 811 procedures (communication, networking, sprinklers, etc.);
- Upgrades to power sources to ready them for Flock power (additional fuses, switches, breakers, etc.)
- Fees or costs associated with filing for required CITY, County, or State permits

## ATTACHMENT D-1 ELECTRICIAN INSTALLATION STEPS

1. Run AC cable and conduit to the box according to NEC Article 300 and any applicable local codes. The gland accepts ½" conduit
2. Run Open the box using hinges
3. Connect AC Mains per wiring diagram below:
  - a. Connect AC Neutral wire to the Surge Protector white Neutral wire using the open position on the lever nut.
  - b. Connect AC Line wire to the Surge Protector black Line wire using the open position on the lever nut.
  - c. Connect AC Ground wire to the Surge Protector green ground wire using the open position on the lever nut.
4. Verify that both the RED LED is lit on the front of the box
5. Close box and zip tie the box shut with the provided zip tie
6. While still on site, call Flock who will remotely verify that power is working correctly:
  - Southeast Region - (678) 562-8766
  - West-Region - (804) 607-9213
  - Central & NE Region - (470) 868-4027



## EXHIBIT A-1 PROFESSIONAL SERVICES TASK ORDER

CONSULTANT shall perform the Services detailed below in accordance with all the terms and conditions of the Agreement referenced in Item 1A below. All exhibits referenced in Item 8 are incorporated into this Task Order by this reference. CONSULTANT shall furnish the necessary facilities, professional, technical and supporting personnel required by this Task Order as described below.

---

CONTRACT NO.

OR PURCHASE ORDER REQUISITION NO. (AS APPLICABLE)

- 1A. MASTER AGREEMENT NO. (MAY BE SAME AS CONTRACT / P.O. NO. ABOVE):
  - 1B. TASK ORDER NO.:
  2. CONSULTANT NAME:
  3. PERIOD OF PERFORMANCE: START: COMPLETION:
  4. TOTAL TASK ORDER PRICE: \$ \_\_\_\_\_  
BALANCE REMAINING IN MASTER AGREEMENT/CONTRACT \$ \_\_\_\_\_
  5. BUDGET CODE \_\_\_\_\_  
COST CENTER \_\_\_\_\_  
COST ELEMENT \_\_\_\_\_  
WBS/CIP \_\_\_\_\_  
PHASE \_\_\_\_\_
  6. CITY PROJECT MANAGER'S NAME & DEPARTMENT: \_\_\_\_\_
  7. DESCRIPTION OF SCOPE OF SERVICES (Attachment A)  
MUST INCLUDE:
    - SERVICES AND DELIVERABLES TO BE PROVIDED
    - SCHEDULE OF PERFORMANCE
    - MAXIMUM COMPENSATION AMOUNT AND RATE SCHEDULE (as applicable)
    - REIMBURSABLE EXPENSES, if any (with "not to exceed" amount)
  8. ATTACHMENTS: A: Task Order Scope of Services B (if any): \_\_\_\_\_
- 

**I hereby authorize the performance of the work described in this Task Order.**

**APPROVED:**  
CITY OF PALO ALTO

BY: \_\_\_\_\_  
Name \_\_\_\_\_  
Title \_\_\_\_\_  
Date \_\_\_\_\_

**I hereby acknowledge receipt and acceptance of this Task Order and warrant that I have authority to sign on behalf of Consultant.**

**APPROVED:**  
COMPANY NAME: \_\_\_\_\_

BY: \_\_\_\_\_  
Name \_\_\_\_\_  
Title \_\_\_\_\_  
Date \_\_\_\_\_

## EXHIBIT B SCHEDULE OF PERFORMANCE

CONSULTANT shall perform the Services so as to complete each milestone within the number of days/weeks specified below. The time to complete each milestone may be increased or decreased by mutual written agreement of the Project Managers for CONSULTANT and CITY so long as all work is completed within the term of the Agreement. CONSULTANT shall provide a detailed schedule of work consistent with the schedule below within 2 weeks of receipt of the notice to proceed (“NTP”) from the CITY.

<b>Milestones</b>	<b>Completion Number of Days/Weeks (as specified below) from NTP</b>
1. ALPR Services 20 Camera Installation – Year 1 (one-time service only)	60 days
2. ALPR Services w/ Advanced Search – Year 1 (June 1, 2023-May 31, 2024)	Ongoing within term of Agreement (subject to completion of milestone 1)
3. ALPR Services w/ Advanced Search – Year 2 (June 1, 2024-May 31, 2025)	Ongoing within term of Agreement (subject to completion of milestone 1)
4. ALPR Services w/ Advanced Search – Year 3 (June 1, 2025-May 31, 2026)	Ongoing within term of Agreement (subject to completion of milestone 1)

☒ Optional Schedule of Performance Provision for On-Call or Additional Services Agreements.  
(This provision only applies if checked and only applies to on-call agreements per Section 1 or agreements with Additional Services per Section 4.)

The schedule of performance shall be as provided in the approved Task Order, as detailed in Section 1 (Scope of Services) in the case of on-call Services, or as detailed in Section 4 in the case of Additional Services, provided in all cases that the schedule of performance shall fall within the term as provided in Section 2 (Term) of this Agreement.

## **EXHIBIT C COMPENSATION**

CITY agrees to compensate CONSULTANT for Services performed in accordance with the terms and conditions of this Agreement, and as set forth in the budget schedule below. Compensation shall be calculated based on the rate schedule attached as Exhibit C-1 up to the not to exceed budget amount for each task set forth below.

CITY's Project Manager may approve in writing the transfer of budget amounts between any of the tasks or categories listed below, provided that the total compensation for the Services, including any specified reimbursable expenses, and the total compensation for Additional Services (if any, per Section 4 of the Agreement) do not exceed the amounts set forth in Section 4 of this Agreement.

CONSULTANT agrees to complete all Services, any specified reimbursable expenses, and Additional Services (if any, per Section 4), within this/these amount(s). Any work performed or expenses incurred for which payment would result in a total exceeding the maximum amount of compensation set forth in this Agreement shall be at no cost to the CITY.

### **BUDGET SCHEDULE**

<b>TASK</b>	<b>NOT TO EXCEED AMOUNT</b>
Task 1 (ALPR Services 20 Camera Installation – Year 1 [one-time service only])	\$9,400
Task 2 (ALPR Services w/ Advanced Search – Year 1 [June 1, 2023-May 31, 2024])	\$52,500
Task 3 (ALPR Services w/ Advanced Search – Year 2 [June 1, 2024-May 31, 2025])	\$52,500
Task 4 (ALPR Services w/ Advanced Search – Year 3 [June 1, 2024-May 31, 2025])	\$52,500
Sub-total for Services	<b>\$166,900</b>
Reimbursable Expenses (if any)	<b>\$0</b>
<b>Total for Services and Reimbursable Expenses</b>	<b>\$166,900</b>
Additional Services (if any, per Section 4 [Year 1 through 3 – \$2,500 annually])	\$7,500
<b>Maximum Total Compensation</b>	<b>\$174,400</b>

### **REIMBURSABLE EXPENSES**

CONSULTANT'S ordinary business expenses, such as administrative, overhead, administrative support time/overtime, information systems, software and hardware, photocopying, telecommunications (telephone, internet), in-house printing, insurance and



other ordinary business expenses, are included within the scope of payment for Services and are not reimbursable expenses hereunder.

Reimbursable expenses, if any are specified as reimbursable under this section, will be reimbursed at actual cost. The expenses (by type, e.g. travel) for which CONSULTANT will be reimbursed are: **NONE** up to the not-to-exceed amount of: **\$0.00**.

## EXHIBIT C-1 SCHEDULE OF RATES

CONSULTANT's schedule of rates is as follows:

### CONSULTANT's Professional Services and One-Time Installation Purchases

Description	Price/Usage Fee	Qty	Subtotal
Professional Services - Standard Implementation	\$350.00	14.00	\$4,900.00
Professional Services - Advanced Implementation	\$750.00	6.00	\$4,500.00

### Hardware and Software Products

Annual recurring amounts over subscription term:

Description	Price/Usage Fee	Qty	Subtotal
Falcon Camera Lease & Software Licensing	\$2,500.00	20.00	\$50,000.00
Flock Safety Advanced Search	\$2,500.00	1.00	\$2,500.00

### Additional Service - ALPR Equipment Replacement & Relocation

(includes installation labor):

Description	Qty	Price/Usage Fee
Camera Replacement	1	\$500.00
Pole Replacement	1	\$500.00

## EXHIBIT D INSURANCE REQUIREMENTS

CONTRACTORS TO THE CITY OF PALO ALTO (CITY), AT THEIR SOLE EXPENSE, SHALL FOR THE TERM OF THE CONTRACT OBTAIN AND MAINTAIN INSURANCE IN THE AMOUNTS FOR THE COVERAGE SPECIFIED BELOW, **AFFORDED BY COMPANIES WITH AM BEST'S KEY RATING OF A-VII, OR HIGHER, AUTHORIZED TO TRANSACT INSURANCE BUSINESS IN THE STATE OF CALIFORNIA.**

AWARD IS CONTINGENT ON COMPLIANCE WITH CITY'S INSURANCE REQUIREMENTS SPECIFIED HEREIN.

REQUIRED	TYPE OF COVERAGE	REQUIREMENT	MINIMUM LIMITS	
			EACH OCCURRENCE	AGGREGATE
YES	WORKER'S COMPENSATION	STATUTORY		
YES	EMPLOYER'S LIABILITY	STATUTORY		
YES	GENERAL LIABILITY, INCLUDING PERSONAL INJURY, BROAD FORM PROPERTY DAMAGE BLANKET CONTRACTUAL, PRODUCTS/COMPLETED OPERATIONS AND FIRE LEGAL LIABILITY	BODILY INJURY	\$2,000,000	\$2,000,000
		PROPERTY DAMAGE	\$2,000,000	\$2,000,000
		BODILY INJURY & PROPERTY DAMAGE COMBINED.	\$2,000,000	\$2,000,000
YES	<p>TECHNOLOGY ERRORS AND OMISSIONS LIABILITY COVERAGE. THE POLICY SHALL AT A MINIMUM COVER PROFESSIONAL MISCONDUCT OR LACK OF REQUISITE SKILL FOR THE PERFORMANCE OF SERVICES DEFINED IN THE CONTRACT AND SHALL ALSO PROVIDE COVERAGE FOR THE FOLLOWING RISKS:</p> <p>(i) NETWORK SECURITY LIABILITY ARISING FROM UNAUTHORIZED ACCESS TO, USE OF, OR TAMPERING WITH COMPUTERS OR COMPUTER SYSTEMS, INCLUDING HACKERS, EXTORTION, AND</p> <p>(ii) LIABILITY ARISING FROM INTRODUCTION OF ANY FORM OF MALICIOUS SOFTWARE INCLUDING COMPUTER VIRUSES INTO, OR OTHERWISE CAUSING DAMAGE TO THE CITY'S OR THIRD PERSON'S COMPUTER, COMPUTER SYSTEM, NETWORK, OR SIMILAR COMPUTER RELATED PROPERTY AND THE DATA, SOFTWARE AND PROGRAMS THEREON. CONTRACTOR SHALL MAINTAIN IN FORCE DURING THE FULL LIFE OF THE CONTRACT.</p> <p>THE POLICY SHALL PROVIDE COVERAGE FOR BREACH RESPONSE COSTS AS WELL AS REGULATORY FINES AND PENALTIES AS WELL AS CREDIT MONITORING EXPENSES WITH LIMITS SUFFICIENT TO RESPOND TO THESE OBLIGATIONS.</p>	ALL DAMAGES	\$2,000,000	\$2,000,000

YES	CYBER AND PRIVACY INSURANCE. SUCH INSURANCE SHALL INCLUDE COVERAGE FOR LIABILITY ARISING FROM COVERAGE IN AN AMOUNT SUFFICIENT TO COVER THE FULL REPLACEMENT VALUE OF DAMAGE TO, ALTERATION OF, LOSS OF, THEFT, DISSEMINATION OR DESTRUCTION OF ELECTRONIC DATA AND/OR USE OF CONFIDENTIAL INFORMATION, “PROPERTY” OF THE CITY OF PALO ALTO THAT WILL BE IN THE CARE, CUSTODY, OR CONTROL OF VENDOR, INFORMATION INCLUDING BUT NOT LIMITED TO, BANK AND CREDIT CARD ACCOUNT INFORMATION OR PERSONAL INFORMATION, SUCH AS NAME, ADDRESS, SOCIAL SECURITY NUMBERS, PROTECTED HEALTH INFORMATION OR OTHER PERSONAL IDENTIFICATION INFORMATION, STORED OR TRANSMITTED IN ELECTRONIC FORM.	ALL DAMAGES	\$2,000,000	\$2,000,000
YES	AUTOMOBILE LIABILITY, INCLUDING ALL OWNED, HIRED, NON-OWNED	BODILY INJURY EACH PERSON EACH OCCURRENCE  PROPERTY DAMAGE  BODILY INJURY AND PROPERTY DAMAGE, COMBINED	\$1,000,000 \$1,000,000 \$1,000,000  \$1,000,000  \$1,000,000	\$1,000,000 \$1,000,000 \$1,000,000  \$1,000,000  \$1,000,000
YES	PROFESSIONAL LIABILITY, INCLUDING, ERRORS AND OMISSIONS, MALPRACTICE (WHEN APPLICABLE), AND NEGLIGENT PERFORMANCE	ALL DAMAGES	\$1,000,000	
YES	<b>THE CITY OF PALO ALTO IS TO BE NAMED AS AN ADDITIONAL INSURED:</b> CONTRACTOR, AT ITS SOLE COST AND EXPENSE, SHALL OBTAIN AND MAINTAIN, IN FULL FORCE AND EFFECT THROUGHOUT THE ENTIRE TERM OF ANY RESULTANT AGREEMENT, THE INSURANCE COVERAGE HEREIN DESCRIBED, INSURING NOT ONLY CONTRACTOR AND ITS SUBCONSULTANTS, IF ANY, BUT ALSO, WITH THE EXCEPTION OF WORKERS’ COMPENSATION, EMPLOYER’S LIABILITY AND PROFESSIONAL INSURANCE, <b>NAMING AS ADDITIONAL INSUREDS CITY, ITS COUNCIL MEMBERS, OFFICERS, AGENTS, AND EMPLOYEES.</b>			

I. INSURANCE COVERAGE MUST INCLUDE:

A. A CONTRACTUAL LIABILITY ENDORSEMENT PROVIDING INSURANCE COVERAGE FOR CONTRACTOR'S AGREEMENT TO INDEMNIFY CITY.

II. CONTRACTOR MUST SUBMIT CERTIFICATE(S) OF INSURANCE EVIDENCING REQUIRED COVERAGE AT THE FOLLOWING URL: <https://www.planetbids.com/portal/portal.cfm?CompanyID=25569>.

III. ENDORSEMENT PROVISIONS, WITH RESPECT TO THE INSURANCE AFFORDED TO "ADDITIONAL INSUREDS"

A. PRIMARY COVERAGE

WITH RESPECT TO CLAIMS ARISING OUT OF THE OPERATIONS OF THE NAMED INSURED, INSURANCE AS AFFORDED BY THIS POLICY IS PRIMARY AND IS NOT ADDITIONAL TO OR CONTRIBUTING WITH ANY OTHER INSURANCE CARRIED BY OR FOR THE BENEFIT OF THE ADDITIONAL INSUREDS.

B. CROSS LIABILITY

THE NAMING OF MORE THAN ONE PERSON, FIRM, OR CORPORATION AS INSUREDS UNDER THE POLICY SHALL NOT, FOR THAT REASON ALONE, EXTINGUISH ANY RIGHTS OF THE INSURED

AGAINST ANOTHER, BUT THIS ENDORSEMENT, AND THE NAMING OF MULTIPLE INSUREDS, SHALL NOT INCREASE THE TOTAL LIABILITY OF THE COMPANY UNDER THIS POLICY.

C. NOTICE OF CANCELLATION

1. IF THE POLICY IS CANCELED BEFORE ITS EXPIRATION DATE FOR ANY REASON OTHER THAN THE NON-PAYMENT OF PREMIUM, THE CONSULTANT SHALL PROVIDE CITY AT LEAST A THIRTY (30) DAY WRITTEN NOTICE BEFORE THE EFFECTIVE DATE OF CANCELLATION.
2. IF THE POLICY IS CANCELED BEFORE ITS EXPIRATION DATE FOR THE NON-PAYMENT OF PREMIUM, THE CONSULTANT SHALL PROVIDE CITY AT LEAST A TEN (10) DAY WRITTEN NOTICE BEFORE THE EFFECTIVE DATE OF CANCELLATION.

**VENDORS ARE REQUIRED TO FILE THEIR EVIDENCE OF INSURANCE  
AND ANY OTHER RELATED NOTICES WITH THE CITY OF PALO ALTO  
AT THE FOLLOWING URL:**

**<HTTPS://WWW.PLANETBIDS.COM/PORTAL/PORTAL.CFM?COMPANYID=25569>**

**OR**

**[HTTP://WWW.CITYOFPALOALTO.ORG/GOV/DEPTS/ASD/PLANET\\_BIDS\\_HOW\\_TO.ASP](HTTP://WWW.CITYOFPALOALTO.ORG/GOV/DEPTS/ASD/PLANET_BIDS_HOW_TO.ASP)**

## **EXHIBIT E**

### **DIR REGISTRATION FOR PUBLIC WORKS CONTRACTS**

This Exhibit shall apply only to a contract for public works construction, alteration, demolition, repair or maintenance work, CITY will not accept a bid proposal from or enter into this Agreement with CONSULTANT without proof that CONSULTANT and its listed subcontractors are registered with the California Department of Industrial Relations (“DIR”) to perform public work, subject to limited exceptions. City requires CONSULTANT and its listed subcontractors, if any, to comply with all applicable requirements of the California Labor Code including but not limited to Labor Code Sections 1720 through 1861, and all applicable related regulations, including but not limited to Subchapter 3, Title 8 of the California Code of Regulations Section 16000 et seq., as amended from time to time. This Exhibit E applies in addition to the provisions of Section 26 (Prevailing Wages and DIR Registration for Public Works Contracts) of the Agreement.

CITY provides notice to CONSULTANT of the requirements of California Labor Code Section 1771.1(a), which reads:

“A contractor or subcontractor shall not be qualified to bid on, be listed in a bid proposal, subject to the requirements of Section 4104 of the Public Contract Code, or engage in the performance of any contract for public work, as defined in this chapter, unless currently registered and qualified to perform public work pursuant to Section 1725.5. It is not a violation of this section for an unregistered contractor to submit a bid that is authorized by Section 7029.1 of the Business and Professions Code or Section 10164 or 20103.5 of the Public Contract Code, provided the contractor is registered to perform public work pursuant to Section 1725.5 at the time the contract is awarded.”

This Project is subject to compliance monitoring and enforcement by DIR. All contractors must be registered with DIR per Labor Code Section 1725.5 in order to submit a bid. All subcontractors must also be registered with DIR. No contractor or subcontractor may be awarded a contract for public work on a public works project unless registered with DIR. Additional information regarding public works and prevailing wage requirements is available on the DIR web site (see e.g. <http://www.dir.ca.gov>) as amended from time to time.

CITY gives notice to CONSULTANT and its listed subcontractors that CONSULTANT is required to post all job site notices prescribed by law or regulation.

CONSULTANT shall furnish certified payroll records directly to the Labor Commissioner (DIR) in accordance with Subchapter 3, Title 8 of the California Code of Regulations Section 16461 (8 CCR Section 16461).

CITY requires CONSULTANT and its listed subcontractors to comply with the requirements of Labor Code Section 1776, including but not limited to:

Keep accurate payroll records, showing the name, address, social security number, work classification, straight time and overtime hours worked each day and week, and the actual per diem wages paid to each journeyman, apprentice, worker, or other employee employed by, respectively, CONSULTANT and its listed subcontractors, in connection with the Project.

The payroll records shall be verified as true and correct and shall be certified and made available for inspection at all reasonable hours at the principal office of CONSULTANT and its listed subcontractors, respectively.

At the request of CITY, acting by its Project Manager, CONSULTANT and its listed subcontractors shall make the certified payroll records available for inspection or furnished upon request to the CITY Project Manager within ten (10) days of receipt of CITY's request.

☒ CITY requests CONSULTANT and its listed subcontractors to submit the certified payroll records to CITY's Project Manager at the end of each week during the Project.

If the certified payroll records are not provided as required within the 10-day period, then CONSULTANT and its listed subcontractors shall be subject to a penalty of one hundred dollars (\$100.00) per calendar day, or portion thereof, for each worker, and CITY shall withhold the sum total of penalties from the progress payment(s) then due and payable to CONSULTANT.

Inform CITY's Project Manager of the location of CONSULTANT's and its listed subcontractors' payroll records (street address, city and county) at the commencement of the Project, and also provide notice to CITY's Project Manager within five (5) business days of any change of location of those payroll records.

Eight (8) hours labor constitutes a legal day's work. CONSULTANT shall forfeit as a penalty to CITY, \$25.00 for each worker employed in the execution of the Agreement by CONSULTANT or any subcontractor for each calendar day during which such worker is required or permitted to work more than eight (8) hours in any one calendar day or forty (40) hours in any one calendar week in violation of the provisions of the Labor Code, and in particular, Sections 1810 through 1815 thereof, except that work performed by employees of CONSULTANT or any subcontractor in excess of eight (8) hours per day, or forty (40) hours during any one week, shall be permitted upon compensation for all hours worked in excess of eight (8) hours per day, or forty (40) hours per week, at not less than one and one-half (1&1/2) times the basic rate of pay, as provided in Section 1815.

CONSULTANT shall secure the payment of workers' compensation to its employees as provided in Labor Code Sections 1860 and 3700 (Labor Code 1861). CONSULTANT shall sign and file with the CITY a statutorily prescribed statement acknowledging its obligation to secure the payment of workers' compensation to its employees before beginning work (Labor Code 1861). CONSULTANT shall post job site notices per regulation (Labor Code 1771.4(a)(2)).

CONSULTANT shall comply with the statutory requirements regarding employment of apprentices including without limitation Labor Code Section 1777.5. The statutory provisions will be enforced for penalties for failure to pay prevailing wages and for failure to comply with wage and hour laws.

## **EXHIBIT F**

### **Claims for Public Contract Code Section 9204 Public Works Projects**

The provisions of this Exhibit are provided in compliance with Public Contract Code Section 9204; they provide the exclusive procedures for any claims pursuant to Public Contract Code Section 9204 related to the Services performed under this Agreement.

**1. Claim Definition.** “Claim” means a separate demand by the Contractor sent by registered mail or certified mail with return receipt requested, for one or more of the following:

(A) A time extension, including, without limitation, for relief from damages or penalties for delay assessed by the City.

(B) Payment by the City of money or damages arising from the Services performed by, or on behalf of, the Contractor pursuant to the Agreement and payment for which is not otherwise expressly provided or to which the Contractor is not otherwise entitled.

(C) Payment of an amount that is disputed by the City.

**2. Claim Process.**

(A) Timing. Any Claim must be submitted to City in compliance with the requirements of this Exhibit no later than fourteen (14) days following the event or occurrence giving rise to the Claim. This time requirement is mandatory; failure to submit a Claim within fourteen (14) days will result in its being deemed waived.

(B) Submission. The Claim must be submitted to City in writing, clearly identified as a “Claim” submitted pursuant to this Exhibit, and must include reasonable documentation substantiating the Claim. The Claim must clearly identify and describe the dispute, including relevant references to applicable portions of the Agreement, and a chronology of relevant events. Any Claim for additional payment must include a complete, itemized breakdown of all labor, materials, taxes, insurance, and subcontract, or other costs. Substantiating documentation such as payroll records, receipts, invoices, or the like, must be submitted in support of each claimed cost. Any Claim for an extension of time or delay costs must be substantiated with schedule analysis and narrative depicting and explaining claimed time impacts.

(C) Review. Upon receipt of a Claim in compliance with this Exhibit, the City shall conduct a reasonable review of the Claim and, within a period not to exceed 45 days from receipt, shall provide the Contractor a written statement identifying what portion of the Claim is disputed and what portion is undisputed. Upon receipt of a Claim, the City and Contractor may, by mutual agreement, extend the time period provided in this paragraph 2.

(D) If City Council Approval Required. If the City needs approval from the City Council to provide the Contractor a written statement identifying the disputed portion and the undisputed portion of the Claim, and the City Council does not meet within the 45 days or within the mutually agreed to extension of time following receipt of a Claim sent by registered mail or certified mail, return receipt requested, the City shall have up to three days following the next duly publicly noticed meeting of the City Council after the 45-day period, or extension, expires to provide the Contractor a written statement identifying the disputed portion and the undisputed portion.



(E) Payment. Any payment due on an undisputed portion of the Claim shall be processed and made within 60 days after the City issues its written statement. If the City fails to issue a written statement, paragraph 3, below, shall apply.

### **3. Disputed Claims**

(A) Meet and Confer. If the Contractor disputes the City's written response, or if the City fails to respond to a Claim submitted pursuant to this Exhibit within the time prescribed, the Contractor may demand in writing an informal conference to meet and confer for settlement of the issues in dispute. Upon receipt of a demand in writing sent by registered mail or certified mail, return receipt requested, the City shall schedule a meet and confer conference within 30 days for settlement of the dispute. Within 10 business days following the conclusion of the meet and confer conference, if the Claim or any portion of the Claim remains in dispute, the City shall provide the Contractor a written statement identifying the portion of the Claim that remains in dispute and the portion that is undisputed. Any payment due on an undisputed portion of the Claim shall be processed and made within 60 days after the City issues its written statement.

(B) Mediation. Any remaining disputed portion of the Claim, as identified by the Contractor in writing, shall be submitted to nonbinding mediation, with the City and the Contractor sharing the associated costs equally. The City and Contractor shall mutually agree to a mediator within 10 business days after the disputed portion of the Claim has been identified in writing by the Contractor. If the parties cannot agree upon a mediator, each party shall select a mediator and those mediators shall select a qualified neutral third party to mediate the disputed portion of the Claim. Each party shall bear the fees and costs charged by its respective mediator in connection with the selection of the neutral mediator. If mediation is unsuccessful, the parts of the Claim remaining in dispute shall be subject to any other remedies authorized by the Agreement and laws.

(i) For purposes of this paragraph 3.B, mediation includes any nonbinding process, including, but not limited to, neutral evaluation or a dispute review board, in which an independent third party or board assists the parties in dispute resolution through negotiation or by issuance of an evaluation. Any mediation utilized shall conform to the timeframes in this section.

(ii) Unless otherwise agreed to by the City and the Contractor in writing, the mediation conducted pursuant to this section shall excuse any further obligation, if any, under Public Contract Code Section 20104.4 to mediate after litigation has been commenced.

**4. City's Failure to Respond**. Failure by the City to respond to a Claim from the Contractor within the time periods described in this Exhibit or to otherwise meet the time requirements of this Exhibit shall result in the Claim being deemed rejected in its entirety. A Claim that is denied by reason of the City's failure to have responded to a Claim, or its failure to otherwise meet the time requirements of this Exhibit, shall not constitute an adverse finding with regard to the merits of the Claim or the responsibility or qualifications of the Contractor.

**5. Interest**. Amounts not paid in a timely manner as required by this section shall bear interest at seven (7) percent per annum.

**6. Approved Subcontractor Claims**. If an approved subcontractor or a lower tier subcontractor lacks legal standing to assert a Claim against the City because privity of contract

does not exist, the Contractor may present to the City a Claim on behalf of a subcontractor or lower tier subcontractor. A subcontractor may request in writing, either on his or her own behalf or on behalf of a lower tier subcontractor, that the Contractor present a Claim for work which was performed by the subcontractor or by a lower tier subcontractor on behalf of the subcontractor. The subcontractor requesting that the Claim be presented to the City shall furnish reasonable documentation to support the Claim. Within 45 days of receipt of this written request, the Contractor shall notify the subcontractor in writing as to whether the Contractor presented the claim to the City and, if the Contractor did not present the claim, provide the subcontractor with a statement of the reasons for not having done so.

7. **Waiver of Provisions.** A waiver of the rights granted by Public Contract Code Section 9204 is void and contrary to public policy, provided, however, that (1) upon receipt of a Claim, the parties may mutually agree to waive, in writing, mediation and proceed directly to the commencement of a civil action or binding arbitration, as applicable; and (2) the City may prescribe reasonable change order, claim, and dispute resolution procedures and requirements in addition to the provisions of Public Contract Code Section 9204, so long as the contractual provisions do not conflict with or otherwise impair the timeframes and procedures set forth in this section.

## EXHIBIT G SURVEILLANCE ORDINANCE

### Surveillance Use Policy for fixed Automated License Plate Recognition (ALPR) Technology

In accordance with Palo Alto Municipal Code Section PAMC 2.30.680(d), the Surveillance Use Policy for the Police Department's use of fixed ALPR technology is as follows:

1. Intended Purpose. The technology is used by the Palo Alto Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including but not limited to identifying stolen or wanted vehicles, stolen license plates and missing persons, suspect interdiction and stolen property recovery.
2. Authorized Uses. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy.

The following uses of the ALPR system are specifically prohibited:

- a. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
- b. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
- c. First Amendment Rights. It is a violation of this policy to use the LPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights of any person.
- d. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

3. Information Collected. A fixed ALPR system captures the date, time, location, license plate (state, partial, paper, and no plate), and vehicle characteristics (make, model, type, and color) of passing vehicles. using the Palo Alto Police Department's ALPR's system and the vendor's vehicle identification technology.
4. Safeguards. All data will be closely safeguarded and protected by both procedural and technological means. The Palo Alto Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):
  - a. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.
  - b. Persons approved to access ALPR data under this policy are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation
  - c. Such ALPR data may only be released to other authorized and verified local enforcement officials and agencies for legitimate law enforcement purposes.

- d. Every ALPR system inquiry must be documented by either the associated case number or incident number, and lawful reason for the inquiry.
- 5. Retention. The City's ALPR vendor, Flock Safety, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data centers. Flock Safety will purge the data 30 days after collection; however, this will not preclude Palo Alto Police Department from maintaining any relevant vehicle data obtained from the system after that period if it has become, or it is reasonable to believe it will become, evidence in a specific criminal investigation or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

Information gathered or collected, and records retained by Flock Safety cameras will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

- 6. Access by non-City Entities. The ALPR data may be shared only with other local law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise required by law, and as provided below:
  - a. Requests
    - i. A law enforcement agency may make a written request for specific data, including the name of the agency and the intended official law enforcement purpose for access
    - ii. The request shall be reviewed by the Chief of Police or the authorized designee and approved before access is granted
    - iii. The approved request is retained on file
    - iv. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed by the Department's custodian of records and fulfilled only as required by law.
  - b. Memoranda of Understanding
    - i. Access to searchable data by other local law enforcement agencies shall only be granted pursuant to an MOU with that specific agency
    - ii. Such MOU will provide that access will only be used for legitimate law enforcement or public safety purposes
  - c. The Chief of Police or the authorized designee will consider the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq), before approving the access to ALPR data. The Palo Alto Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement.
- 7. Compliance Procedures. The Investigative Services Captain (or other police administrator as designated by the Police Chief) shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):
  - a. Only properly trained sworn officers, crime analysts, and police staff are allowed access to the ALPR system or to collect ALPR information.
  - b. Ensuring that training requirements are completed for authorized users.
  - c. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.

- d. Ensuring that procedures are followed for system operators and to maintain records of in compliance with Civil Code § 1798.90.52.
- e. The title and name of the current designee in overseeing the ALPR operation is maintained. Continually working with the Custodian of Records on the retention and destruction of ALPR data as required.
- f. Ensuring this policy and related procedures are conspicuously posted on the Department's dedicated ALPR website.

It is the responsibility of the Investigative Services Captain (or other police administrator as designated by the Police Chief) to ensure that an audit is conducted of ALPR detection inquiries at least once during each calendar year. The Department will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding six-month period and determine if each inquiry meets the requirements established by policy. This audit shall take the form of an internal Department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be filed and retained by the Department.

## EXHIBIT H

### INFORMATION PRIVACY POLICY

DocuSign Envelope ID: 87E1232D-F46E-405A-95CD-91CC38106A93

POLICY AND PROCEDURES 1-64/IT

Revised: December 2017



#### INFORMATION PRIVACY POLICY

##### POLICY STATEMENT

The City of Palo Alto (the "City") strives to promote and sustain a superior quality of life for persons in Palo Alto. In promoting the quality of life of these persons, it is the policy of the City, consistent with the provisions of the California Public Records Act, California Government Code §§ 6250 – 6270, to take appropriate measures to safeguard the security and privacy of the personal (including, without limitation, financial) information of persons, collected in the ordinary course and scope of conducting the City's business as a local government agency. These measures are generally observed by federal, state and local authorities and reflected in federal and California laws, the City's rules and regulations, and industry best practices, including, without limitation, the provisions of California Civil Code §§ 1798.3(a), 1798.24, 1798.79.8(b), 1798.80(e), 1798.81.5, 1798.82(e), 1798.83(e)(7), and 1798.92(c). Though some of these provisions do not apply to local government agencies like the City, the City will conduct business in a manner which promotes the privacy of personal information, as reflected in federal and California laws. The objective of this Policy is to describe the City's data security goals and objectives, to ensure the ongoing protection of the Personal Information, Personally Identifiable Information, Protected Critical Infrastructure Information and Personally Identifying Information of persons doing business with the City and receiving services from the City or a third party under contract to the City to provide services. The terms "Personal Information," "Protected Critical Infrastructure Information", "Personally Identifiable Information" and "Personally Identifying Information" (collectively, the "Information") are defined in the California Civil Code sections, referred to above, and are incorporated in this Policy by reference.

##### PURPOSE

The City, acting in its governmental and proprietary capacities, collects the Information pertaining to persons who do business with or receive services from the City. The Information is collected by a variety of means, including, without limitation, from persons applying to receive services provided by the City, persons accessing the City's website, and persons who access other information portals maintained by the City's staff and/or authorized third-party contractors. The City is committed to protecting the privacy and security of the Information collected by the City. The City acknowledges federal and California laws, policies, rules, regulations and procedures, and industry best practices are dedicated to ensuring the Information is collected, stored and utilized in compliance with applicable laws.

## **POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

The goals and objectives of the Policy are: (a) a safe, productive, and inoffensive work environment for all users having access to the City's applications and databases; (b) the appropriate maintenance and security of database information assets owned by, or entrusted to, the City; (c) the controlled access and security of the Information provided to the City's staff and third party contractors; and (d) faithful compliance with legal and regulatory requirements.

### **SCOPE**

The Policy will guide the City's staff and, indirectly, third party contractors, which are by contract required to protect the confidentiality and privacy of the Information of the persons whose personal information data are intended to be covered by the Policy and which will be advised by City staff to conform their performances to the Policy should they enjoy conditional access to that information.

### **CONSEQUENCES**

The City's employees shall comply with the Policy in the execution of their official duties to the extent their work implicates access to the Information referred to in this Policy. A failure to comply may result in employment and/or legal consequences.

### **EXCEPTIONS**

In the event that a City employee cannot fully comply with one or more element(s) described in this Policy, the employee may request an exception by submitting Security Exception Request. The exception request will be reviewed and administered by the City's Information Security Manager (the "ISM"). The employee, with the approval of his or her supervisor, will provide any additional information as may be requested by the ISM. The ISM will conduct a risk assessment of the requested exception in accordance with guidelines approved by the City's Chief Information Officer ("CIO") and approved as to form by the City Attorney. The Policy's guidelines will include at a minimum: purpose, source, collection, storage, access, retention, usage, and protection of the Information identified in the request. The ISM will consult with the CIO to approve or deny the exception request. After due consideration is given to the request, the exception request disposition will be communicated, in writing, to the City employee and his or her supervisor. The approval of any request may be subject to countermeasures established by the CIO, acting by the ISM.

### **MUNICIPAL ORDINANCE**

This Policy will supersede any City policy, rule, regulation or procedure regarding information privacy.

### **RESPONSIBILITIES OF CITY STAFF**

## **POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

### **A. RESPONSIBILITY OF CIO AND ISM**

The CIO, acting by the ISM, will establish an information security management framework to initiate and coordinate the implementation of information security measures by the City's government.

The City's employees, in particular, software application users and database users, and, indirectly, third party contractors under contract to the City to provide services, shall be guided by this Policy in the performance of their job responsibilities.

The ISM will be responsible for: (a) developing and updating the Policy; (b) enforcing compliance with and the effectiveness of the Policy; (c) the development of privacy standards that will manifest the Policy in detailed, auditable technical requirements, which will be designed and maintained by the persons responsible for the City's IT environments; (d) assisting the City's staff in evaluating security and privacy incidents that arise in regard to potential violations of the Policy; (e) reviewing and approving department-specific policies and procedures which fall under the purview of this Policy; and (f) reviewing Non-Disclosure Agreements (NDAs) signed by third party contractors, which will provide services, including, without limitation, local or 'cloud-based' software services to the City.

### **B. RESPONSIBILITY OF INFORMATION SECURITY STEERING COMMITTEE**

The Information Security Steering Committee (the "ISSC"), which is comprised of the City's employees, drawn from the various City departments, will provide the primary direction, prioritization and approval for all information security efforts, including key information security and privacy risks, programs, initiatives and activities. The ISSC will provide input to the information security and privacy strategic planning processes to ensure that information security risks are adequately considered, assessed and addressed at the appropriate City department level.

### **C. RESPONSIBILITY OF USERS**

All authorized users of the Information will be responsible for complying with information privacy processes and technologies within the scope of responsibility of each user.

### **D. RESPONSIBILITY OF INFORMATION TECHNOLOGY (IT) MANAGERS**

The City's IT Managers, who are responsible for internal, external, direct and indirect connections to the City's networks, will be responsible for configuring, maintaining and securing the City's IT networks in compliance with the City's information security and privacy policies. They are also responsible for timely internal reporting of events that may have compromised network, system or data security.



**POLICY AND PROCEDURES 1-64/IT**  
Revised: December 2017

**E. RESPONSIBILITY OF AUTHORIZATION COORDINATION**

The ISM will ensure that the City's employees secure the execution of Non-Disclosure Agreements (NDA), whenever access to the Information will be granted to third party contractors, in conjunction with the Software as a Service (SaaS) Security and Privacy Terms and Conditions. An NDA must be executed prior to the sharing of the Information of persons covered by this Policy with third party contractors. The City's approach to managing information security and its implementation (i.e. objectives, policies, processes, and procedures for information security) will be reviewed independently by the ISM at planned intervals, or whenever significant changes to security implementation have occurred.

The CIO, acting by the ISM, will review and recommend changes to the Policy annually, or as appropriate, commencing from the date of its adoption.

**GENERAL PROCEDURE FOR INFORMATION PRIVACY**

**A. OVERVIEW**

The Policy applies to activities that involve the use of the City's information assets, namely, the Information of persons doing business with the City or receiving services from the City, which are owned by, or entrusted to, the City and will be made available to the City's employees and third party contractors under contract to the City to provide Software as a Service consulting services. These activities include, without limitation, accessing the Internet, using e-mail, accessing the City's intranet or other networks, systems, or devices.

The term "information assets" also includes the personal information of the City's employees and any other related organizations while those assets are under the City's control. Security measures will be designed, implemented, and maintained to ensure that only authorized persons will enjoy access to the information assets. The City's staff will act to protect its information assets from theft, damage, loss, compromise, and inappropriate disclosure or alteration. The City will plan, design, implement and maintain information management systems, networks and processes in order to assure the appropriate confidentiality, integrity, and availability of its information assets to the City's employees and authorized third parties.

**B. PERSONAL INFORMATION AND CHOICE**

Except as permitted or provided by applicable laws, the City will not share the Information of any person doing business with the City, or receiving services from the City, in violation of this Policy, unless that person has consented to the City's sharing of such information during the conduct of the City's business as a local government agency with third parties under contract to the City to provide services.

**POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

**C. METHODS OF COLLECTION OF PERSONAL INFORMATION**

The City may gather the Information from a variety of sources and resources, provided that the collection of such information is both necessary and appropriate in order for the City to conduct business as a local government agency in its governmental and proprietary capacities. That information may be gathered at service windows and contact centers as well as at web sites, by mobile applications, and with other technologies, wherever the City may interact with persons who need to share such formation in order to secure the City's services.

The City's staff will inform the persons whose Information are covered by this Policy that the City's web site may use "cookies" to customize the browsing experience with the City of Palo Alto web site. The City will note that a cookie contains unique information that a web site can use to track, among others, the Internet Protocol address of the computer used to access the City's web sites, the identification of the browser software and operating systems used, the date and time a user accessed the site, and the Internet address of the website from which the user linked to the City's web sites. Cookies created on the user's computer by using the City's web site do not contain the Information, and thus do not compromise the user's privacy or security. Users can refuse the cookies or delete the cookie files from their computers by using any of the widely available methods. If the user chooses not to accept a cookie on his or her computer, it will not prevent or prohibit the user from gaining access to or using the City's sites.

**D. UTILITIES SERVICE**

In the provision of utility services to persons located within Palo Alto, the City of Palo Alto Utilities Department ("CPAU") will collect the Information in order to initiate and manage utility services to customers. To the extent the management of that information is not specifically addressed in the Utilities Rules and Regulations or other ordinances, rules, regulations or procedures, this Policy will apply; provided, however, any such Rules and Regulations must conform to this Policy, unless otherwise directed or approved by the Council. This includes the sharing of CPAU-collected Information with other City departments except as may be required by law.

Businesses and residents with standard utility meters and/or having non-metered monthly services will have secure access through a CPAU website to their Information, including, without limitation, their monthly utility usage and billing data. In addition to their regular monthly utilities billing, businesses and residents with non-standard or experimental electric, water or natural gas meters may have their usage and/or billing data provided to them through non-City electronic portals at different intervals than with the standard monthly billing.

**POLICY AND PROCEDURES 1-64/IT**  
Revised: December 2017

Businesses and residents with such non-standard or experimental metering will have their Information covered by the same privacy protections and personal information exchange rules applicable to Information under applicable federal and California laws.

**E. PUBLIC DISCLOSURE**

The Information that is collected by the City in the ordinary course and scope of conducting its business could be incorporated in a public record that may be subject to inspection and copying by the public, unless such information is exempt from disclosure to the public by California law.

**F. ACCESS TO PERSONAL INFORMATION**

The City will take reasonable steps to verify a person's identity before the City will grant anyone online access to that person's Information. Each City department that collects Information will afford access to affected persons who can review and update that information at reasonable times.

**G. SECURITY, CONFIDENTIALITY AND NON-DISCLOSURE**

Except as otherwise provided by applicable law or this Policy, the City will treat the Information of persons covered by this Policy as confidential and will not disclose it, or permit it to be disclosed, to third parties without the express written consent of the person affected. The City will develop and maintain reasonable controls that are designed to protect the confidentiality and security of the Information of persons covered by this Policy.

The City may authorize the City's employee and or third party contractors to access and/or use the Information of persons who do business with the City or receive services from the City. In those instances, the City will require the City's employee and/or the third party contractors to agree to use such Information only in furtherance of City-related business and in accordance with the Policy.

If the City becomes aware of a breach, or has reasonable grounds to believe that a security breach has occurred, with respect to the Information of a person, the City will notify the affected person of such breach in accordance with applicable laws. The notice of breach will include the date(s) or estimated date(s) of the known or suspected breach, the nature of the Information that is the subject of the breach, and the proposed action to be taken or the responsive action taken by the City.

**H. DATA RETENTION / INFORMATION RETENTION**

**POLICY AND PROCEDURES 1-64/IT**

Revised: December 2017

The City will store and secure all Information for a period of time as may be required by law, or if no period is established by law, for seven (7) years, and thereafter such information will be scheduled for destruction.

**I. SOFTWARE AS A SERVICE (SAAS) OVERSIGHT**

The City may engage third party contractors and vendors to provide software application and database services, commonly known as Software-as-a-Service (SaaS).

In order to assure the privacy and security of the Information of those who do business with the City and those who received services from the City, as a condition of selling goods and/or services to the City, the SaaS services provider and its subcontractors, if any, including any IT infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, while it performs such services and/or furnishes goods to the City, to the extent any scope of work or services implicates the confidentiality and privacy of the Information.

These requirements include information security directives pertaining to: (a) the IT infrastructure, by which the services are provided to the City, including connection to the City's IT systems; (b) the SaaS services provider's operations and maintenance processes needed to support the IT environment, including disaster recovery and business continuity planning; and (c) the IT infrastructure performance monitoring services to ensure a secure and reliable environment and service availability to the City. The term "IT infrastructure" refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

Prior to entering into an agreement to provide services to the City, the City's staff will require the SaaS services provider to complete and submit an Information Security and Privacy Questionnaire. In the event that the SaaS services provider reasonably determines that it cannot fulfill the information security requirements during the course of providing services, the City will require the SaaS services provider to promptly inform the ISM.

**J. FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003**

CPAU will require utility customers to provide their Information in order for the City to initiate and manage utility services to them.

Federal regulations, implementing the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108-159), including the Red Flag Rules, require that CPAU, as a "covered financial institution or creditor" which provides services in advance of payment and which can affect consumer credit, develop and implement procedures for an identity theft program for new and existing accounts to detect, prevent, respond and mitigate potential identity theft of its customers' Information.

**POLICY AND PROCEDURES 1-64/IT**  
Revised: December 2017

CPAU procedures for potential identity theft will be reviewed independently by the ISM annually or whenever significant changes to security implementation have occurred. The ISM will recommend changes to CPAU identity theft procedures, or as appropriate, so as to conform to this Policy.

There are California laws which are applicable to identity theft; they are set forth in California Civil Code § 1798.92.

NOTE: Questions regarding this policy should be referred to the Information Technology Department, as appropriate.

Recommended:	<div>DocuSigned by: <i>Jonathan Richenthal</i> 7914D9887578424...</div>	12/5/2017
	Director Information Technology/CIO	Date
Approved:	<div>DocuSigned by: <i>J. L. J. Jr.</i> 39E7298F92064D8...</div>	12/13/2017
	City Manager	Date

## EXHIBIT I

### CYBERSECURITY TERMS AND CONDITIONS

In order to assure the privacy and security of the personal information of the City's customers and people who do business with the City, including, without limitation, vendors, utility customers, library patrons, and other individuals and companies, who are required to share such information with the City, as a condition of receiving services from the City or selling goods and services to the City, including, without limitation, the Software as a Service services provider (the "Consultant") and its subcontractors, if any, including, without limitation, any Information Technology ("IT") infrastructure services provider, shall design, install, provide, and maintain a secure IT environment, described below, while it renders and performs the Services and furnishes goods, if any, described in the Statement of Work, Exhibit B, to the extent any scope of work implicates the confidentiality and privacy of the personal information of the City's customers. The Consultant shall fulfill the data and information security requirements (the "Requirements") set forth in Part A below.

A "secure IT environment" includes (a) the IT infrastructure, by which the Services are provided to the City, including connection to the City's IT systems; (b) the Consultant's operations and maintenance processes needed to support the environment, including disaster recovery and business continuity planning; and (c) the IT infrastructure performance monitoring services to ensure a secure and reliable environment and service availability to the City. "IT infrastructure" refers to the integrated framework, including, without limitation, data centers, computers, and database management devices, upon which digital networks operate.

In the event that, after the Effective Date, the Consultant reasonably determines that it cannot fulfill the Requirements, the Consultant shall promptly inform the City of its determination and submit, in writing, one or more alternate countermeasure options to the Requirements (the "Alternate Requirements" as set forth in Part B), which may be accepted or rejected in the reasonable satisfaction of the Information Security Manager (the "ISM").

#### **Part A. Requirements:**

The Consultant shall at all times during the term of any contract between the City and the Consultant:

- (a) Appoint or designate an employee, preferably an executive officer, as the security liaison to the City with respect to the Services to be performed under this Agreement.
- (b) Comply with the City's Information Privacy Policy:
- (c) Have adopted and implemented information security and privacy policies that are documented, are accessible to the City, and conform to ISO 27001/2 – Information Security Management Systems (ISMS) Standards. See the following:  
[http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103)  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=50297](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297)
- (d) Conduct routine data and information security compliance training of its personnel that is appropriate to their role.
- (e) Develop and maintain detailed documentation of the IT infrastructure, including software versions and patch levels.

- (f) Develop an independently verifiable process, consistent with industry standards, for performing professional and criminal background checks of its employees that (1) would permit verification of employees' personal identity and employment status, and (2) would enable the immediate denial of access to the City's confidential data and information by any of its employees who no longer would require access to that information or who are terminated.
- (g) Provide a list of IT infrastructure components in order to verify whether the Consultant has met or has failed to meet any objective terms and conditions.
- (h) Implement access accountability (identification and authentication) architecture and support role-based access control ("RBAC") and segregation of duties ("SoD") mechanisms for all personnel, systems, and Software used to provide the Services. "RBAC" refers to a computer systems security approach to restricting access only to authorized users. "SoD" is an approach that would require more than one individual to complete a security task in order to promote the detection and prevention of fraud and errors.
- (i) Assist the City in undertaking annually an assessment to assure that: (1) all elements of the Services' environment design and deployment are known to the City, and (2) it has implemented measures in accordance with industry best practices applicable to secure coding and secure IT architecture.
- (j) Provide and maintain secure intersystem communication paths that would ensure the confidentiality, integrity, and availability of the City's information.
- (k) Deploy and maintain IT system upgrades, patches and configurations conforming to current patch and/or release levels by not later than one (1) week after its date of release. Emergency security patches must be installed within 24 hours after its date of release.
- (l) Provide for the timely detection of, response to, and the reporting of security incidents, including on-going incident monitoring with logging.
- (m) Notify the City within one (1) hour of detecting a security incident that results in the unauthorized access to or the misuse of the City's confidential data and information.
- (n) Inform the City that any third party service provider(s) meet(s) all of the Requirements.
- (o) Perform security self-audits on a regular basis and not less frequently than on a quarterly basis, and provide the required summary reports of those self-audits to the ISM on the annual anniversary date or any other date agreed to by the Parties.
- (p) Accommodate, as practicable, and upon reasonable prior notice by the City, the City's performance of random site security audits at the Consultant's site(s), including the site(s) of a third-party service provider(s), as applicable. The scope of these audits will extend to the Consultant's and its third-party service provider(s)' awareness of security policies and practices, systems configurations, access authentication and authorization, and incident detection and response.
- (q) Cooperate with the City to ensure that to the extent required by applicable laws, rules and regulations, and the Confidential Information will be accessible only by the Consultant and any authorized third-party service provider's personnel.
- (r) Perform regular, reliable secured backups of all data needed to maximize the availability of the Services. Adequately encrypt the City of Palo Alto's data, during the operational process, hosted at rest, and the backup stage at the Vendors' environment (including Vendor's contracting organization's environment).
- (s) Maintain records relating to the Services for a period of three (3) years after the expiration or earlier termination of this Agreement and in a mutually agreeable storage medium. Within thirty (30) days after the effective date of expiration or earlier termination of this

Agreement, all of those records relating to the performance of the Services shall be provided to the ISM.

- (t) Maintain the Confidential Information in accordance with applicable federal, state, and local data and information privacy laws, rules, and regulations.
- (u) Encrypt the Confidential Information before delivering the same by electronic mail to the City and or any authorized recipient.
- (v) Provide Network Layer IP filtering services to allow access only from the City of Palo Alto's IP address to the Vendor environment (primarily hosted for the City of Palo Alto).
- (w) Offer a robust disaster recovery and business continuity (DR-BCP) solutions to the City for the systems and services the Vendor provides to the City.
- (x) Provide and support Single Sign-on (SSO) and Multifactor Authentication (MFA) solutions for authentication and authorization services from the "City's environment to the Vendor's environment," and Vendor's environment to the Vendor's cloud services/hosted environment." The Vendor shall allow two employees of the City to have superuser and super-admin access to the Vendor's IT environment, and a cloud-hosted IT environment belongs to the City.
- (y) Unless otherwise addressed in the Agreement, shall not hold the City liable for any direct, indirect or punitive damages whatsoever including, without limitation, damages for loss of use, data or profits, arising out of or in any way connected with the City's IT environment, including, without limitation, IT infrastructure communications.
- (z) The Vendor must provide evidence of valid cyber liability insurance policy per the **City's EXHIBIT "D" INSURANCE REQUIREMENTS.**



**EXHIBIT J**  
**FLOCK GROUP SERVICES ADDITIONAL TERMS OF SERVICE**

**FLOCK GROUP INC.**

**SERVICES AGREEMENT**

**ORDER FORM**

This Order Form together with the Terms (as defined herein) describe the relationship between Flock Group Inc. (“**Flock**”) and the customer identified below (“**Agency**”) (each of Flock and Customer, a “**Party**”). This order form (“**Order Form**”) hereby incorporates and includes the “GOVERNMENT AGENCY AGREEMENT” attached (the “**Terms**”) which describe and set forth the general legal terms governing the relationship (collectively, the “**Agreement**”). The Terms contain, among other things, warranty disclaimers, liability limitations and use limitations.

The Agreement will become effective when this Order Form is executed by both Parties (the “**Effective Date**”).

<b>Agency:</b> CA - Palo Alto Police Department	<b>Contact Name:</b> James Reifschneider
<b>Legal Entity Name:</b> City of Palo Alto	
<b>Address:</b> 275 Forest Ave Palo Alto, California 94301	<b>Phone:</b> (650) 329-2406 <b>E-Mail:</b> james.reifschneider@cityofpaloalto.org
<b>Expected Payment Method:</b> \FSExpectedPaymentMethod1\	<b>Billing Contact:</b> \FSBillingContact1\ (if different than above)

<b>Initial Term:</b> 36 months <b>Optional Renewal Term:</b> 24 months	<b>Billing Term:</b> Annual payment due Net 30 per terms and conditions <b>Billing Frequency:</b> Annual Plan - First Year Invoiced at Signing
---	---

**Professional Services and One-Time Purchases**

<b>Name</b>	<b>Price/Usage Fee</b>	<b>QTY</b>	<b>Subtotal</b>
Professional Services - Standard Implementation Fee	\$350.00	14.00	\$4,900.00

Professional Services - Advanced Implementation Fee	\$750.00	6.00	\$4,500.00
---	----------	------	------------

**Hardware and Software Products**

Annual recurring amounts over subscription term

<b>Name</b>	<b>Price/Usage Fee</b>	<b>QTY</b>	<b>Subtotal</b>
Falcon	\$2,500.00	20.00	\$50,000.00
Flock Safety Advanced Search	\$2,500.00	1.00	\$2,500.00

<b>Subscription with Installation Subtotal Year 1:</b>	\$61,900.00
<b>Annual Subscription Year 2 &amp; 3 Subtotal:</b>	\$104,000.00
<b>Subscription Term:</b>	36 Months
<b>Estimated Sales Tax:</b>	\$0.00
<b>Total Year 1 through 3 Subscription Amount:</b>	<b>\$166,900.00</b>
Additional Services for Camera & Pole Relocation/Replacement (if any):	\$ 7,500.00
<b>Maximum Subscription and Additional Services Total:</b>	<b>\$174,400.00</b>

# flock safety

## GOVERNMENT AGENCY AGREEMENT

This Government Agency Agreement (this “**Agreement**”) is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Rd NW Suite 210, Atlanta, GA 30318 (“**Flock**”) and the police department or government agency identified in the signature block this Agreement (“**Agency**”) (each a “**Party**,” and together, the “**Parties**”).

### RECITALS

**WHEREAS**, Flock offers a software and hardware situational awareness solution for automatic license plates, video and audio detection through Flock’s technology platform (the “**Flock Service**”), and upon detection, the Flock Services are capable of capturing audio, video, image, and recording data and can provide notifications to Agency upon the instructions of Non-Agency End User (as defined below) (“**Notifications**”);

**WHEREAS**, Agency desires access to the Flock Service on existing cameras, provided by Agency, or Flock provided Flock Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, including those from Non-Agency End Users of the Flock Service (where there is an investigative or bona fide lawful purpose) such as schools, neighborhood homeowners associations, businesses, and individual users;

**WHEREAS**, Flock deletes all Footage on a rolling thirty (30) day basis, excluding Wing Replay which is deleted after seven (7) days. Agency is responsible for extracting, downloading and archiving Footage from the Flock System on its own storage devices for auditing for prosecutorial/administrative purposes; and

**WHEREAS**, Flock desires to provide Agency the Flock Service and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime, bona fide investigations by police departments, and archiving for evidence gathering (“**Permitted Purpose**”).

### AGREEMENT

**NOW, THEREFORE**, Flock and Agency agree that this Agreement, and any addenda attached hereto or referenced herein, constitute the complete and exclusive statement of the Agreement of the Parties with respect to the subject matter of this Agreement, and replace and supersede all prior agreements, term sheets, purchase orders, correspondence, oral or written communications and negotiations by and between the Parties.

#### 1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

1.1 “**Advanced Search**” means the provision of Services, via the web interface using Flock’s software applications, which utilize advanced evidence delivery capabilities including convoy analysis, multi-geo search, visual search, cradlepoint integration for automatic vehicle location, and common plate analysis.

1.2 “**Agency Data**” means the data, media and content provided by Agency through the Services. For the avoidance of doubt, the Agency Data will include the Footage.

1.3 “**Agency Generated Data**” means the messages, text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, other information or materials posted, uploaded, displayed, published, distributed, transmitted, broadcasted, or otherwise made available on or submitted through the Wing Suite.

1.4. “**Agency Hardware**” means the third-party camera owned or provided by Agency and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Services.

1.5. “**Aggregated Data**” means information that relates to a group or category of individuals, from which any potential individuals’ personal identifying information has been permanently “anonymized” by commercially available standards to irreversibly alter data in such a way that a data subject (i.e., individual person or impersonal entity) can no longer be identified directly or indirectly.

1.6 “**Authorized End User(s)**” means any individual employees, agents, or contractors of Agency accessing or using the Services through the Web Interface, under the rights granted to Agency pursuant to this Agreement.

1.7 “**Deployment Plan**” means the strategic geographic mapping of the location(s) and implementation of Flock Hardware, and/or other relevant Services required under this Agreement.

1.8 “**Documentation**” means text and/or graphical documentation, whether in electronic or printed format, that describe the features, functions and operation of the Services which are provided by Flock to Agency in accordance with the terms of this Agreement.

1.9 “**Embedded Software**” means the software and/or firmware embedded or preinstalled on the Flock Hardware or Agency Hardware.

1.10 “**Falcon Flex**” means an infrastructure-free, location-flexible license plate reader camera that enables the Agency to self-install.

1.11 “**Flock Hardware**” means the Flock cameras or device, pole, clamps, solar panel, installation components, and any other physical elements that interact with the Embedded Software and the Web Interface to provide the Flock Services.

1.12 “**Flock IP**” means the Services, the Documentation, the Embedded Software, the Installation Services, and any and all intellectual property therein or otherwise provided to Agency and/or its Authorized End Users in connection with the foregoing.

1.13 “**Flock Safety Falcon™**” means an infrastructure-free license plate reader camera that utilizes Vehicle Fingerprint™ technology to capture vehicular attributes.

1.14 “**Flock Safety Raven™**” means an audio detection device that provides real-time alerting to law enforcement based on programmed audio events such as gunshots, breaking glass, and street racing.

1.15 “**Flock Safety Sparrow™**” means an infrastructure-free license plate reader camera for residential roadways that utilizes Vehicle Fingerprint™ technology to capture vehicular attributes.

1.17 “**Footage**” means still images, video, audio and other data captured by the Flock Hardware or Agency Hardware in the course of and provided via the Services.

1.18 “**Hotlist(s)**” means a digital file containing alphanumeric license plate related information pertaining to vehicles of interest, which may include stolen vehicles, stolen vehicle license plates, vehicles owned or associated with wanted or missing person(s), vehicles suspected of being involved with criminal or terrorist activities, and other legitimate law enforcement purposes. Hotlist also includes, but is not limited to, national data (i.e. NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and includes manually entered license plate information associated with crimes that have occurred in any local jurisdiction.

1.19 “**Implementation Fee(s)**” means the monetary fees associated with the Installation Services, as defined below.

1.20 “**Installation Services**” means the services provided by Flock for installation of Agency Hardware and/or Flock Hardware, including any applicable installation of Embedded Software on Agency Hardware.

1.21 “**Non-Agency End User(s)**” means any individual, entity, or derivative therefrom, authorized to use the Services through the Web Interface, under the rights granted to pursuant to the terms (or to those materially similar) of this Agreement.

1.22 “**Services**” or “**Flock Services**” means the provision, via the Web Interface, of Flock’s software applications for automatic license plate detection, alerts, audio detection, searching image records, video and sharing Footage.

1.23 “**Support Services**” means Monitoring Services, as defined in Section 2.10 below.

1.24 “**Usage Fee**” means the subscription fees to be paid by the Agency for ongoing access to Services.

1.25 “**Web Interface**” means the website(s) or application(s) through which Agency and its Authorized End Users can access the Services, in accordance with the terms of this Agreement.

1.26 “**Wing Suite**” means the Flock interface which provides real-time access to the Flock Services, location of Flock Hardware, Agency Hardware, third-party cameras, live-stream video, Wing Livestream, Wing LPR, Wing Replay, alerts and other integrations.

1.27 “**Wing Livestream**” means real-time video integration with third-party cameras via the Flock interface.

1.28 “**Wing LPR**” means software integration with third-party cameras utilizing Flock’s Vehicle Fingerprint Technology™ for license plate capture.

1.29 “**Wing Replay**” means enhanced situational awareness encompassing Footage retention, replay ability, and downloadable content from Hot Lists integrated from third-party cameras.

1.30 “**Vehicle Fingerprint™**” means the unique vehicular attributes captured through Services such as: type, make, color, state registration, missing/covered plates, bumper stickers, decals, roof racks, and bike racks.

## 2. SERVICES AND SUPPORT

**2.1 Provision of Access.** Subject to the terms of this Agreement, Flock hereby grants to Agency a non-exclusive, non-transferable right to access the features and functions of the Services via the Web Interface during the Term, solely for the Authorized End Users. The Footage will be available for Agency’s designated administrator, listed on the Order Form, and any Authorized End Users to access and download via the Web Interface for thirty (30) days. Authorized End Users will be required to sign up for an account and select a password and username (“**User ID**”). Flock will also provide Agency with the Documentation to be used in accessing and using the Services. Agency shall be responsible for all acts and omissions of Authorized End Users, and any act or omission by an Authorized End User which, if undertaken by Agency, would constitute a breach of this Agreement, shall be deemed a breach of this Agreement by Agency. Agency shall undertake reasonable efforts to make all Authorized End Users aware of the provisions of this Agreement as applicable to such Authorized End User’s use of the Services and shall cause Authorized End Users to comply with such provisions. Flock may use the services of one or more third parties to deliver any part of the Services, (such as using a third party to host the Web Interface for cloud storage or a cell phone provider for wireless cellular coverage) which makes the Services available to Agency and Authorized End Users. Warranties provided by said third party service providers are the agency’s sole and exclusive remedy and Flock’s sole and exclusive liability with regard to such third-party services, including without limitation hosting the Web Interface. Agency agrees to comply with any acceptable use policies and other terms of any third-party service provider that are provided or otherwise made available to Agency from time to time.

**2.2 Embedded Software License.** Subject to all terms of this Agreement, Flock grants Agency a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Embedded Software as installed on the Flock Hardware or Agency Hardware; in each case, solely as necessary for Agency to use the Services.

**2.3 Documentation License.** Subject to the terms of this Agreement, Flock hereby grants to Agency a non-exclusive, non-transferable right and license to use the Documentation during the

Term in connection with its use of the Services as contemplated herein, and under Section 2.5 below.

**2.4 Wing Suite License.** Subject to all terms of this Agreement, Flock grants Agency a limited, non-exclusive, non-transferable, non-sublicensable (except to the Authorized End Users), revocable right to use the Wing Suite software and interface.

## **2.5 Usage Restrictions.**

**2.5.1 Flock IP.** The permitted purpose for usage of the Flock Hardware, Agency Hardware, Documentation, Services, support, and Flock IP are solely to facilitate gathering evidence that could be used in a lawful criminal investigation by the appropriate government agency (“*Permitted Purpose*”). Agency will not, and will not permit any Authorized End Users to, (i) copy or duplicate any of the Flock IP; (ii) decompile, disassemble, reverse engineer, or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock IP is compiled or interpreted, or apply any other process or procedure to derive the source code of any software included in the Flock IP; (iii) attempt to modify, alter, tamper with or repair any of the Flock IP, or attempt to create any derivative product from any of the foregoing; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock IP; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within any of the Services or Flock IP; (vi) use the Services, support, Flock Hardware, Documentation, or the Flock IP for anything other than the Permitted Purpose; or (vii) assign, sublicense, sell, resell, lease, rent, or otherwise transfer, convey, pledge as security, or otherwise encumber, Agency’s rights under Sections 2.1, 2.2, 2.3, or 2.4.

**2.5.2. Flock Hardware.** Agency understands that all Flock Hardware is owned exclusively by Flock, and that title to any Flock Hardware does not pass to Agency upon execution of this Agreement. Except for Falcon Flex products, which are designed for self-installation, Agency is not permitted to remove, reposition, re-install, tamper with, alter, adjust or otherwise take possession or control of Flock Hardware. Notwithstanding the notice and cure period set for in Section 6.3, Agency agrees and understands that in the event Agency is found to engage in any of the restricted actions of this Section 2.5.2, all warranties herein shall be null and void, and this Agreement shall be subject to immediate termination (without opportunity to cure) for material breach by Agency.

**2.6 Retained Rights; Ownership.** As between the Parties, subject to the rights granted in this Agreement, Flock and its licensors retain all right, title and interest in and to the Flock IP and its components, and Agency acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement. Agency further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock’s sole discretion. There are no implied rights.

## **2.7 Suspension.**

**2.7.1 Service Suspension.** Notwithstanding anything to the contrary in this Agreement, Flock may temporarily suspend Agency’s and any Authorized End User’s access to any portion or all of the Flock IP or Flock Service if Flock reasonably determines that (a) there is a threat or attack on any of the Flock IP by Agency; (b) Agency’s or any Authorized End User’s use of the Flock

IP disrupts or poses a security risk to the Flock IP or any other customer or vendor of Flock; (c) Agency or any Authorized End User is/are using the Flock IP for fraudulent or illegal activities; (d) Agency has violated any term of this provision, including, but not limited to, utilizing the Services for anything other than the Permitted Purpose; or (e) any unauthorized access to Flock Services through Agency's account ("**Service Suspension**"). Agency shall not be entitled to any remedy for the Service Suspension period, including any reimbursement, tolling, or credit.

**2.7.2 Service Interruption.** Services may be interrupted in the event that: (a) Flock's provision of the Services to Agency or any Authorized End User is prohibited by applicable law; (b) any third-party services required for Services are interrupted; (c) if Flock reasonably believe Services are being used for malicious, unlawful, or otherwise unauthorized use; (d) there is a threat or attack on any of the Flock IP by a third party; or (e) scheduled or emergency maintenance ("**Service Interruption**"). Flock will make commercially reasonable efforts to provide written notice of any Service Interruption to Agency and to provide updates regarding resumption of access to Flock Services. Flock will use commercially reasonable efforts to resume providing access to the Services as soon as reasonably possible after the event giving rise to the Service Interruption is cured. Flock will have no liability for any damage, liabilities, losses (including any loss of data or profits), or any other consequences that Agency or any Authorized End User may incur as a result of a Service Interruption. To the extent that the Service Interruption is not caused by Agency's direct actions or by the actions of parties associated with the Agency, the expiration of the Term will be tolled by the duration of the Service Interruption (for any continuous suspension lasting at least one full day) prorated for the proportion of cameras on the Agency's account that have been impacted. For example, in the event of a Service Interruption lasting five (5) continuous days, Agency will receive a credit for five (5) free days at the end of the Term.

## **2.8 Installation Services.**

**2.8.1 Designated Locations.** For installation of Flock Hardware, excluding Falcon Flex products, prior to performing the physical installation of the Flock Hardware, Flock shall advise Agency on the location and positioning of the Flock Hardware for optimal license plate image capture, as conditions and location allow. Flock may consider input from Agency regarding location, position and angle of the Flock Hardware ("**Designated Location**") and collaborate with Agency to design the Deployment Plan confirming the Designated Locations. Flock shall have final discretion on location of Flock Hardware. Flock shall have no liability to Agency resulting from any poor performance, functionality or Footage resulting from or otherwise relating to the Designated Locations or delay in installation due to Agency's delay in confirming Designated Locations, in ordering and/or having the Designated Location ready for installation including having all electrical work preinstalled and permits ready, if necessary. After installation, any subsequent changes to the Deployment Plan ("**Reinstalls**") will incur a charge for Flock's then-current list price for Reinstalls, as listed in the then-current Reinstall policy (available at <https://www.flocksafety.com/reinstall-fee-schedule>) and any equipment fees. For clarity, Agency will receive prior notice and provide approval for any such fees. These changes include but are not limited to re-positioning, adjusting of the mounting, re-angling, removing foliage, replacement, changes to heights of poles, regardless of whether the need for Reinstalls related to vandalism, weather, theft, lack of criminal activity in view, and the like. Flock shall have full discretion on decision to reinstall Flock Hardware.



**2.8.2 Agency Installation Obligations.** Agency agrees to allow Flock and its agents reasonable access in and near the Designated Locations at all reasonable times upon reasonable notice for the purpose of performing the installation work. Although Flock Hardware is designed to utilize solar power, certain Designated Locations may require a reliable source of 120V or 240V AC power. In the event adequate solar power is not available, Agency is solely responsible for costs associated with providing a reliable source of 120V or 240V AC power to Flock Hardware. Flock will provide solar options to supply power at each Designated Location. If Agency refuses recommended solar options, Agency waives any reimbursement, tolling, or credit for any suspension period of Flock Services due to low solar power. Additionally, Agency is solely responsible for (i) any permits or associated costs, and managing the permitting process of installation of cameras or AC power; (ii) any federal, state, or local taxes including property, license, privilege, sales, use, excise, gross receipts, or other similar taxes which may now or hereafter become applicable to, measured by or imposed upon or with respect to the installation of the Flock Hardware, its use (excluding tax exempt entities), or (iii) any other supplementary cost for services performed in connection with installation of the Flock Hardware, including but not limited to contractor licensing, engineered drawings, rental of specialized equipment, or vehicles, third-party personnel (i.e. Traffic Control Officers, Electricians, State DOT-approved poles, etc., if necessary), such costs to be approved by the Agency (“**Agency Installation Obligations**”). In the event that a Designated Location for Flock Hardware requires permits, Flock may provide the Agency with a temporary alternate location for installation pending the permitting process. Once the required permits are obtained, Flock will relocate the Flock Hardware from the temporary alternate location to the permitted location at no additional cost. Without being obligated or taking any responsibility for the foregoing, Flock may pay and invoice related costs to Agency if Agency did not address them prior to the execution of this Agreement or a third party requires Flock to pay. Agency represents and warrants that it has, or shall lawfully obtain, all necessary right title and authority and hereby authorizes Flock to install the Flock Hardware at the Designated Locations and to make any necessary inspections or tests in connection with such installation.

**2.8.3 Flock’s Obligations.** Installation of Flock Hardware shall be installed in a workmanlike manner in accordance with Flock’s standard installation procedures, and the installation will be completed within a reasonable time from the time that the Designated Locations are confirmed. Upon removal of Flock Hardware, Flock shall restore the location to its original condition, ordinary wear and tear excepted. Following the initial installation of the Flock Hardware and any subsequent Reinstalls or maintenance operations, Flock’s obligation to perform installation work shall cease; however, for the sole purpose of validating installation, Flock will continue to monitor the performance of Flock Hardware for the length of the Term and will receive access to the Footage for a period of seven (7) business days after the initial installation for quality control and provide any necessary maintenance. Labor may be provided by Flock or a third-party. Flock is not obligated to install, reinstall, or provide physical maintenance to Agency Hardware. Notwithstanding anything to the contrary, Agency understands that Flock will not provide installation services for Falcon Flex products.

**2.8.4 Ownership of Hardware.** Flock Hardware shall remain the personal property of Flock and will be removed upon the natural expiration of this Agreement at no additional cost to Agency. Agency shall not perform any acts which would interfere with the retention of title of the Flock Hardware by Flock. Should Agency default on any payment of the Flock Services, Flock may remove Flock Hardware at Flock’s discretion. Such removal, if made by Flock, shall not be

deemed a waiver of Flock's rights to any damages Flock may sustain as a result of Agency's default and Flock shall have the right to enforce any other legal remedy or right.

**2.9 Hazardous Conditions.** Unless otherwise stated in the Agreement, Flock's price for its services under this Agreement does not contemplate work in any areas that contain hazardous materials, or other hazardous conditions, including, without limit, asbestos, lead, toxic or flammable substances. In the event any such hazardous materials are discovered in the designated locations in which Flock is to perform services under this Agreement, Flock shall have the right to cease work immediately in the area affected until such materials are removed or rendered harmless.

**2.10 Support Services.** Subject to the payment of fees, Flock shall monitor the performance and functionality of Flock Services and may, from time to time, advise Agency on changes to the Flock Services, Installation Services, or the Designated Locations which may improve the performance or functionality of the Services or may improve the quality of the Footage. The work, its timing, and the fees payable relating to such work shall be agreed by the Parties prior to any alterations to or changes of the Services or the Designated Locations ("**Monitoring Services**"). Flock will use commercially reasonable efforts to respond to requests for support. Flock will provide Agency with reasonable technical and on-site support and maintenance services ("**On-Site Services**") in-person or by email at [support@flocksafety.com](mailto:support@flocksafety.com), at no additional cost. Notwithstanding anything to the contrary, Agency is solely responsible for installation of Falcon Flex products. Agency further understands and agrees that Flock will not provide monitoring services or on-site services for Falcon Flex.

**2.11 Special Terms.** From time to time, Flock may offer certain special terms related to guarantees, service and support which are indicated in the proposal and on the Order Form and will become part of this Agreement, upon Agency's prior written consent ("**Special Terms**"). To the extent that any terms of this Agreement are inconsistent or conflict with the Special Terms, the Special Terms shall control.

**2.12 Upgrades to Platform.** Flock may, in its sole discretion, make any upgrades to system or platform that it deems necessary or useful to (i) maintain or enhance (a) the quality or delivery of Flock's products or services to its agencies, (b) the competitive strength of, or market for, Flock's products or services, (c) such platform or system's cost efficiency or performance, or (ii) to comply with applicable law. Parties understand that such upgrades are necessary from time to time and will not materially change any terms or conditions within this Agreement.

### 3. RESTRICTIONS AND RESPONSIBILITIES

**3.1 Agency Obligations.** Flock will assist Agency Authorized End Users in the creation of a User ID. Agency agrees to provide Flock with accurate, complete, and updated registration information. Agency may not select as its User ID a name that Agency does not have the right to use, or another person's name with the intent to impersonate that person. Agency may not transfer its account to anyone else without prior written permission of Flock. Agency will not share its account or password with anyone and must protect the security of its account and password. Unless otherwise stated and defined in this Agreement, Agency may not designate Authorized End Users for persons who are not officers, employees, or agents of Agency. Authorized End Users shall only use Agency-issued email addresses for the creation of their User ID. Agency is responsible for any activity associated with its account. Agency shall be

responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the Services. Agency will, at its own expense, provide assistance to Flock, including, but not limited to, by means of access to, and use of, Agency facilities, as well as by means of assistance from Agency personnel to the limited extent any of the foregoing may be reasonably necessary to enable Flock to perform its obligations hereunder, including, without limitation, any obligations with respect to Support Services or any Installation Services.

**3.2 Agency Representations and Warranties.** Agency represents, covenants, and warrants that Agency will use the Services only in compliance with this Agreement and all applicable laws and regulations, including but not limited to any laws relating to the recording or sharing of video, photo, or audio content. Although Flock has no obligation to monitor Agency's use of the Services, Flock may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of the foregoing.

#### **4. CONFIDENTIALITY; AGENCY DATA**

**4.1 Confidentiality.** To the extent allowable by applicable FOIA and state-specific Public Records Acts, each Party (the "**Receiving Party**") understands that the other Party (the "**Disclosing Party**") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "**Proprietary Information**" of the Disclosing Party). Proprietary Information of Flock includes non-public information regarding features, functionality and performance of the Services. Proprietary Information of Agency includes non-public data provided by Agency to Flock or collected by Flock via the Flock Hardware or Agency Hardware, to enable the provision of the Services, which includes but is not limited to geolocation information and environmental data collected by sensors. The Receiving Party agrees: (i) to take the same security precautions to protect against disclosure or unauthorized use of such Proprietary Information that the Party takes with its own proprietary information, but in no event will a Party apply less than reasonable precautions to protect such Proprietary Information, and (ii) not to use (except in performance of the Services or as otherwise permitted herein) or divulge to any third person any such Proprietary Information. Flock's use of the Proprietary Information may include processing the Proprietary Information to send Agency alerts, or to analyze the data collected to identify motion or other events. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. For clarity, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to: (a) comply with a legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Flock, its users, a third party, or the public as required or permitted by law, including respond to an emergency situation. Flock may store deleted Footage in order to comply with

certain legal obligations, but such retained Footage will not be retrievable without a valid court order.

**4.2 Agency Data.** As between Flock and Agency, all right, title and interest in the Agency Data, belong to and are retained solely by Agency. Agency hereby grants to Flock a limited, non-exclusive, royalty-free, worldwide license to (i) use the Agency Data and perform all acts with respect to the Agency Data as may be necessary for Flock to provide the Flock Services to Agency, including without limitation the Support Services set forth in Section 2.10 above, and a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify, display, and distribute the Agency Data as a part of the Aggregated Data, (ii) disclose the Agency Data (both inclusive of any Footage) to enable law enforcement monitoring for elected law enforcement Hotlists as well as provide Footage search access to law enforcement for investigative purposes only, and (iii) and obtain Aggregated Data as set forth below in Section 4.5. As between Agency and Non-Agency End Users that have prescribed access of Footage to Agency, each of Agency and Non-Agency End Users will share all right, title and interest in the Non-Agency End User Data. This Agreement does not by itself make any Non-Agency End User Data the sole property or the Proprietary Information of Agency. Flock will automatically delete Footage older than thirty (30) days. Agency has a thirty (30) day window to view, save and/or transmit Footage to the relevant government agency prior to its deletion. Notwithstanding the foregoing, Flock automatically deletes Wing Replay after seven (7) days, during which time Agency may view, save and/or transmit such data to the relevant government agency prior to deletion. Flock does not own and shall not sell Agency Data.

**4.3 Agency Generated Data in Wing Suite.** Parties understand that Flock does not own any right, title, or interest to third-party video integrated into the Wing Suite. Flock may provide Agency with the opportunity to post, upload, display, publish, distribute, transmit, broadcast, or otherwise make available on or submit through the Wing Suite, messages, text, illustrations, files, images, graphics, photos, comments, sounds, music, videos, information, content, ratings, reviews, data, questions, suggestions, or other information or materials produced by Agency. Agency shall retain whatever legally cognizable right, title, and interest that Agency has in Agency Generated Data. Agency understands and acknowledges that Flock has no obligation to monitor or enforce Agency's intellectual property rights to Agency Generated Data. To the extent legally permissible, Agency grants Flock a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify, display, and distribute the Agency Generated Data for the sole purpose of providing Flock Services. Flock does not own and shall not sell Agency Generated Data.

**4.4 Feedback.** If Agency provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency hereby assigns (and will cause its agents and representatives to assign) to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

**4.5 Aggregated Data.** Flock shall have the right to collect, analyze, and anonymize Agency Data and Agency Generated Data to create Aggregated Data to use and perform the Services and related systems and technologies, including the training of machine learning algorithms. Agency hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right (during and after the Term hereof) to use and distribute such Aggregated Data to improve and enhance the

Services and for other development, diagnostic and corrective purposes, other Flock offerings, and crime prevention efforts. Parties understand that the aforementioned license is required for continuity of Services. No rights or licenses are granted except as expressly set forth herein.

Flock does not sell Aggregated Data

5. Reserved.

**6. TERM AND TERMINATION.**

**6.1 Term.** The initial term of this Agreement shall be for the period of time set forth on the Order Form and shall commence at the time outlined in this section below (the “**Term**”).

Following the Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a “**Renewal Term**”) unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.

- a. For Wing Suite products: the Term shall commence upon execution of this Agreement and continue for one (1) year, after which, the Term may be extended by mutual consent of the Parties, unless terminated by either Party.
- b. For Falcon and Sparrow products: the Term shall commence upon first installation and validation of Flock Hardware.
- c. For Raven products: the Term shall commence upon first installation and validation of Flock Hardware.
- d. For Falcon Flex products: the Term shall commence upon execution of this Agreement.
- e. For Advanced Search products: the Term shall commence upon execution of this Agreement.

**6.2 Termination for Convenience.** At any time during the agreed upon Term, either Party may terminate this Agreement for convenience. Termination for convenience of the Agreement by the Agency will be effective immediately. Termination for convenience by Agency will result in a one-time removal fee of \$500 per Flock Hardware. Termination for convenience by Flock will not result in any removal fees. Upon termination for convenience, a refund will be provided for Flock Hardware, prorated for any fees for the remaining Term length set forth previously. Wing Suite products and Advanced Search are not subject to refund for early termination. Flock will provide advanced written notice and remove all Flock Hardware at Flock’s own convenience, within a commercially reasonable period of time upon termination. Agency’s termination of this Agreement for Flock’s material breach of this Agreement shall not be considered a termination for convenience for the purposes of this Section 6.2.

**6.3 Termination.** Notwithstanding the termination provisions in Section 2.5.2, in the event of any material breach of this Agreement, the non-breaching Party may terminate this Agreement prior to the end of the Term by giving thirty (30) days prior written notice to the breaching Party; provided, however, that this Agreement will not terminate if the breaching Party has cured the breach prior to the expiration of such thirty (30) day period. Either Party may terminate this Agreement, without notice, (i) upon the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other Party's making an assignment for the benefit of creditors, or (iii) upon the other Party's dissolution or ceasing to do business. Upon termination for Flock’s material breach, Flock will refund to Agency a pro-rata portion of the pre-paid fees for Services not received due to such termination.

**6.4 No-Fee Term.** Flock will provide Agency with complimentary access to Hotlist alerts, as further described in Section 4.2 (“*No-Fee Term*”). In the event a Non-Agency End User grants Agency access to Footage and/or notifications from a Non-Agency End User, Agency will have access to Non-Agency End User Footage and/or notifications until deletion, subject to a thirty (30) day retention policy for all products except Wing Replay, which is subject to a seven (7) day retention policy. Flock may, in their sole discretion, provide access or immediately terminate the No-Fee Term. The No-Fee Term will survive the Term of this Agreement. Flock, in its sole discretion, can determine to impose a price per No-Fee Term upon thirty (30) days’ notice to Agency. Agency may terminate any No-Fee Term or access to future No-Fee Terms upon thirty (30) days’ notice.

**6.5 Survival.** The following Sections will survive termination: 2.5, 2.6, 3, 4, 5, 6.4, 7.3, 7.4, 8.1, 8.2, 8.3, 8.4, 9.1 and 9.6.

## **7. REMEDY; WARRANTY AND DISCLAIMER**

**7.1 Remedy.** Upon a malfunction or failure of Flock Hardware or Embedded Software (a “*Defect*”), Agency must notify Flock’s technical support as described in Section 2.10 above. If Flock is unable to correct the Defect, Flock shall, or shall instruct one of its contractors to repair or replace the Flock Hardware or Embedded Software suffering from the Defect. Flock reserves the right in their sole discretion to refuse or delay replacement or its choice of remedy for a Defect until after it has inspected and tested the affected Flock Hardware provided that such inspection and test shall occur within a commercially reasonable time, but no longer than seven (7) business days after Agency notifies the Flock of a known Defect. In the event of a Defect, Flock will repair or replace the defective Flock Hardware at no additional cost to Agency. Absent a Defect, in the event that Flock Hardware is lost, stolen, or damaged, Agency may request that Flock replace the Flock Hardware at a fee according to the then-current Reinstall policy (<https://www.flocksafety.com/reinstall-fee-schedule>). Agency shall not be required to replace subsequently lost, damaged or stolen Flock Hardware, however, Agency understands and agrees that functionality, including Footage, will be materially affected due to such subsequently lost, damaged or stolen Flock Hardware and that Flock will have no liability to Agency regarding such affected functionality nor shall the Usage Fee or Implementation Fees owed be impacted. Flock is under no obligation to replace or repair Flock Hardware or Agency Hardware.

**7.2 Exclusions.** Flock will not provide the remedy described in Section 7.1 if Agency has misused the Flock Hardware, Agency Hardware, or Service in any manner.

**7.3 Warranty.** Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of other causes beyond Flock’s reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

**7.4 Disclaimer.** THE REMEDY DESCRIBED IN SECTION 7.1 ABOVE IS AGENCY’S SOLE REMEDY, AND FLOCK’S SOLE LIABILITY, WITH RESPECT TO DEFECTIVE EMBEDDED SOFTWARE. FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS

TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED “AS IS” AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER OF SECTION 7.4 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 9.6.

**7.5 Insurance.** Flock will maintain commercial general liability policies with policy limits reasonably commensurate with the magnitude of Flock’s business risk. Certificates of Insurance can be provided upon request.

**7.6 Force Majeure.** Parties are not responsible or liable for any delays or failures in performance from any cause beyond their control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, acts or omissions of third-Party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, supply chain shortages of equipment or supplies, weather conditions or acts of hackers, internet service providers or any other third Party acts or omissions. Force Majeure includes the novel coronavirus Covid-19 pandemic, and the potential spread of variants, which is ongoing as of the date of the execution of this Agreement.

## **8. LIMITATION OF LIABILITY; NO FEE TERM; INDEMNITY**

**8.1 Limitation of Liability.** NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL HARDWARE AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY, INCOMPLETENESS OR CORRUPTION OF DATA OR FOOTAGE OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND FLOCK’S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE OR IDENTIFY AND/OR CORRELATE A LICENSE PLATE WITH THE FBI DATABASE; (D) FOR ANY PUBLIC DISCLOSURE OF PROPRIETARY INFORMATION MADE IN GOOD FAITH; (E) FOR CRIME PREVENTION; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY AGENCY TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY OF SECTION 8 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 9.6. NOTWITHSTANDING THE FOREGOING, THE LIMITATIONS OF LIABILITY LIMIT SET FORTH HEREIN SHALL NOT APPLY TO (1) DAMAGES CAUSED BY CONSULTANT'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, (2) CONSULTANT'S

OBLIGATIONS TO INDEMNIFY AND DEFEND CITY (3) CLAIMS OR GENERAL DAMAGES THAT FALL WITHIN THE INSURANCE COVERAGE OF THIS AGREEMENT, (4) STATUTORY DAMAGES, AND (5) WRONGFUL DEATH CAUSED BY CONSULTANT.

**8.2 Additional No-Fee Term Requirements.** IN NO EVENT SHALL FLOCK'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THE COMPLIMENTARY NO-FEE TERM AS DESCRIBED IN SECTION 6.4 EXCEED \$100, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE. Parties acknowledge and agree that the essential purpose of this Section 8.2 is to allocate the risks under the No-Fee Term described in Section 6.4 and limit potential liability given the aforementioned complimentary service, which would have been substantially higher if Flock were to assume any further liability other than as set forth herein. Flock has relied on these limitations in determining whether to provide the complementary No-Fee Term. The limitations set forth in this Section 8.2 shall not apply to claims or damages resulting from Flock's other obligations under this Agreement.

**8.3 Responsibility.** Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, deputies, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable (if at all) only for the torts of its own officers, agents, or employees.

## **9. Reserved.**

## **10. MISCELLANEOUS**

**10.1 Compliance With Laws.** The Agency agrees to comply with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules, including responding to any subpoena request(s). In the event Flock is legally compelled to comply with a judicial order, subpoena, or government mandate, to disclose Agency Data or Agency Generated Data, Flock will provide Agency with notice.

**10.2 Severability.** If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect.

**10.3 Assignment.** This Agreement is not assignable, transferable or sublicensable by either Party, without prior consent. Notwithstanding the foregoing, either Party may assign this Agreement, without the other Party's consent, (i) to any parent, subsidiary, or affiliate entity, or (ii) to any purchaser of all or substantially all of such Party's assets or to any successor by way of merger, consolidation or similar transaction

**10.4 Entire Agreement.** This Agreement, together with the Order Form(s), the then-current Reinstall policy (<https://www.flocksafety.com/reinstall-fee-schedule>), Deployment Plan(s), and any attached addenda are the complete and exclusive statement of the mutual understanding of the Parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both



Parties, except as otherwise provided herein. None of Agency's purchase orders, authorizations or similar documents will alter the terms of this Agreement, and any such conflicting terms are expressly rejected. In the event of any conflict of terms found in this Agreement or any other terms and conditions, the terms of this Agreement shall prevail.

- 10.5 Relationship.** No agency, partnership, joint venture, or employment is created as a result of this Agreement and Agency does not have any authority of any kind to bind Flock in any respect whatsoever. Flock shall at all times be and act as an independent contractor.
- 10.6 Governing Law; Venue.** This Agreement shall be governed by the laws of the State in which the Agency is located. The Parties hereto agree that venue would be proper in the chosen courts of the State of which the Agency is located. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this Agreement.
- 10.7 Publicity.** Upon prior consent from Agency, Flock has the right to reference and use Agency's name and trademarks and disclose the nature of the Services provided hereunder in each case in business and development and marketing efforts, including without limitation on Flock's website.
- 10.8 Export.** Agency may not remove or export from the United States or allow the export or re-export of the Flock IP or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority. As defined in Federal Acquisition Regulation ("FAR"), section 2.101, the Services, the Flock Hardware and Documentation are "commercial items" and according to the Department of Defense Federal Acquisition Regulation ("DFAR") section 252.2277014(a)(1) and are deemed to be "commercial computer software" and "commercial computer software documentation." Flock is compliant with FAR Section 889 and does not contract or do business with, use any equipment, system, or service that uses the enumerated banned Chinese telecommunication companies, equipment or services as a substantial or essential component of any system, or as critical technology as part of any Flock system. Consistent with DFAR section 227.7202 and FAR section 12.212, any use, modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.
- 10.9 Headings.** The headings are merely for organization and should not be construed as adding meaning to the Agreement or interpreting the associated sections.
- 10.10 Authority.** Each of the below signers of this Agreement represent that they understand this Agreement and have the authority to sign on behalf of and bind the Parties they are representing.

## **Surveillance Use Policy for fixed Automated License Plate Recognition (ALPR) Technology**

In accordance with Palo Alto Municipal Code Section PAMC 2.30.680(d), the Surveillance Use Policy for the Police Department's use of fixed ALPR technology is as follows:

1. **Intended Purpose.** The technology is used by the Palo Alto Police Department to convert data associated with vehicle license plates and vehicle descriptions for official law enforcement purposes, including but not limited to identifying stolen or wanted vehicles, stolen license plates and missing persons, suspect interdiction and stolen property recovery.
2. **Authorized Uses.** Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy.

The following uses of the ALPR system are specifically prohibited:

- a. Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.
  - b. Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.
  - c. First Amendment Rights. It is a violation of this policy to use the LPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights of any person.
  - d. Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).
3. **Information Collected.** A fixed ALPR system captures the date, time, location, license plate (state, partial, paper, and no plate), and vehicle characteristics (make, model, type, and color) of passing vehicles. using the Palo Alto Police Department's ALPR's system and the vendor's vehicle identification technology.
  4. **Safeguards.** All data will be closely safeguarded and protected by both procedural and technological means. The Palo Alto Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):
    - a. All ALPR data shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

- b. Persons approved to access ALPR data under this policy are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation
  - c. Such ALPR data may only be released to other authorized and verified local enforcement officials and agencies for legitimate law enforcement purposes.
  - d. Every ALPR system inquiry must be documented by either the associated case number or incident number, and lawful reason for the inquiry.
5. **Retention.** The City's ALPR vendor, Flock Safety, will store the data (data hosting) and ensure proper maintenance and security of data stored in their data centers. Flock Safety will purge the data 30 days after collection; however, this will not preclude Palo Alto Police Department from maintaining any relevant vehicle data obtained from the system after that period if it has become, or it is reasonable to believe it will become, evidence in a specific criminal investigation or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

Information gathered or collected, and records retained by Flock Safety cameras will not be sold, accessed, or used for any purpose other than legitimate law enforcement or public safety purposes.

6. **Access by non-City Entities.** The ALPR data may be shared only with other local law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise required by law, and as provided below:
- a. Requests
    - i. A law enforcement agency may make a written request for specific data, including the name of the agency and the intended official law enforcement purpose for access
    - ii. The request shall be reviewed by the Chief of Police or the authorized designee and approved before access is granted
    - iii. The approved request is retained on file
    - iv. Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed by the Department's custodian of records and fulfilled only as required by law.
  - b. Memorandum of Understanding
    - i. Access to searchable data by other local law enforcement agencies shall only be granted pursuant to an MOU with that specific agency
    - ii. Such MOU will provide that access will only be used for legitimate law enforcement or public safety purposes
  - c. The Chief of Police or the authorized designee will consider the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq), before approving the access to ALPR data. The Palo Alto Police Department does not permit the sharing of ALPR data gathered by the City or its contractors/subcontractors for purpose of federal immigration enforcement.

7. **Compliance Procedures.** The Investigative Services Captain (or other police administrator as designated by the Police Chief) shall be responsible for compliance with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):
- a. Only properly trained sworn officers, crime analysts, and police staff are allowed access to the ALPR system or to collect ALPR information.
  - b. Ensuring that training requirements are completed for authorized users.
  - c. ALPR system monitoring to ensure the security of the information and compliance with applicable privacy laws.
  - d. Ensuring that procedures are followed for system operators and to maintain records of in compliance with Civil Code § 1798.90.52.
  - e. The title and name of the current designee in overseeing the ALPR operation is maintained. Continually working with the Custodian of Records on the retention and destruction of ALPR data as required.
  - f. Ensuring this policy and related procedures are conspicuously posted on the Department's dedicated ALPR website.

It is the responsibility of the Investigative Services Captain (or other police administrator as designated by the Police Chief) to ensure that an audit is conducted of ALPR detection inquiries at least once during each calendar year. The Department will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. The audit shall randomly select at least 10 detection browsing inquiries conducted by department employees during the preceding six-month period and determine if each inquiry meets the requirements established by policy. This audit shall take the form of an internal Department memorandum to the Chief of Police. The memorandum shall include any data errors found so that such errors can be corrected. After review by the Chief of Police, the memorandum and any associated documentation shall be filed and retained by the Department.



# MAKING SMART DECISIONS ABOUT SURVEILLANCE

A GUIDE FOR COMMUNITY  
TRANSPARENCY,  
ACCOUNTABILITY  
& OVERSIGHT

THE ACLU  
OF CALIFORNIA  
APRIL 2016

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

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

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

We hope you will find this document and its supporting materials (available online at [aclunc.org/smartabouts-surveillance](https://aclunc.org/smartabouts-surveillance)) useful in ensuring your community is making informed decisions about surveillance.



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



Peter Bibring  
Police Practices Director  
ACLU of California

## CONTENTS

<b>Technology Overview</b> .....	2
<b>Key Questions to Answer Before Moving Forward with Any Surveillance Proposal</b> .....	3
<b>Why It Matters: The Costs and Consequences of Surveillance</b> .....	4
Surveillance Impacts Civil Rights and Community Trust .....	4
Surveillance Carries Both Immediate and Ongoing Financial Costs .....	7
Surveillance Must Take Evolving Privacy Law into Account .....	8
<b>Necessary Steps when Considering a Surveillance Proposal</b> .....	11
Collectively Evaluate the Effectiveness, Costs and Alternatives Before Making Decisions about Surveillance .....	11
Establish a Surveillance Use Policy to Mitigate Harms and Protect Rights .....	17
Ensure Accountability by Enforcing Policies and Encouraging Ongoing Public Engagement .....	21
<b>Conclusion</b> .....	24
<b>Appendix: Model Surveillance &amp; Community Safety Ordinance</b> .....	25
<b>Endnotes</b> .....	29

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

**Contributing Writers:** Addison Litton and Thomas Mann Miller

**Design & Layout:** Gigi Pandian & Daniela Bernstein

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

**PUBLISHED BY THE ACLU OF CALIFORNIA  
SECOND EDITION — APRIL 2016**



# TECHNOLOGY OVERVIEW

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

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

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

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

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

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

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

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

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



# KEY QUESTIONS TO ANSWER BEFORE MOVING FORWARD WITH ANY SURVEILLANCE PROPOSAL

## WHY ARE YOU CONSIDERING SURVEILLANCE?

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

## WHAT ARE THE COSTS AND RISKS?

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

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

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

## IS SURVEILLANCE THE RIGHT CHOICE?

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

## WILL THESE QUESTIONS BE ANSWERED EVERY TIME?

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

## Why It Matters: The Costs and Consequences of Surveillance

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

### A. SURVEILLANCE IMPACTS CIVIL RIGHTS AND COMMUNITY TRUST

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

“[S]urveillance programs follow a long history of law enforcement targeting African American and other minority groups.... We need ... a future in the city where our police department and other public institutions have true community oversight and accountability.”

The Rev. B.T. Lewis and Taymah Jahsi, Organizers, Faith in Community in Fresno<sup>2</sup>

#### 1. SURVEILLANCE CAN INTRUDE UPON COMMUNITY MEMBERS' RIGHTS

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

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

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

study showed that “the young, the male and the black were systematically and disproportionately targeted not because of their involvement in crime or disorder, but for ‘no obvious reason.’”<sup>8</sup>

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

### SURVEILLANCE OF POLITICAL AND SOCIAL ACTIVISTS

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

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

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

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

“One of the most alarming parts of that history has been the ways that surveillance has been misused against Black people who have been advocating for their justice. It’s been used to discredit, abuse, and incarcerate.”

Opal Tometi, Black Lives Matter co-founder<sup>17</sup>

Surveillance carries privacy and free speech threats even if it is conducted solely in public places. This is particularly true when surveillance information is aggregated to build a robust data profile that can “reveal

“Those of us from marginalized communities grew up in environments very much shaped by surveillance, which has been utilized to ramp up the criminal justice system and increase deportations....”

Steven Renderos, Center for Media Justice<sup>18</sup>

much more in combination than any isolated record.”<sup>19</sup> As Supreme Court Justice Sonia Sotomayor has noted, “a precise, comprehensive record of a person’s public movements ... reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” In addition, “[a]wareness that the Government may be watching chills associational and expressive freedoms.”<sup>20</sup>

## 2. SURVEILLANCE CAN ERODE TRUST IN LAW ENFORCEMENT

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

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

“The effects of surveillance on New York Muslim communities have been devastating.... Community members’ ties to local police precincts have deteriorated due to distrust and fear.”

Hina Shamsi, ACLU National Security Project Director<sup>22</sup>

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



## B. SURVEILLANCE CARRIES BOTH IMMEDIATE AND ONGOING FINANCIAL COSTS

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

### 1. SURVEILLANCE REQUIRES INFRASTRUCTURE, STAFFING, TRAINING, AND MAINTENANCE

The hidden costs of infrastructure, training and staffing, operations and maintenance, and the potential for budget overruns, can dwarf the cost of acquiring surveillance technology in the first place. Communities that have failed to accurately estimate the full financial cost of a surveillance system have dealt with massive cost overruns and programs that failed to accomplish their stated purpose. For example, Philadelphia planned to

“When you’re considering a new technology, it’s important to evaluate not only the upfront costs but also the costs of maintenance and upgrades that will occur down the road.”

Captain Michael Grinstead, Newport News (VA) Police Department<sup>24</sup>

spend \$651,672 for a video surveillance program featuring 216 cameras. Instead, it spent \$13.9 million on the project and wound up with only 102 functional cameras after a year, a result the city controller described as “exceedingly alarming, and outright excessive — especially when \$13.9 million is equivalent to the cost of putting 200 new police recruits on our streets.”<sup>25</sup> To avoid a similar incident in your community, it is essential to identify all of the costs required to install, use, and maintain surveillance technology before making a decision about whether to do so.

### 2. SURVEILLANCE CAN CREATE FINANCIAL RISKS INCLUDING LITIGATION AND DATA BREACH

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

“After public backlash about Oakland’s proposed Domain Awareness Center, we really had to regroup and think about how we needed to proceed.”

Renee Domingo, former Oakland Emergency Services Coordinator<sup>29</sup>

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

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

Failing to thoroughly discuss surveillance proposals and listen to community concerns early in the process can result in massive backlash and wasted time and funds when plans are suspended or ultimately cancelled. Oakland was forced to scrap most of the planning for its ill-fated Domain Awareness Center and scale the project back considerably after community members protested the misleading mission statement and lack of transparency for the project.<sup>32</sup> In Santa Clara County, a secretive process to purchase a Stingray cell surveillance device was derailed by the County Executive after it sidestepped necessary community debate and county oversight.<sup>33</sup>

Community members grounded San Jose's secret drone purchase and the police were forced to apologize for the lack of transparency and community input.<sup>35</sup> Engaging with the community before taking steps to go forward with a surveillance proposal is essential to avoiding similar mistakes that spark widespread community outrage and waste time and resources.

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

San Jose Police Department<sup>34</sup>

### C. SURVEILLANCE MUST TAKE EVOLVING PRIVACY LAW INTO ACCOUNT

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

In recent years, federal courts have repeatedly reinforced legal protections for individual rights in the context of today's technology. In 2015, the U.S. Supreme Court unanimously told law enforcement to "get a warrant" to search an arrestee's cell phone. In another unanimous decision, the Court also ruled a warrant is required

"The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."

*Riley v. California*, U.S. Supreme Court<sup>36</sup>

to use a GPS beeper to track a suspect's vehicle, with a majority of the Court suggesting that using technology to track an individual's location — even in public — over an extended period of time triggers constitutional scrutiny.<sup>37</sup> Finally, multiple federal courts declared the NSA's warrantless collection of telephone metadata unlawful, with one criticizing its "almost Orwellian" scope.<sup>38</sup> Surveillance programs that fail to account for this trend may well be held unconstitutional, and criminal investigations based on evidence from those programs could be jeopardized.

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

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

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

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

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

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

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

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

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

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

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

“With a surveillance equipment ordinance, any of the existing equipment that Oakland might already have or any that is soon to come out will have to go through the vetting process.”

Brian Hofer, Chair, Oakland Domain Awareness Center Privacy Committee<sup>51</sup>

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

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



## Necessary Steps when Considering a Surveillance Proposal

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

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

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

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

#### 1. *DECIDE AS A COMMUNITY: INVOLVE THE ENTIRE COMMUNITY FROM THE START*

The best way to consider whether surveillance is the right choice and to avoid costly mistakes is to engage the entire community — including law enforcement, local lawmakers, and members of the public — in a thorough discussion about any surveillance proposal.

Different segments of your community are likely to bring valuable perspectives to the process of evaluating whether to acquire and use surveillance technology. And the time to engage with your community is at the very beginning of the process, *before* any funding is sought, technology is acquired, or system is used.

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

Fewer than 15 percent of California communities publicly debated surveillance programs before moving forward. (ACLU 2014)<sup>54</sup>

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

Joe DeVries, Oakland Assistant to the City Administrator<sup>56</sup>

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

"Technology can only serve democracy to the degree that it is democratized."

Malkia Cyril, Director, Center for Media Justice<sup>58</sup>

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

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

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

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

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

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

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

An informed debate also requires that your community have access to a wide range of information in order to assess how surveillance would work in practice and whether it would advance local goals. Community meetings with various speakers representing different perspectives (not just law enforcement and the technology vendor) can help the community understand how the surveillance technology actually works and its potential implications. The entity seeking to acquire new surveillance technology should also prepare and release a Surveillance Impact Report and a

Surveillance Use Policy to help everyone understand how a technology will work, its potential costs, and the safeguards that will prevent its misuse if the proposal were approved. Your community may also consider convening an ad-hoc committee of local residents, experts and advocates who can work together to make recommendations or help complete these documents.

"It is critical to our judicial system and our democracy that the public and our elected representatives be informed about the use of these devices so that we can have a discussion about their privacy implications and make informed decisions about policies for their use."

Joe Simitian, Santa Clara County Supervisor<sup>63</sup>

### USE A SURVEILLANCE IMPACT REPORT TO MAKE AN INFORMED DECISION

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

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

A worksheet to help your community prepare a Surveillance Impact Report is available at [aclunc.org/smartaboutsurance](http://aclunc.org/smartaboutsurance).

### CASE STUDY: SANTA CRUZ COUNCILMEMBERS LACK INFORMATION FOR ALPR DECISION

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

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

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

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

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

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

## **2. DEFINE THE PURPOSE: ASK HOW AND WHETHER THIS TECHNOLOGY WILL AID YOUR COMMUNITY**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**3. IDENTIFY THE COSTS AND RISKS: EXAMINE FINANCIAL, LEGAL, AND PRACTICAL CONSEQUENCES**

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

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

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

"One more question to ask ourselves is whether we are carefully considering the infrastructure that is needed to support technology — the costs of monitoring it and of staffing technology units at a time when departments are laying off civilians. We really need to think about all of the aspects of technology when initial investments are being made."

Police Executive Research Forum, "How Are Innovations in Technology Affecting Policing?"<sup>70</sup>

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

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

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

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

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



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

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

### **CASE STUDY: REDLANDS DEPLOYS INSECURE CAMERA NETWORK**

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

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

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

### **CASE STUDY: ALAMEDA COUNTY SOLICITS PUBLIC INPUT FOR STINGRAY POLICY**

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

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

### 1. *USE APPROPRIATELY: PLACE CLEAR LIMITS ON SURVEILLANCE*

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

#### ➤ *When is surveillance permitted or prohibited?*

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

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

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

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

The police need to “have more of a dialog with the council, because we are the ones that . . . approve funding decisions and we want to make sure . . . that you are hearing everything that we hear as well.”

Seattle Councilmember Bruce Harrell<sup>76</sup>

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

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

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

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

#### ➤ *How are officers trained before they conduct surveillance?*

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



➤ *Are you only collecting necessary data?*

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

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

### **CASE STUDY: OHIO STATE HIGHWAY PATROL RETAINS ONLY ALPR HITS**

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

## **2. PREVENT MISUSE OF DATA: LIMIT WHEN DATA CAN BE USED AND WHO CAN ACCESS IT**

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

➤ *How will surveillance data be secured?*

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

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

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

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

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

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

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

### **CASE STUDY: LAX POLICIES LEAD TO “LOVEINT” ABUSE**

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

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

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

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

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

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

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

To maximize the usefulness of your technology and minimize civil liberties concerns, a retention period should not be longer than necessary to directly advance community purposes. For instance, deploying automated license plate readers to

locate stolen or Amber Alert vehicles is not aided by the collection of historical data. Retaining data “just in case it becomes useful” increases the risk that data will be used contrary to the purpose agreed upon by the community or wind up in the hands of

a bad actor. Retaining data can also increase the costs of surveillance by requiring expensive storage solutions and making it harder to effectively use the system. Focusing on the specific objective that surveillance is intended to accomplish can help you determine a retention period that balances that objective with the costs and risks associated with data retention.

“If there’s anything of a criminal nature recorded on video, it’s grabbed and inventoried within hours. Most everything else is never looked at again, so it’s purged automatically.”

Commander Steven Caluris, Chicago Police Department<sup>83</sup>

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

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

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

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

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

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

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

## 1. IDENTIFY AND ADDRESS ABUSES: AUDIT USE OF TECHNOLOGIES AND DATA AND ADDRESS ANY MISUSE

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

### ➤ *How are operators supervised?*

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

“As stewards of the public’s interests, we know the government doesn’t get to simply say ‘trust us’ and carry on: we have to earn that trust on a daily basis. We have to be accountable and transparent...”

Former Oakland Mayor Jean Quan<sup>84</sup>

### ➤ *How will misuses of the technology be identified?*

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

## CASE STUDY: FRESNO ADOPTS ANNUAL AUDIT OF VIDEO SURVEILLANCE

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

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

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

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

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

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

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

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

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

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

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

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

## Conclusion

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

## Appendix: Model Surveillance & Community Safety Ordinance

### A. KEY PRINCIPLES OF THE MODEL ORDINANCE

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

### B. MODEL ORDINANCE TEXT

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

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

#### Section 1. Title

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

#### Section 2. [Council/Board] Approval Requirement

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

### **Section 3. Information Required**

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

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

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

### **Section 5. Compliance for Existing Surveillance Technology**

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

### **Section 6. Oversight Following [Council/Board] Approval**

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

### **Section 7. Definitions**

The following definitions apply to this Ordinance:

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



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

## **Section 8. Enforcement**

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

## **Section 9. Severability**

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

## **Section 10. Effective Date**

This Ordinance shall take effect on [DATE].

## Endnotes

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

- <sup>21</sup> Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, Huffington Post (Feb 25, 2012), [http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over\\_n\\_1298997.html](http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html); Adam Goldman & Matt Apuzzo, *New York Drops Unit That Spied on Muslims*, N.Y. Times, April 15, 2014, *available at* <http://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html>.
- <sup>22</sup> Hina Shamsi and Ramzi Kassem, *The NYPD spied on Muslim Americans. Will a court settlement change anything?*, The Guardian, Jan. 8, 2016, <http://www.theguardian.com/commentisfree/2016/jan/08/nypd-spied-muslim-americans-will-court-settlement-bring-change>.
- <sup>23</sup> Angel Jennings, Richard Winston & James Rainey, *Sheriff's Secret Air Surveillance of Compton Sparks Outrage*, L.A. Times, Apr. 23, 2014, *available at* <http://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html>.
- <sup>24</sup> *Police Executive Research Forum, How Are Innovations in Technology Transforming Policing?* 26 (Jan. 2012) [hereinafter PERF Report], *available at* [http://www.policeforum.org/assets/docs/Critical\\_Issues\\_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf](http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf).
- <sup>25</sup> Press Release, Office of the Controller, *Butkovitz Alarmed by Police Camera Program*, June 20, 2012, <http://www.philadelphiacontroller.org/page.asp?id=792>.
- <sup>26</sup> See *Fazaga v. FBI*, 844 F.Supp.2d 1022 (C.D. Cal. 2012).
- <sup>27</sup> Adam Goldman, *NYPD settles lawsuits over Muslim monitoring*, Wash. Post, Jan. 7, 2016, *available at* [https://www.washingtonpost.com/world/national-security/nypd-settles-lawsuits-over-muslim-monitoring/2016/01/07/bdc8eb98-b3dc-11e5-9388-466021d971de\\_story.html](https://www.washingtonpost.com/world/national-security/nypd-settles-lawsuits-over-muslim-monitoring/2016/01/07/bdc8eb98-b3dc-11e5-9388-466021d971de_story.html).
- <sup>28</sup> See Tim Cushing, *Another Bogus Hit from a License Plate Reader Results in Another Citizen Surrounded by Cops with Guns Out*, TechDirt (May 23, 2014), <https://www.techdirt.com/articles/20140513/07404127218/another-bogus-hit-license-plate-reader-results-another-citizen-surrounded-cops-with-guns-out.shtml>.
- <sup>29</sup> Symposium, *The Value of Privacy*, U. Cal.-Hastings School of L. Const. L. Q., Apr. 7, 2014 (oral remarks), *available at* <http://livestre.am/4P7Lk>.
- <sup>30</sup> Cal. Civil Code § 1798.29 (2014).
- <sup>31</sup> Larry Ponemon, *Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis'*, May 27, 2015, <https://securityintelligence.com/cost-of-a-data-breach-2015/>.
- <sup>32</sup> Will Kane, *Oakland to Limit Surveillance Center to Port, Airport*, S.F. Gate, Mar. 6, 2014, *available at* <http://www.sfgate.com/bayarea/article/Oakland-to-limit-surveillance-center-to-port-5290273.php>.
- <sup>33</sup> Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, <http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/>.
- <sup>34</sup> Press Release, *San Jose Police Provide Statement Regarding Purchase of Unmanned Aerial System (UAS)*, San Jose Police Dept., Aug. 5, 2014, *available at* <http://www.sjpd.org/iNews/viewPressRelease.asp?ID=1874>.
- <sup>35</sup> Robert Salonga, *San Jose: Police apologize for drone secrecy, promise transparency*, San Jose Mercury News, Aug. 5, 2014, *available at* [http://www.mercurynews.com/crime-courts/ci\\_26279254/san-jose-police-apologize-secret-drone-purchase-promise](http://www.mercurynews.com/crime-courts/ci_26279254/san-jose-police-apologize-secret-drone-purchase-promise).
- <sup>36</sup> *Riley v. California*, 573 U.S. (2014), Slip Op. at \*28.
- <sup>37</sup> *U.S. v. Jones*, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, Ginsberg, Breyer, and Kagan, J., concurring in the judgment).
- <sup>38</sup> Charlie Savage and Jonathan Wiseman, *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*, N.Y. Times, May 7, 2015, *available at* <http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html>; *Klayman v. Obama*, Civ. No. 13-0851 (D.D.C. Dec. 16, 2013).
- <sup>39</sup> Ballot Pamphlet, Proposed Amendments to Cal. Const. with Arguments to Voters, Gen. Elec. (Nov. 7, 1972).
- <sup>40</sup> *White v. Davis*, 533 P.2d (Cal. 1975).
- <sup>41</sup> *People v. Cook* 41 Cal. 3d 373 (1985).
- <sup>42</sup> *Robins v. Pruneyard Shopping Center*, 592 P.2d 899 (Cal. 1979) (holding that, under the California Constitution, members of the public have a legal right to pass out pamphlets and seek signatures in a privately owned shopping center), *aff'd*, 447 U.S. 74 (1980).
- <sup>43</sup> Cal. Penal Code §§ 1546-1546.4. See generally Tracy Seipel and Eric Kurhi, *California digital privacy laws boosted, protecting consumers from Big Brother, big business*, San Jose Mercury News, Oct. 9, 2015, *available at* [http://www.mercurynews.com/health/ci\\_28948653/california-digital-privacy-laws-boosted-protecting-consumers-from](http://www.mercurynews.com/health/ci_28948653/california-digital-privacy-laws-boosted-protecting-consumers-from).
- <sup>44</sup> Cal. Gov't Code § 53166.
- <sup>45</sup> Cal. Civil Code §§ 1798.29, 1798.82, and 1798.90.5.

- <sup>46</sup> Jennifer Steinhauer and Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. Times, Jun. 2, 2015, available at [http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html?\\_r=0](http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html?_r=0); see also U.S.A. Freedom Act, H.R. 2048, 114th Cong. (2016).
- <sup>47</sup> Allie Bohm, *Status of Location Privacy Legislation in the States*, ACLU Free Future (April 8, 2014), <https://www.aclu.org/blog/technology-and-liberty-national-security/status-location-privacy-legislation-states> (as of May 6, 2014).
- <sup>48</sup> Allie Bohm, *Status of 2014 Domestic Drone Legislation in the States*, ACLU Free Future (April 22, 2014), <https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states> (as of May 6, 2014).
- <sup>49</sup> *Smart About Surveillance*, ACLU of California, <http://www.aclunc.org/smartabouts-surveillance>.
- <sup>50</sup> *Id.*
- <sup>51</sup> Interview with Brian Hofer, *Transparency over secrecy: Oakland's surveillance policy*, KALW Local Public Radio, available at <http://kalw.org/post/transparency-over-secrecy-oakland-s-surveillance-policy#stream/0>.
- <sup>52</sup> See Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, available at [http://www.mercurynews.com/breaking-news/ci\\_25766277/menlo-park-council-approves-ordinance-regulating-police-use](http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approves-ordinance-regulating-police-use); *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), <http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/>.
- <sup>53</sup> U.S. Dep't of Homeland Security, *CCTV: Developing Best Practices* (2007), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_rpt\\_cctv\\_2007.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf).
- <sup>54</sup> *State of Surveillance in California – Findings and Recommendations*, ACLU of California, Jan. 2015, available at [https://www.aclunc.org/sites/default/files/201501-aclu\\_ca\\_surveillancetech\\_summary\\_and\\_recommendations.pdf](https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf).
- <sup>55</sup> Redlands Police Department, Citizen Privacy Council, <http://www.cityofredlands.org/police/CPC>.
- <sup>56</sup> Halima Kazen, *Watching the Watchers: Oakland Seeks Control of Law Enforcement Surveillance*, The Guardian, July 13, 2015, available at <http://www.theguardian.com/us-news/2015/jul/13/oakland-law-enforcement-surveillance>.
- <sup>57</sup> Memorandum, *Establishing Ad Hoc Committee to Review the Community Warning System and Industrial Safety Ordinance* (Sept. 18, 2012), [http://64.166.146.155/agenda\\_publish.cfm?mt=ALL&get\\_month=9&get\\_year=2012&dsp=agm&seq=12339&rev=0&ag=241&ln=23604&nseq=0&nrev=0&pseq=12303&prev=0](http://64.166.146.155/agenda_publish.cfm?mt=ALL&get_month=9&get_year=2012&dsp=agm&seq=12339&rev=0&ag=241&ln=23604&nseq=0&nrev=0&pseq=12303&prev=0).
- <sup>58</sup> Keynote address of Malkia Cyril, *Targeted Surveillance, Civil Rights, and the Fight for Democracy*, Center for Media Justice, Oct. 13, 2015, available at <http://centerformediajustice.org/2015/10/13/targeted-surveillance-civil-rights-and-the-fight-for-democracy/>.
- <sup>59</sup> See Memorandum, City Administrator's Weekly Report (Apr. 25, 2014), <http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak046804.pdf>.
- <sup>60</sup> <http://www2.oaklandnet.com/Government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm>
- <sup>61</sup> Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times, Mar. 15, 2015, available at [http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?\\_r=0](http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0); Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, <http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/>.
- <sup>62</sup> Ali Winston, *Oakland City Council Rolls Back the Domain Awareness Center*, East Bay Express (Mar. 5, 2014), <http://www.eastbayexpress.com/SevenDays/archives/2014/03/05/oakland-city-council-rolls-back-the-dac>.
- <sup>63</sup> Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, <http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/>.
- <sup>64</sup> John Malkin, *Surveillance City?* GoodTimes, Jan 29, 2014, <http://www.gtweekly.com/index.php/santacruznews/goodtimescoverstories/5386surveillancecity.html>.
- <sup>65</sup> Robert Salonga, *San Jose: Police Apologize for Drone Secrecy, Promise Transparency*, San Jose Mercury News, Aug 5, 2014, available at [http://www.mercurynews.com/crime-courts/ci\\_26279254/san-jose-police-apologize-secret-drone-purchase-promise](http://www.mercurynews.com/crime-courts/ci_26279254/san-jose-police-apologize-secret-drone-purchase-promise).
- <sup>66</sup> See Oakland City Auditor, *Police Technology Performance Audit: FY 2006–07 through 2010–11* (2012), available at <http://www.oaklandauditor.com/images/oakland/auditreports/0pd%20tech.pdf>.
- <sup>67</sup> See Citris, *Citris Study on SF Public Cameras Released* (Jan. 9, 2009), <http://citris-uc.org/citris-study-on-sf-public-cameras-released/>.
- <sup>68</sup> See David P. Farrington & Brandon C. Welsh, *Effects of Improved Street Lighting on Crime: A Systematic Review*, Home Office Research Study 251 (Aug. 2002), p. 42; Ronald V. Clarke, U.S. Department of Justice, Office of Community Oriented Policing Services, *Improving Street Lighting to Reduce Crime in Residential Areas* (Dec. 2008), available at <http://cops.usdoj.gov/Publications/e1208-StreetLighting.pdf>; Jay Beeber, *Collision Analysis of the Photo Enforced Intersection in Walnut, CA*, <http://www.thenewspaper.com/rlc/docs/2014/ca-walnut.pdf>.
- <sup>69</sup> See Steve Scauzillo, *Red Light Cameras Being Stopped*, L.A. Daily News (Jan. 21, 2014), <http://www.dailynews.com/general-news/20140121/red-light-cameras-being-stopped>.

<sup>70</sup> PERF Report, *supra* note 24, at 44.

<sup>71</sup> United States v. Jones, 132 S. Ct. 945 (2012); Joann Pan, *FBI Turns Off 3000 GPS Devices After Ruling*, Mashable (Feb. 27, 2012), <http://mashable.com/2012/02/27/fbi-turns-off-3000-gps-devices/>.

<sup>72</sup> Kashmir Hill, *Whoops, Anyone Could Watch California City's Police Surveillance Cameras*, Forbes.com (Aug. 21, 2014), <http://www.forbes.com/sites/kashmirhill/2014/08/11/surveillance-cameras-for-all/>.

<sup>73</sup> *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), <http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/>; Jamela Debelak, ACLU of Washington, *Surveillance: Spokane Acts to Protect Privacy and Provide Transparency* (Aug. 21, 2013), <https://aclu-wa.org/blog/surveillance-spokane-acts-protect-privacy-and-provide-transparency>.

<sup>74</sup> Matt Cagle, *Alameda County Just Got a Privacy Upgrade – Alameda County, It's Your Move*, ACLU of Northern California blog, Nov. 17, 2015, <https://www.aclunc.org/blog/california-just-got-privacy-upgrade-alameda-county-its-your-move>.

<sup>75</sup> *State of Surveillance in California – Findings and Recommendations*, ACLU of California, Jan. 2015, *available at* [https://www.aclunc.org/sites/default/files/201501-aclu\\_ca\\_surveillancetech\\_summary\\_and\\_recommendations.pdf](https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf).

<sup>76</sup> Seattle City Council, Public Safety, Civil Rights and Technology Committee May 2, 2012, Seattle Channel, at 38:55, <http://www.seattlechannel.org/mayor-and-council/city-council/20122013-public-safety-civil-rights-and-technology-committee/?videoid=x23397>.

<sup>77</sup> Terry McFadden, *Technology Helping Police to Receive Warrants Faster*, WNDU.com (July 8, 2013), <http://www.wndu.com/news/specialreports/headlines/Technology-helping-police-to-receive-search-warrants-faster--214651051.html>.

<sup>78</sup> 18 U.S.C. § 2518(5) (2014).

<sup>79</sup> Ohio State Highway Patrol Policy No. OSP-103.29 (revised Dec. 23, 2008).

<sup>80</sup> Julia Reynolds, *Monterey County Grand Jury Finds Computer Data Risks*, Monterey Herald, Aug. 21, 2014, *available at* [http://www.montereyherald.com/news/ci\\_26009592/monterey-county-grand-jury-finds-computer-data-risks](http://www.montereyherald.com/news/ci_26009592/monterey-county-grand-jury-finds-computer-data-risks).

<sup>81</sup> Dianne Feinstein, *NSA Officers Spy on Love Interests*, Wall St. J., Aug. 23, 2013, *available at* <http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/>; Anjali Hemphill, *Dating on Duty: Officers Accused of Screening Dates Using Police System*, CBS 13 Sacramento (Aug. 22, 2014), <http://sacramento.cbslocal.com/2014/08/22/dating-on-duty-officers-accused-of-screening-dates-using-police-system/>.

<sup>82</sup> See Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, *available at* [http://www.mercurynews.com/breaking-news/ci\\_25766277/menlo-park-council-approves-ordinance-regulating-police-use](http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approves-ordinance-regulating-police-use).

<sup>83</sup> PERF Report, *supra* note 24, at 36.

<sup>84</sup> Dan Brekke, *Oakland Approves Scaled-Back Version of Disputed Surveillance Center*, KQED.com, Mar. 5, 2014, <http://www.kqed.org/news/2014/03/04/oakland-mayor-jean-quan-suggests-scaling-back-domain-awareness-center>.

<sup>85</sup> George Hostetter, *Former Judge Wanger Writes Far-Ranging Audit on Fresno Video Policing*, Fresno Bee, Jan. 7, 2014, *available at* <http://www.fresnobee.com/2014/01/07/3701754/judge-wanger-delivers-impressive.html>.

## Back Cover Citations

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

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

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

Editorial, *ACLU push for surveillance policy is timely*, San Jose Mercury News, Nov. 13, 2014, *available at* [http://www.mercurynews.com/opinion/ci\\_26932183/mercury-news-editorial-aclu-push-surveillance-policy-is](http://www.mercurynews.com/opinion/ci_26932183/mercury-news-editorial-aclu-push-surveillance-policy-is).





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

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

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

*—Editorial, Los Angeles Times*

*"We urge more city and county governments to...[study] an ordinance that would set specific rules about what can be done with citizens' private information."*

*—Editorial, San Francisco Chronicle*

*"It's easy to see the value in [ACLU's] approach—in all areas of government..."*

*—Steven Greenhut, San Diego Union-Tribune*

*"Elected leaders, not police departments, should set policy for the use of surveillance equipment. This is the ACLU recommendation. It's also common sense."*

*—Editorial, San Jose Mercury News*



**From:** [Kat Snyder](#)  
**To:** [Council, City](#)  
**Subject:** public comment: opposition to the ALPR program  
**Date:** Monday, April 3, 2023 11:37:43 AM

---

**CAUTION: This email originated from outside of the organization. Be cautious of opening attachments and clicking on links.**

---

Dear City Council,

I am writing to express my concern and opposition to the proposed Automatic License Plate Reader program for the police department. While I understand the desire to improve public safety, expanded surveillance does not improve public safety, and often leads to violations of privacy and civil liberties. History has shown us that once personal information is collected, it can be used for purposes beyond its original intention, often to the detriment of vulnerable populations.

If you choose to move forward with this project, I ask that you send it for policy consideration to the HRC to best protect our most vulnerable folks from the harms of surveillance.

Take care,  
~Kat Snyder



**From:** [Aram James](#)  
**To:** [Jethroe Moore](#); [Sean Allen](#); [Binder, Andrew](#); [Reifschneider, James](#); [Wagner, April](#); [Perron, Zachary](#); [Stump, Molly](#); [Josh Becker](#); [bryan.gobin@uncbusiness.net](#); [Joe Simitian](#); [Council, City](#); [Stump, Molly](#); [DuJuan Green](#); [Jeff Rosen](#); [Human Relations Commission](#); [dennis burns](#); [DuJuan Green](#); [Kevin Jensen](#); [Shikada, Ed](#); [Figueroa, Eric](#); [Michael Gennaco](#); [Foley, Michael](#); [chuck jagoda](#); [Rebecca Eisenberg](#)  
**Subject:** License plate readers -quotes from- BRENNAN CENTER Report  
**Date:** Sunday, April 2, 2023 9:02:58 PM

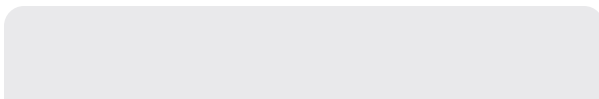
---

**CAUTION: This email originated from outside of the organization. Be cautious of opening attachments and clicking on links.**

---

**Impact on protected First Amendment rights:** Law enforcement agencies have a history of misusing license plate surveillance to monitor First Amendment–protected activity. During the 2008 presidential election, the Virginia State Police recorded the license plate numbers of attendees at political rallies for Barack Obama and Sarah Palin — and subsequently at President Obama’s inauguration — and kept the data for more than three years until it was purged following an opinion from the Virginia Attorney General warning that ongoing retention would violate the state’s Government Data Collection and Dissemination Practices Act. <sup>100</sup> Similarly, police in Denver spied on anti-logging activists and shared license plate information with the FBI’s Joint Terrorism Task Force when the activists held a training on nonviolence. <sup>101</sup>

Such surveillance — whether it involves the locations of multiple cars that appear together in the same place, or of a single car at places like a mosque, synagogue, or rally — has a chilling effect on Americans’ First Amendment rights to freedoms of association, religion, and speech. <sup>102</sup> An investigation into an NYPD program that monitored mosque visitors’ license plates found that this surveillance “chilled constitutionally protected rights — curtailing religious practice, censoring speech and stunting political organizing.” <sup>103</sup> The International Association of Chiefs of Police has noted that ALPRs can cause people to “become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance.” <sup>104</sup> And there is always the specter of more flagrant abuse, such as putting a political opponent’s license plate on a hot list and using it to keep track of that person’s whereabouts. ■





Brennan Center for Justice | Home  
[brennancenter.org](https://brennancenter.org)

Sent from my iPhone

**From:** [Aram James](#)  
**To:** [Council, City](#); [Shikada, Ed](#); [Jethroe Moore](#); [Sean Allen](#); [Josh Becker](#); [Joe Simitian](#); [Binder, Andrew](#); [Reifschneider, James](#); [Wagner, April](#); [Kevin Jensen](#); [DuJuan Green](#); [dennis burns](#); [Jeff Rosen](#); [Human Relations Commission](#); [Iadoris cordell](#); [Rebecca Eisenberg](#); [chuck jagoda](#); [Michael Gennaco](#); [Jay Boyarsky](#); [Enberg, Nicholas](#); [Shana Segal](#); [Angie Evans](#); [Perron, Zachary](#); [Cecilia Taylor](#); [Stump, Molly](#); [Shikada, Ed](#)  
**Subject:** Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use | Brennan Center for Justice  
**Date:** Sunday, April 2, 2023 8:53:22 PM

---

CAUTION: This email originated from outside of the organization. Be cautious of opening attachments and clicking on links.

---

<https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations>

Sent from my iPhone

**From:** [Aram James](#)  
**To:** [Council, City](#)  
**Cc:** [Human Relations Commission](#); [Binder, Andrew](#); [Reifschneider, James](#); [Wagner, April](#); [Stump, Molly](#); [Bryan Gobin](#); [Shikada, Ed](#); [Jethroe Moore](#); [Sean Allen](#); [DuJuan Green](#); [Kevin Jensen](#); [Foley, Michael](#); [Michael Gennaco](#)  
**Subject:** License plate readers  
**Date:** Sunday, April 2, 2023 8:49:56 PM

---

**CAUTION: This email originated from outside of the organization. Be cautious of opening attachments and clicking on links.**

---

In the wake of nationwide protests that followed the police killings of George Floyd and Breonna Taylor, public attention has increasingly focused on the ongoing instances of police brutality and racial bias in policing. However, there is a risk that police departments and legislators may incorrectly propose surveillance as a neutral alternative. Surveillance that disproportionately targets communities of color carries a distinct and cognizable equal protection harm: branding them with a badge of inferiority. As one appellate court wrote, “Our nation’s history teaches the uncomfortable lesson that those not on discrimination’s receiving end can all too easily gloss over the ‘badge of inferiority’ inflicted by unequal treatment itself. Closing our eyes to the real and ascertainable harms of discrimination inevitably leads to morning-after regret.” ■

Quote from:

# Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use



**SUMMARY:** The proliferation of ALPR technology raises serious civil

rights and civil liberties concerns. Courts, lawmakers, and technology vendors must take action.



Ángel Díaz



Rachel Levinson-Waldman

Sent from my iPhone

**From:** [Jeanne Fleming](#)  
**To:** [Council, City](#)  
**Cc:** [Clerk, City](#)  
**Subject:** Principled surveillance use policy for Automated License Plate Recognition technology  
**Date:** Sunday, April 2, 2023 3:29:39 PM

---

**CAUTION: This email originated from outside of the organization. Be cautious of opening attachments and clicking on links.**

---

Dear Mayor Kou, Vice-Mayor Stone and Councilmembers Burt, Lauing, Lythcott-Haims, Tanaka and Veenker,

I am writing to urge you to take steps to ensure that Palo Alto's use of Automated License Plate Recognition (ALPR) technology respects residents' rights.

Specifically, I urge to you to incorporate the following types of protections in the city's ALPR surveillance use policy:

1. The Palo Alto Police Department will not provide direct online access, or bulk data transfer, to any other government agencies, or to private entities other than Flock Safety, for the license plate data it collects;
2. Only a small number of Palo Alto Police Department personnel will be permitted to access the online ALPR  
System, and those who have been permitted access a) must be designated by name, and b) may only access the ALPR System for official purposes and in accordance with Palo Alto Police Department policies.
3. After one week, the license plate information of citizens who are not on the state or city's vehicle stop list, or who are not  
currently under investigation, must be permanently destroyed.
4. The license plate information of citizens who are not on the state or city's vehicle stop list, or who are not  
currently under investigation, may not be shared with other government agencies, or with private entities other than Flock Safety.
5. Flock Safety may not share any information collected in Palo Alto with any entity except the Palo Alto Police Department.

Thank you for your consideration.

Sincerely,

Jeanne Fleming

Jeanne Fleming, PhD  
[JFleming@Metricus.net](mailto:JFleming@Metricus.net)  
650-325-5151

**From:** [Hamilton Hitchings](#)  
**To:** [Council, City](#)  
**Cc:** [Reifschneider, James](#); [Binder, Andrew](#)  
**Subject:** ALPR Policy Input to City Council for the First Action Item on Monday April 3rd  
**Date:** Tuesday, March 28, 2023 6:32:48 PM

---

Some people who received this message don't often get email from hitchingsh@yahoo.com. [Learn why this is important](#)

**CAUTION: This email originated from outside of the organization. Be cautious of opening attachments and clicking on links.**

---

Dear Council,

I appreciate the Police department's proposals to limit access and retention of Automatic License Plate Reader data beyond what many other departments in the Bay Area are doing and to hold our department to a higher standard. However, because of other California law enforcement agencies' poor ALPR privacy protections and some of them sharing with ICE and the FBI, I would suggest the following amendment to the PAPD's policy.

Proposed Amendment:

**PAPD will not provide direct online access or bulk data transfer to any other agencies for the license plate data it collects.**

While I appreciate the PAPD's idea of MOUs as an additional step in protection, I think other California law enforcement agencies are unlikely to effectively implement the privacy protections required in the MOU and thus it's a waste of PAPD time. For example,

The California State Auditor conducted an audit of ALPR data collected by the Fresno Police Department, Los Angeles Police Department, Marin County Sheriff's Office, and Sacramento County Sheriff's Office.

- The audit found none of the agencies fully implemented the practices required by law since 2016 in Senate Bill 34, which includes training of personnel on use of the system and restrictions on transfer of ALPR data
- Fresno, Marin and Sacramento all were unable to confirm who has access to the system, who is responsible for oversight, or how to delete ALPR data.
- LAPD did not even have a usage or privacy policy and the other agencies ones did not implement all the legally mandated requirements
- Sacramento shares their ALPR data with one thousand agencies.
- In Marin, a former employee retained access to the ALPR after resigning for over a



year.

- Marin was also forced to settle a lawsuit with three residents who alleged the Sheriff was sharing data with federal, state and local agencies in violation of SB34.

In addition:

- Milpitas does not even keep track of who accesses their ALPR database.
- Daly City shares its data via an MOU with fusion center and 15 northern california counties with no clear limit on what it can be used for.
- Pasadena, Long Beach and BART all shared their data with ICE despite all saying they would not.

Since only a small subset of the access to the PAPD ALPR database will be audited each year, it is unlikely misuse will be detected.

That is why I recommend not giving direct access to our ALPR database to other law enforcement agencies. This will increase accountability and privacy protection of Palo Alto residents, employees and visitors vehicles location and time data. PAPD will still be able to respond to queries from other California law enforcement agencies but it will be PAPD's personnel doing the queries. I thank the PAPD for their proactive approach on privacy and for engaging the community to solicit feedback.

Hamilton Hitchings

**From:** [Tom DuBois](#)  
**To:** [Kou, Lydia](#); [greer.stone@cityofpaloalto.com](mailto:greer.stone@cityofpaloalto.com); [Tanaka, Greg](#); [Julie lythcott-Haims](#); [Vicki Veenker](#); [Burt, Patrick](#); [Ed Lauing](#)  
**Cc:** [Clerk, City](#)  
**Subject:** Item #11 for April 3 Meeting, Automated License Plate readers and surveillance technology policy  
**Date:** Tuesday, March 28, 2023 11:06:55 AM

---

**CAUTION: This email originated from outside of the organization. Be cautious of opening attachments and clicking on links.**

---

Dear Council members,

Item #11 of the April 3 meeting on Automated License Plate Readers (ALPR) surveillance policy deserves your careful consideration. Please excuse the length of this email on this important topic.

As the result of an April 25, 2016 colleagues memo by Council Member Berman, Vice Mayor Scharff, Council Member Schmid, and Council Member Wolbach, the Policy and Services committee had an extensive discussion about surveillance technologies on Dec 14, 2016 ([Staff report here](#), [detailed minutes linked here](#) starting on page 53).

License plate readers were explicitly discussed in that meeting. Council Member Scharff asked about the potential loss of privacy due to someone searching ALPR data not for a crime but to monitor citizens. In response then City Manager Jim Keene was supportive of the Council having a key oversight role when such invasive technology was adopted saying *"I agree with you...I think partly the ordinance is also designed to inject more formality into our ...acquisition of technology because I will tell you, I wasn't aware initially, when...we received a grant...I said well, you know we don't have a policy for using license plate readers We can't be using this equipment... this policy would invert all of that sort of thing so that we have a sort of gatekeeper, override from the Council."* You have a key oversight role to play with this surveillance technology.

On Dec 14, 2016 the Palo Alto City Council unanimously adopted ordinance [2.3.640 The Surveillance Privacy Protection Ordinance](#)(link). The County of Santa Clara adopted a similar ordinance just prior to Palo Alto (the county ordinance is linked further down in this letter).

Here's the Key provisions from the Palo Alto ordinance

*"Surveillance Use Policy" means a stand-alone policy or a section in a comprehensive policy that is approved by Council and contains:*

*(1) The intended purpose of the Surveillance Technology.*

*(2) Uses that are authorized, any conditions on uses, and uses that are prohibited.*

*(3) The information that can be collected by the Surveillance Technology.*

*(4) The safeguards that protect information from unauthorized access, including, but not limited to, encryption, access-control, and access-oversight mechanisms.*

*(5) The time period for which information collected by the Surveillance Technology will be routinely retained; the process by which the information is regularly deleted after that period lapses; and conditions and procedures for retaining information beyond that period.*

*(6) If and how non-City entities can access or use the information, including conditions and rationales for sharing information, and any obligations imposed on the recipient of the information.*

*(7) A description of compliance procedures, including functions and roles of City officials, internal recordkeeping, measures to monitor for errors or misuse, and corrective procedures that may apply.*

Installing twenty(20) Automated License Plate Readers around town is the first **major** use of this ordinance. In your oversight role, you need to ensure that these seven key provisions are truly addressed.

In this case, particularly provisions #4, #5 and #6 should be spelled out in more detail.

The intent of the adoption of the ordinance was to protect privacy, protect the city from data misuse and ensure our policies strike the right balance.

**For item #4, “Ensuring Against Unauthorized Access”**, Council should ensure it knows who specifically has access and that it is limited to a strong “need to know” basis. Good privacy management practices would lean towards a limited number of users able to access, with unalterable logging and regular reporting for oversight. Login credentials should be tied to single individuals and not shared. Having a limited number of PAPD officers with access to the system would ensure the city can enforce this policy overall, rather than giving access to the entire police force. Council should consider access restrictions. Please also verify that all data will be encrypted both during transit and at rest, and protections will be in place to prevent a hacker from extracting large volumes of data.

**For item #5, “The Data Retention Period”**, Council should have a policy of “long

enough but no longer". Our residents have an inalienable right to privacy under the California Constitution. In the case of ALPR data, thirty days is an extremely long time period to retain data to search for active crimes. While the proposed policy says for example that data will not be shared with federal immigration enforcement (ICE), the longer the data is retained, the more it is susceptible to unforeseen uses in the future by local, state or federal authorities. If we do not retain it, it can't be abused. Datamining the travel patterns of residents or visitors who were not apriori suspected of any crime, would violate our right to privacy and enable other potential abuses. Why not start with a 24 or 48 hour data retention policy and see if that is sufficient?

The goal should be to resolve crimes as they are happening or soon after. If 90% of the cases can be caught using data retained for 24 hours, then the impact on our privacy rights will be minimized while still achieving a huge benefit in public safety. If the Council thinks about a scale that balances personal privacy with public safety, asking for 30 days is putting a heavy thumb on the public safety side of that scale. While it may be understandable why someone responsible for public safety would want this, it is up to Council to act as a counterweight for privacy rights.

**For item #6, "If and How Non-City Entities Can Access"** an MOU is mentioned with **no** details on what obligations will be imposed on those non-city entities in order to access the system.

Will these entities take liability for any data leaks, legal violations, or any other issues that arise from their use of the data? Will they ensure they comply with all the conditions of our use policy? How will it be enforced?

Santa Clara County had an answer with explicit enforcement provisions. [Santa Clara County's Ordinance relating to surveillance technology and community safety \(link\)](#) is very much worth reading. Page 9 of the ordinance includes

- a.  
Monetary fines
- b.  
Grounds for discipline of employees
- c.  
Misdemeanor charges for misuse of surveillance data.

Council should require a Data Sharing Contract - not an MOU - and adopt similar language that applies to Palo Alto staff and to any agency that signs a contract if Council decides that moving forward with data sharing from the start is desirable.

**For item #7, "Description of Oversight and Compliance"**, Council would do well to

adopt provisions similar to the County Ordinance as part of its oversight responsibility. Paraphrasing the language in the county ordinance:

*Council should receive an annual ALPR report in order for council to determine whether the benefits to the impacted department(s) and the community of the surveillance technology outweigh the costs and whether reasonable safeguards exist to address reasonable concerns regarding privacy, civil liberties, and civil rights impacted by deployment of the surveillance technology. If the benefits or reasonably anticipated benefits do not outweigh the costs or civil liberties or civil rights are not reasonably safeguarded, the 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 Council's concerns; and/or (3) directing a report-back from the department regarding steps taken to address the Council's concerns.*

*The Council shall hold a public meeting, with Annual Surveillance Reports agendized on the regular (non-consent) calendar.*

*Annual Surveillance Report means a written report concerning ALPR technology that includes all of the following:*

- (1) A description of how the surveillance technology was used, including whether it captured images, sound, or information regarding members of the public who are not suspected of engaging in unlawful conduct;*
- (2) 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;*
- (3) A summary of community complaints or concerns about the surveillance technology;*
- (4) The results of any non-privileged internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;*
- (5) Whether the surveillance technology has been effective at achieving its identified purpose;*
- (6) Statistics and information about 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.*

There is an opportunity to do this well, apprehending more crimes committed with cars within Palo Alto, while at the same time respecting our citizens rights to privacy and protecting the City from a scandal caused by a data leak or the illicit use of surveillance data. Please consider:

1.  
Limiting access to a few individuals
2.  
Retaining data for 48 hours (with exceptions for data tied to a crime)
3.  
Require a strong data sharing Contract with other police agencies before providing access.
4.  
Require an annual review by Council

Thanks for your consideration,

Tom DuBois

# Public Input on ALPR Technology

Submission date: **9 March 2023, 9:37AM**

Receipt number: **7**

Related form version: **2**

## Ask a question about ALPR technology...

Thank you for reaching out to the community and providing a detailed FAQ with valuable information.

Are we using the same ALPR vendor as surrounding agencies?

Can PAPD and other agencies retrieve and share information in real time?

Will PAPD roll out a test ALPR deployment to get the bugs worked out?

Do SB 1421 and AB 748 apply to ALPR images? If so, how does the 30 retention limit comport with the 45 day release deadline in California law?

What are the proposed changes to PAPD Policy 462 with this new technology?

## Please share your thoughts with us!

I support the Palo Alto Police Department's deployment of static ALPR technology in our city. This technology is an important crime fighting tool that is inexpensive, has already shown value for neighboring police agencies and is a force multiplier for law enforcement.

I encourage council to work with the police department in updating the PAPD's Policy Manual to cover static ALPR deployments and clarifying the use and release of ALPR images under California law.

### Optional contact information...

Joe Landers  
Barron Avenue  
Palo Alto



# Public Input on ALPR Technology

Submission date: **6 March 2023, 10:16AM**

Receipt number: **6**

Related form version: **2**

**Ask a question about ALPR technology...**

---

**Please share your thoughts with us!**

**Seems like an easy decision for helping our Police Department. Please approve the ALPR.**

**Optional contact information...**

---

# Public Input on ALPR Technology

Submission date: **3 March 2023, 6:40AM**

Receipt number: **5**

Related form version: **2**

**Ask a question about ALPR technology...**

---

**Please share your thoughts with us!**

I am in favor of adding ALPR technology to our streets. Crime seems to have increased lately and with the limitations in place (no facial recognition and short storage period) this seems like a useful tool with limited downside.

**Optional contact information...**

---

# Public Input on ALPR Technology

Submission date: 28 February 2023, 11:53AM

Receipt number: 4

Related form version: 2

## Ask a question about ALPR technology...

Dear Chief Binder,

As I am sure you can all see, we have a tremendous retail vacay in downtown Palo Alto. You can't pick up a newspaper or turn on the news station without seeing something about how bad the crime rate has grown.

In the last 5 years when a new merchant is interested in moving to Palo Alto, they ask me how safe the city is and how bad the theft problem is. It is a hard question to answer as both of these things have been increasing over the years and so has crime, so I bite my tongue if I can.

I am writing this letter because I have been in the retail business for the last 50 years, owning apparel and shoe stores. I truly understand the hardship it is for someone going into business in our city. In order to start a business you have to get a city permit to build out your store front, which the cost has gone up. You have to hire an architect, which the cost has gone up. You have to hire a contractor, which the cost has gone up, and then the operating expenses (taxes, salaries, insurance, etc.) has gone up. The only thing that hasn't gone up is the margins of profits, which

has gone down for the independent retailer. This is why it is so tough to stay in business when your store is robbed after all of the hard work that is put in. I feel that anything the city and police department can do that is safer is a great idea. I am supporting the ALPR technology in order to help catch the thieves. I believe it will be a big deterrent and a step in the right direction in helping the retailers.

In ending, we would all like to see a clean and safe city like it used to be.

Roxy Rapp  
265 Lytton Ave., Suite 303  
650 575 9488

**Please share your thoughts with us!**

Dear Chief Binder and P.A. City Council,

As I am sure you can all see, we have a tremendous retail vacancy in downtown Palo Alto. You can't pick up a newspaper or turn on the news station without seeing something about how bad the crime rate has grown.

In the last 5 years when a new merchant is interested in moving to Palo Alto, they ask me how safe the city is and how bad the theft problem is. It is a hard question to answer as both of these things have been increasing over the years and so has crime, so I bite my tongue if I can.

I am writing this letter because I have been in the retail business for the last 50 years, owning apparel and shoe stores. I truly understand the hardship it is for someone going into business in our city. In order to start a business you have to get a city permit to build

out your store front, which the cost has gone up. You have to hire an architect, which the cost has gone up. You have to hire a contractor, which the cost has gone up, and then the operating expenses (taxes, salaries, insurance, etc.) has gone up. The only thing that hasn't gone up is the margins of profits, which has gone down for the independent retailer. This is why it is so tough to stay in business when your store is robbed after all of the hard work that is put in. I feel that anything the city and police department can do that is safer is a great idea. I am supporting the ALPR technology in order to help catch the thieves. I believe it will be a big deterrent and a step in the right direction in helping the retailers.

In ending, we would all like to see a clean and safe city like it used to be.

Roxy Rapp  
265 Lytton Ave., Suite 303  
650 575 9488

Optional contact information...

# Public Input on ALPR Technology

Submission date: 24 February 2023, 12:35AM

Receipt number: 3

Related form version: 2

## Ask a question about ALPR technology...

Hi

May i ask who needs this information so badly that our city needs to be collecting it.

This information is not going to make it safer to live.

Isn't this information already being collected via a private company in palo Alto

## Please share your thoughts with us!

Hi

I want to know why the City needs to collect information on who owns what car on the roads of Palo Alto.

.if you don't know who or what is driving a car, what does it matter ?

If it's a registered car, can't that car go Anywhere it wants?

## Optional contact information...

**Jeff Kolence@gmail..com**

**Cubberley**

**High school**

**Graduate**

**And Palo Alto Resident**

# Public Input on ALPR Technology

Submission date: 20 February 2023, 8:12PM

Receipt number: 2

Related form version: 2

Ask a question about ALPR technology...

Please share your thoughts with us!

Please approve ALPR. I am a card carrying member of the ACLU. I do not believe this is an invasion of privacy. This will reduce crime, and it will make it easier to solve crimes.

Optional contact information...

Eddie Gornish  
3694 South Court  
Palo Alto, CA 94306



# Public Input on ALPR Technology

Submission date: 14 February 2023, 10:16AM

Receipt number: 1

Related form version: 2

## Ask a question about ALPR technology...

Hi, my name is Morgan Sin. I am a Sales and Marketing Analyst here at Route1 Inc. We specialize in ALPR technology as well as professional services to support the technology after implementation. We have a contract with the state of California to provide LPR technology for the least expensive price in the state. One of our largest customers in California is the California Highway Patrol (CHP). I would appreciate some time to discuss our LPR offerings as well as hear more about how Palo Alto Police Department plans to use the technology. We also provide a full suite of police technology, such as rugged devices, printers, scanners, and more.

Please reach out to me at [morgan.sin@route1.com](mailto:morgan.sin@route1.com) or call me at 602-558-9355. Thank you!

## Please share your thoughts with us!

Hi, my name is Morgan Sin. I am a Sales and Marketing Analyst here at Route1 Inc. We specialize in ALPR technology as well as professional services to support the technology after implementation. We have a contract with the State of California to provide LPR technology for the least expensive price in the State. One of our largest customers in California is the California Highway Patrol (CHP). I would appreciate some time to discuss our LPR offerings as well as hear more about how Palo Alto Police Department plans to use the technology. We also provide a full suite of police technology, such as rugged devices, printers, scanners, and more. Please reach out to me at [morgan.sin@route1.com](mailto:morgan.sin@route1.com) or call me at 602-558-9355. Thank you!

#### Optional contact information...

Morgan Sin  
[morgan.sin@route1.com](mailto:morgan.sin@route1.com)  
602-558-9355  
<https://www.route1.com/>



# Use of Automated License Plate Recognition (ALPR) Technology

Report # 2301-0741

# ALPR – Agenda Action Items

---

Staff is recommending that the Council:

- Approve a 3-year contract with Flock Safety to implement fixed ALPR technology, in an amount not to exceed \$174,400;
- Approve the use of fixed ALPR technology to deter and investigate criminal activity
- Approve the fixed ALPR surveillance use policy



# ALPR – What is it?

---

- **Automated License Plate Recognition (ALPR)** technology uses a combination of cameras and computer software to scan the license plates of passing vehicles.
- These computer-readable images allow law enforcement to compare plate numbers against plates of wanted vehicles and vehicles associated with wanted persons, missing persons, etc.



# ALPR – Types

---

Two types of ALPR:



## MOBILE

(mounted on a police vehicle)

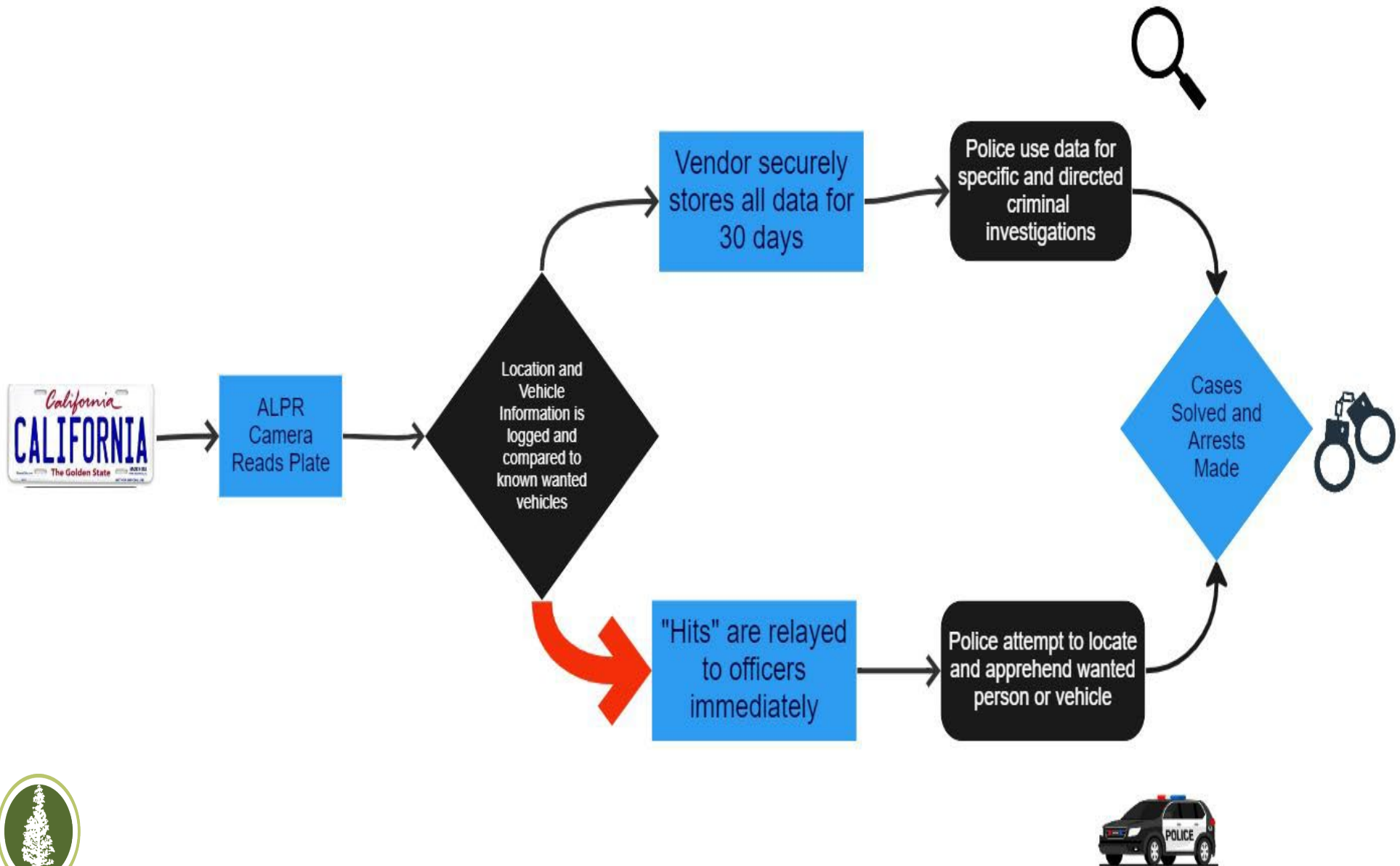


## FIXED

(mounted on pole or other piece of infrastructure)



# ALPR – How It Works



# ALPR – What Problems Does it Address?

---

- Regional increases in property crimes, including catalytic converter thefts, auto burglaries, vehicle thefts and organized retail thefts
- Recent, albeit rare, brazen robberies and assaults
- Offender behavior:
  - use of vehicles;
  - use of stolen vehicles or vehicles with a stolen plate;
  - engage in crimes in multiple jurisdictions;
- Cost-effective force multiplier





# ALPR – What Information is Captured?

---

- A fixed ALPR system is designed to capture:
  - the date, time, and location;
  - license plate (state, partial, paper, and no plate);
  - vehicle characteristics (make, model, type, and color)



# ALPR – What Information Is *Not* Captured?

---

- A fixed ALPR system *is not* intended to capture images of vehicle occupants
- A fixed ALPR system *does not* use facial recognition



# ALPR – Fixed ALPR vs. Red Light Cameras

---

- A red light camera is designed to capture driver images for driver identification
- A fixed ALPR system is designed to capture rear license plate images for vehicle identification



# ALPR – Uses & Benefits

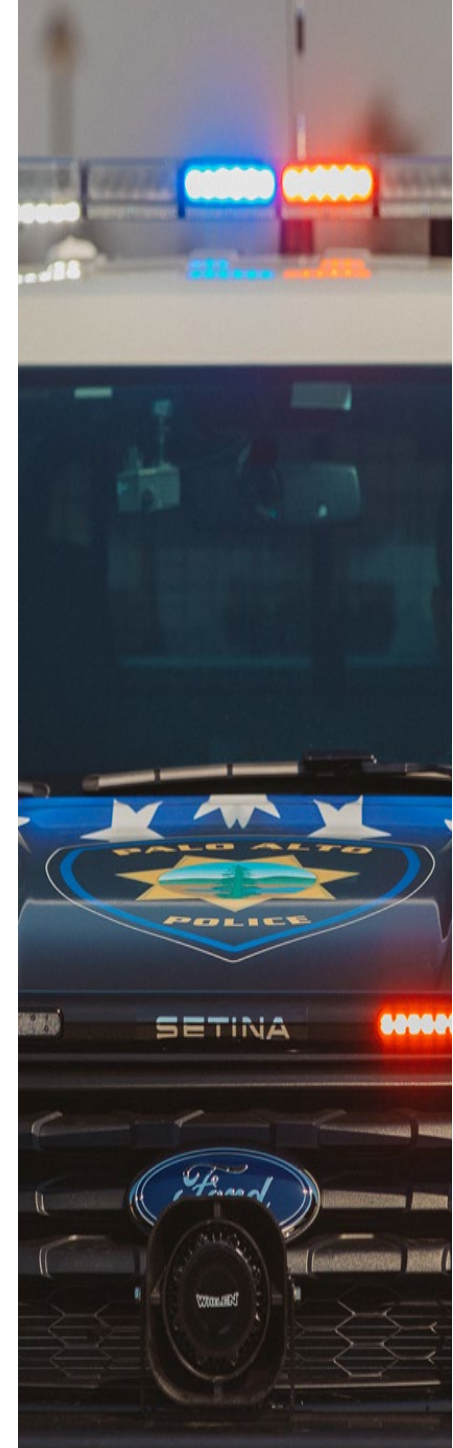
---

## USES

- Proactive  
Real-time alerts
- Reactive (Investigative)  
Searchable database

## BENEFITS

- ✓ Real-time Alerts
- ✓ Deterrence
- ✓ Solve Crimes Already Committed
- ✓ Regional Coordination
- ✓ Expanded Searchable Data Set



# ALPR – Local Implementation & Collaboration

---

- ALPR technology is an existing tool for local law enforcement including many neighboring communities – a growing number of Bay Area agencies already use Flock Safety or are pursuing it
- Numerous success stories and examples of where it *could* have been used in Palo Alto
- Private businesses, HOAs, and individuals have ALPR and may elect to share that data with law enforcement



## ALPR – Local Implementation & Collaboration (cont.)

---

- Implementation plan calls for 20 total cameras to be installed at strategically-selected locations based on several factors: crime statistics, common vehicular ingress and egress points, and traffic volume
- No ALPR cameras permanently installed in residential neighborhoods. Could *temporarily* relocate an ALPR camera into a neighborhood long enough to address a specific crime trend in that area



# ALPR – Legal Considerations

---

## Palo Alto

### Surveillance Technology Ordinance

- Council approval required
- Weigh benefits versus costs and concerns
- Surveillance use policy

## State Law

- Requires training
- Requires limitations/controls on access
- Requires limitations on sharing
- Criminal penalties for unauthorized access



# ALPR – Surveillance Use Policy Components

---

## Training and Access

- Need to know and right to know only;
- Training provided to employees;
- Individual log-in and purpose required;
- Agency controls with whom data is shared;
  - Local law enforcement only (no fusion centers)
  - Via MOU or individual query only
  - No bulk data transfers
  - No outside sharing by vendor

## Data Security

- CJIS-compliant transmission and storage by vendor

## Data Retention

- Automatically purged after 30 days\*

## Auditing

- Queries logged and auditable
- Compliance officer





# ALPR – Why Flock Safety?

---

- Technology
  - Confidence in durability and reliability of hardware and support
  - Improved ability to collaborate with others
  - Technology captures other vehicle information (e.g., make, model, color)
  - Agency ownership and customizable control over its own data
  - Robust auditing capabilities of all queries
  - Transparency Portal
- Implementation
  - Expertise with installation on state highways and county roadways (i.e., SR-82, Oregon Expressway)
  - Locating cameras to maximize efficiency



# ALPR – Resource Impact

---

- 3-year contract with Flock Safety
- City does not install, own, or maintain cameras
- Total estimated costs of deployment:
  - \$61,900 (balance of FY23, plus FY24)
    - Installation
    - Subscription (data storage and access)
  - \$52,000 per subsequent year (FY25 and FY26)
  - Funding for years 1-2 to come from SLES fund balance
  - Option to renew for 2 additional years



# ALPR –Community Outreach and Input

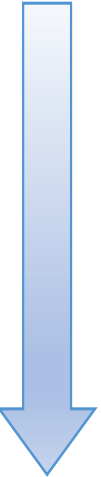
---

- |                                       |               |
|---------------------------------------|---------------|
| • Council Study Session               | October 2022  |
| • ACLU meeting                        | November 2022 |
| • Chamber & neighborhood meetings     | December 2022 |
| • Launch of ALPR info webpage         | February 2023 |
| • Community virtual info session      | March 2023    |
| • Draft surveillance policy published | March 2023    |



# ALPR – Next Steps

---

- 
- ✓ Council's feedback and discussion on potential implementation of ALPR technology
  - ✓ Gather community feedback
  - ✓ Complete a procurement process
  - Council approval of agreement, deployment plan, and associated surveillance use policy
  - Implementation (projected to occur within 8 weeks of approval)





CITY OF  
**PALO  
ALTO**