



City of Palo Alto

City Council Staff Report

(ID # 8834)

Report Type: Consent Calendar

Meeting Date: 9/10/2018

Summary Title: Surveillance Technology Ordinance

Title: Policy and Services Committee Recommendation to Adopt an Ordinance Adding Sections 2.30.620 - 2.30.690 to Title 2 of the Administrative Code to Establish Criteria and Procedures for Protecting Personal Privacy When Considering the Acquisition and Use of Surveillance Technologies, and Provide for Ongoing Monitoring and Reporting

From: City Manager

Lead Department: City Manager

Recommendation

The Policy & Services Committee recommends City Council adopt an ordinance adding Sections 2.30.620 – 2.30.690 to Title 2 of the Municipal Code (Attachment B) to establish criteria and procedures for protecting personal privacy when considering the acquisition and use of surveillance technologies by the City, and providing for ongoing monitoring and reporting.

Background

In April 2016, Councilmembers Wolbach, Berman and Scharff presented a Colleagues Memo to City Council proposing the adoption of a City Policy or Ordinance to increase transparency and oversight in the acquisition and deployment of surveillance technologies (Attachment A). At the April 25, 2016 Council Meeting, Council voted to refer this Colleagues Memo to the Policy and Services Committee to discuss and potentially make recommendations to Council, with a focus on technology that collects personally identifiable information.

In December 2016, City staff presented to the Policy and Services Committee research and in depth information on current surveillance technologies used within the City and outlined some methods other governmental agencies are using to balance transparency, innovation and public safety through the pursuit of smart city strategies. The Committee instructed staff to return to Policy and Services Committee with a potential Ordinance that would establish department policies and practices in order to reinforce the protection of individual privacy.

Subsequently, in June 2017, staff returned to the Policy and Services Committee with proposed tenets to form the framework for an Ordinance to protect personal privacy in the use of surveillance technologies by the City. The Committee recommended (3-0, Wolbach, Kniss, and

Kou in favor, DuBois absent) City Council approval of an Ordinance based on the tenets presented.

Discussion

Personally Identifiable Information as defined by the U.S. Department of Labor is, “any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.” As new technologies emerge the City seeks to reaffirm the commitment to the privacy rights of its community members by establishing an Ordinance that will increase City Council oversight and transparency in the purchase and use of surveillance technologies.

City Staff have reviewed the landscape of laws and policies in place regarding surveillance technologies purchased and used by government agencies, and sought feedback from stakeholders. This led to the comprehensive information provided to the Policy & Services Committee in December 2016 and July 2017.

Given this, based on staff’s proposal the Policy and Services Committee recommends an Ordinance that addresses technologies of concern today while also allowing for inclusion of new surveillance technologies that may be developed in the future. This approach establishes reporting and approval processes that can increase transparency without compromising public safety, limiting local control, or requiring additional resources.

Summary of the Recommended Ordinance:

Definition of Surveillance Technology: The breadth of what is defined in the Ordinance as surveillance technology will dictate the frequency of requests to Council and resources required to comply with reporting and approval tenets. The recommended Ordinance reflects a measured approach as a starting point from which to build:

“Surveillance Technology” means any device or system primarily designed and actually used or intended to be used to collect and retain audio, electronic, visual, location, or similar information constituting personally identifiable information associated with any specific individual or group of specific individuals, for the purpose of tracking, monitoring or analysis associated with that individual or group of individuals. Examples of surveillance technology include, but are not limited to, drones with cameras or monitoring capabilities, automated license plate readers, closed-circuit cameras/televisions, cell-site simulators, biometrics-identification technology, and facial-recognition technology.

In addition to public safety, staff expects that technology applications for transportation and smart city purposes may meet the above definition. Through existing policies and procedures (1-63 and 1-64) staff evaluates prospective purchases and contracted services for potential data security and information privacy impacts. The attached ordinance anticipates the need for Council adoption of surveillance policies for each type of surveillance technology. Building on

these existing practices, staff will advance applications for City Council review and approval where the potential for collecting personally identifiable information has been determined to exist.

Explicit Council Authorization: Any purchase or contractual agreement for use of surveillance technology, no matter the cost, would require prior City Council authorization. This ensures that even low-cost technology is given thorough review prior to the City purchase or deploying.

Public Oversight: Staff reports requesting authorization will be placed on the Council agenda to ensure public awareness and Council oversight. The City Manager in consultation with the Mayor will determine whether to place the item on the Action or Consent Agenda, with consideration for the significance of the technology and competing demands on Council's time. Reports will at a minimum include:

- a detailed description of the technology with an explanation of how it works and what information it captures;
- statutory and/or regulatory rules governing use of the technology;
- measures that will be taken to protect private information;
- how data will be managed and retained; and,
- existing and/or recommended City administrative policies and procedures regarding use of the technology and the information it produces.

Transparency and Ongoing Oversight: To continue oversight of the City's use of surveillance technology after the initial authorization, the City Manager will annually submit a report to the City Council. This is proposed to occur within the first quarter of each calendar year, with the report to include:

- identification of applicable technologies and date of City Council authorization;
- department(s) utilizing the technology;
- frequency of deployment during the year; and,
- purpose and outcome of the deployments.

This report will be made easily accessible via the City's website to reinforce transparency. Staff anticipates that the annual report will be a summary description of technologies in use and statistical report on deployments. This report would avoid divulging potentially sensitive incident or investigatory details.

In addition to reporting on the use of surveillance technology, the annual report will provide a regular opportunity to review the effectiveness of the Ordinance and consider amendments as may be desirable.

Attachments:

- Attachment A: Colleagues Memo 4-25-16
- Attachment B: Surveillance ORD April 2018 0140191
- Attachment C: Policy and Services Committee Action Minutes June 13, 2017
- Attachment D: Surveillance Technologies Staff Report #8180 June 13, 2017



City of Palo Alto

COLLEAGUES MEMO

DATE: April 25, 2016

TO: City Council Members

FROM: Council Member Berman, Vice Mayor Scharff, Council Member Schmid, Council Member Wolbach

SUBJECT: COLLEAGUES MEMO: DEVELOPING CITY POLICY ON ACQUISITION, USE, AND SAFEGUARDS FOR SURVEILLANCE AND INFORMATION-GATHERING TECHNOLOGIES

SUMMARY

In order to maintain public trust, ensure protection of privacy, and provide clarity for city staff, Palo Alto should proactively adopt an ordinance establishing a general policy governing consideration, adoption, and use of surveillance and information-gathering technologies by city departments, contractors, or partners.

RECOMMENDATION

We recommend the City Council refer this memo to the Policy and Services Committee to discuss (supported by appropriate staff) creation of an ordinance or other policy governing surveillance and information-gathering technology. Such an ordinance would establish a standard operating procedure (SOP) to be utilized prior to adoption or re-purposing of any technology for potential surveillance applications by City departments, contractors, or partners, as well as prior to seeking funding for such technologies. In addition, the ordinance would require annual reporting on uses of such technologies by the City. Policy and Services should consider the following:

1. Whether and when public hearings and other community engagement are appropriate prior to adoption of surveillance technology by the City, contractor, or partner;
2. The mechanism for Council approval prior to adoption of, re-purposing of, or seeking funding for surveillance technology;
3. Information, such as a Surveillance Impact Report or statement in a City Manager's Report, to be prepared by staff prior to approval which would include information on operations and management; data use; data minimization and limitation; secure data storage and transmission; data access; data retention; data sharing; handling of Public Records Act requests and any individualized policy recommendations;
4. The requirements of federal, state and local laws, regulations and programs that protect and/or regulate gathering, access, retention and use of personally identifiable information and surveillance technology (such as HIPPA, PCII, PII, VISA, VMS, PRA and

- Records Retention). The Committee should survey the existing field of regulation as part of its preparation for developing new regulations;
5. Measures to accommodate community interests in smart city initiatives and other innovations, data-gathering to support planning efforts and other policy development, use of technology to facilitate access to City services and programs, security of persons and property, and cost efficiency, to strike the right balance for Palo Alto;
 6. Information sharing between jurisdictions; and
 7. What type of oversight, evaluation, auditing, or enforcement are appropriate.

For further discussion of possible components, see the model ordinance by the American Civil Liberties Union (Attachment A, pages 22-25) and recommendations by the International Association of Chiefs of Police (Attachment B, pages 3-7).

BACKGROUND

Technology

Examples of technology with surveillance applications include but are not limited to: automated license plate readers (ALPRs), image and video recording, audio recording, unmanned aerial vehicles (aka "drones"), voice recognition, facial recognition, gait analysis, location tracking, automated social media monitoring, cell phone interceptors / cell phone tower emulators (international mobile subscriber identity catchers "IMSI", e.g. Stingrays), electronic communication surveillance (e.g. internet and phone interception), hacking, and data mining.

Palo Alto

Palo Alto currently uses audio recording, cameras in police vehicles, body-worn cameras for police officers, and received one ALPR through a County grant. The Council also recently (October 5, 2015) approved a contract to deploy low resolution cameras to count pedestrian and bicycle traffic (the City Manager added a privacy clause to the contract). For video recording in particular, Palo Alto has a staff-written policy that was revised as recently as January 2015. (See Attachment E).

Other Cities

Other municipalities around the state (see Attachment C) and country have adopted various other technologies, often without notification to the public or elected officials, and without robust policies governing data protection, data access, and data retention. Boston, it was recently revealed, collected ALPR data (tracking residents' locations) which was stored online and accessible by the public. Alameda, CA, recently adopted a policy for Stingrays which was transparent, and well received by privacy advocates and the community as a good example.

County

Santa Clara County recently rejected adoption of Stingray cell phone interceptors after concerns raised by Supervisor Joe Simitian, in particular due to concerns about transparency. (See attachment D). Santa Clara County is currently considering an ordinance governing surveillance technology use by county agencies.

State

In 2015, Governor Jerry Brown signed several bills regarding privacy and modern technology. Two by Senator Jerry Hill deal with ALPRs (SB 34) and cell phone interceptors (SB 741). SB 178 by Senators Mark Leno and Joel Anderson requires a warrant prior to searching cell phones, emails, etc. AB 856 by Assemblymember Ian Calderon restricts use of drones over private property. AB 1116 by Assemblymember Mike Gatto restricts uses of voice recordings by private companies.

Federal

The Northern California Regional Intelligence Center (aka NCRIC or Fusion Center) in San Francisco links local surveillance with federal, raising concerns for residents about how data collected by local agencies will be shared with federal agencies. Federal intelligence, military, and law enforcement have been the subject of much controversy regarding surveillance technology - the nature, adoption, use, security, and legal justification of which have been questioned.

DISCUSSION

Law enforcement and government depend on the trust of the community. Use of technologies which has the appearance, potential, or effect of violating privacy or civil liberties can diminish community trust in government, particularly when adopted and used without transparency. The City's contracting processes include security and other requirements for data and personal information, and the City has a video management procedure that applies to visual information gathering, such as at sensitive utility infrastructure facilities, public garages, etc.

Rapidly evolving surveillance technology raises concerns for the City including, but not limited to: privacy of residents and visitors; chilling effects on expression, research, travel, association, or other rights; misuse of data; data breach (access by unauthorized parties); and adoption, use, or expansion of capabilities without Council oversight.

Rather than attempt to predict or react to each piece of emerging technology, the proposed ordinance would proactively establish a high level policy to be followed prior to the City (or contractor or partner) seeking funding, adopting, or re-purposing any specific technology. This standard operating procedure would provide clarity and predictability for City departments, the City Council, and the community.

As technology advances in coming years, our Police Department in particular will benefit from the confidence of our community that such technologies will only be adopted and utilized in a transparent and responsible manner with clear oversight by the elected City Council and the public to whom they are accountable.

Staff Impact

Resources from the following departments will be needed to support a policy discussion in Policy & Services: Information Technology, Police Department, Planning & Community

Environment, Utilities, Public Works, Emergency Services, City Manager's Office, City Clerk's Office and City Attorney's Office.

Depending on its breadth and specific requirements, significant staff resources may be needed to administer and maintain any new program. As a result of the evolving landscape of technology and security threads, privacy issues and the value of well-conceived policies are not limited to police and public safety activities alone. Utilities, for example, are increasingly working with data that can be sensitive for customers, and this sensitivity will increase with the roll-out of smart meter and smart grid technologies. Similarly, the capability of traffic and parking technologies to collect granular data presents another opportunity to examine the need for balancing data analytics and privacy priorities, while advancing the City's smart city initiatives.

Staff is not suggesting that these issues be overlooked. To the contrary, this may be a topic in which Palo Alto is uniquely positioned to demonstrate leadership in thoughtful stakeholder engagement and policy development. It should be recognized, however, that this effort may be a significant undertaking requiring consummate resources and prioritization to address effectively.

Ordinance No. _____

Ordinance of the Council of the City of Palo Alto Adding Sections 2.30.620 – 2.30.690 to Title 2 of the Palo Alto Municipal Code to Establish Procedures for the Relating to Surveillance Technology

The Council of the City of Palo Alto does ORDAIN as follows:

SECTION 1. Findings and Recitals. The Council of the City of Palo Alto finds and declares as follows:

To promote public trust and ensure protection of privacy, the Palo Alto City Council desires to establish a general policy governing consideration, acquisition and use of technologies by the City, including its contractors and partners, that gather information about specific individuals or groups of individuals;

The City also recognizes the value of and wishes to foster Smart City initiatives that enhance City programs and services to citizens and visitors through the use of technology;

Accordingly, the City adopts the following ordinance to increase transparency, oversight and accountability in the acquisition and deployment of technologies that collect and retain personally identifiable information of persons not accused of unlawful activity.

SECTION 2. PART 6A – SURVEILLANCE AND PRIVACY PROTECTIONS, Sections 2.30.620 – 2.30.690, is added to Chapter 2.30 [Contracts and Purchasing Procedures], of Title 2 [Administrative Code] of the Palo Alto Municipal Code to read as follows:

2.30.620 Title.

This Part 6A shall be known as the Surveillance and Privacy Protection Ordinance.

2.30.630 Council Approval Required for Contracts, Agreements, Grant Applications and Donations Involving Surveillance Technology.

The Council shall approve each of the following:

(a) Applications for grants, acceptance of state or federal funds, or acceptance of in-kind or other donations of Surveillance Technology;

(b) Notwithstanding any delegation of authority to award contracts in this Chapter 2.30, contracts of any type and any amount that include acquisition of new Surveillance Technology;

(c) Use of Council-approved Surveillance Technology for a purpose, in a manner, or in a location outside the scope of prior Council approval; or

(d) Agreements with a non-City entity to acquire, share, or otherwise use Surveillance Technology or the information it provides.

2.30.640 Council Approval of Surveillance Use Policy.

The Council shall approve a Surveillance Use Policy addressing each activity that it approves that is listed in Section 2.30.630. If no current Surveillance Use Policy covers an approved activity, Council shall adopt a new policy or amend an existing policy to address the new activity.

2.30.650 Information Required.

Unless it is not reasonably possible or feasible to do so, before Council approves a new activity listed in Section 2.30.630, the City should make available to the public a Surveillance Evaluation and a proposed Surveillance Use Policy for the proposed activity.

2.30.660 Determination by Council that Benefits Outweigh Costs and Concerns.

Before approving any new activity listed in Section 2.30.630, the Council shall assess whether the benefits of the Surveillance Technology outweigh its costs. The Council should consider all relevant factors, including financial and operational impacts, enhancements to services and programs, and impacts on privacy, civil liberties, and civil rights.

2.30.670 Oversight Following Council Approval.

Beginning fiscal year 2019 and annually thereafter, the City shall produce and make available to the public an Annual Surveillance Report. The Annual Surveillance Report should be noticed as an informational report to the Council. The Council may calendar the Annual Surveillance Report or any specific technology included in the report for further discussion or action, and may direct that (a) use of the Surveillance Technology be modified or ended; (b) the Surveillance Use Policy be modified; or (c) other steps be taken to address Council and community concerns.

2.30.680 Definitions.

The following definitions apply to this Section:

(a) "Annual Surveillance Report" means a written report, submitted after the close of the fiscal year and that includes the following information with respect to the prior fiscal year:

- (1) A description of how each Council-approved 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 types of data disclosed, and the reason for the disclosure;

- (3) A summary of any community complaints or concerns about the surveillance technology;
- (4) Non-privileged and non-confidential information regarding the results of any internal audits, 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) The number and nature of Public Records Act requests relating to the Surveillance Technology;
- (7) Annual costs for the Surveillance Technology and for compliance with this Surveillance and Privacy Protection Ordinance, including personnel and other ongoing costs, and sources of funding; and
- (8) Other relevant information as determined by the City Manager.

The Annual Surveillance Report will not include information that may compromise the integrity or limit the effectiveness of a law enforcement investigation.

(b) "Surveillance Evaluation" means written information, including as part of a staff report, including:

- (1) A description of the Surveillance Technology, including how it works and what information it captures;
- (2) Information on the proposed purpose, use and benefits of the Surveillance Technology;
- (3) The location or locations where the Surveillance Technology may be used;
- (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;
- (5) The costs for the Surveillance Technology, including acquisition, maintenance, personnel and other costs, and current or potential sources of funding.

(c) "Surveillance Technology" means any device or system primarily designed and actually used or intended to be used to collect and retain audio, electronic, visual, location, or similar information associated with any specific individual or group of specific individuals, for the purpose of tracking, monitoring or analysis associated with that individual or group of individuals. Examples of Surveillance Technology include drones with cameras or monitoring capabilities, automated license plate readers, closed-circuit cameras/televisions, cell-site

simulators, biometrics-identification technology and facial-recognition technology. For the purposes of this Ordinance, "Surveillance Technology" does not include:

- (1) Any technology that collects information exclusively on or regarding City employees or contractors;
- (2) Standard word-processing software; publicly available databases; and standard message tools and equipment, such as voicemail, email, and text message tools;
- (3) Information security tools such as web- filtering, virus detection software;
- (4) Audio and visual recording equipment used exclusively at open and public events, or with the consent of members of the public;
- (5) Medical devices and equipment used to diagnose, treat, or prevent disease or injury.

(d) "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.

2.30.690 No Private Right of Action.

This Surveillance and Privacy Protection Ordinance is not intended and shall not be interpreted to create a private right of action for damages or equitable relief on behalf of any person or entity against the City or any of its officers or employees.

SECTION 3. Severability. If any provision, clause, sentence or paragraph of this ordinance, or the application to any person or circumstances, shall be held invalid, such invalidity shall not affect the other provisions of this ordinance which can be given effect without the invalid provision or application and, to this end, the provisions of this ordinance are hereby declared to be severable.

SECTION 4. CEQA. This ordinance is exempt from the requirements of the California Environmental Protection Act (CEQA) pursuant to Section 15061(b)(3) of Title 14 of the California Code of Regulations since it can be seen with certainty that there is no possibility the adoption and implementation of this ordinance may have significant effect on the environment.

SECTION 5. Effective Date. This ordinance shall be effective on the thirty-first date after the date of its adoption.

INTRODUCED:

PASSED:

AYES:

NOES:

ABSTENTIONS:

ABSENT:

ATTEST:

APPROVED:

City Clerk

Mayor

APPROVED AS TO FORM:

City Manager

City Attorney



POLICY AND SERVICES COMMITTEE ACTION MINUTES

Special Meeting
Tuesday, June 13, 2017

Chairperson Wolbach called the meeting to order at 6:06 P.M. in the Community Meeting Room, 250 Hamilton Avenue, Palo Alto, California.

Present: Kniss, Kou, Wolbach (Chair)

Absent: DuBois

Agenda Items

1. Consideration of a City Ordinance Protecting Personal Privacy in the Acquisition and use of Surveillance Technologies by the City.

MOTION: Chair Wolbach moved, seconded by Vice Mayor Kniss to recommend the City Council adopt an Ordinance establishing criteria and procedures for protecting personal privacy when considering the acquisition and use of surveillance technologies by the City with an emphasis on public privacy, personally identifiable information, including acquisition from any source, data acquisition, data retention and data dissemination.

INCORPORATED INTO THE MOTION WITH THE CONSENT OF THE MAKER AND THE SECONDER to add to the Motion "and to consider the Staff proposed Ordinance tenets as a basis for the Ordinance."

MOTION RESTATED: Chair Wolbach moved, seconded by Vice Mayor Kniss to recommend the City Council adopt an Ordinance establishing criteria and procedures for protecting personal privacy when considering the acquisition and use of surveillance technologies by the City with an emphasis on public privacy, personally identifiable information, including acquisition from any source, data acquisition, data retention and data dissemination, and to consider the Staff proposed Ordinance tenets as a basis for the Ordinance.

MOTION PASSED: 3-0 DuBois absent

2. Recreational and Medical Marijuana: Review and Discussion of State Law Developments and Input to Staff on Next Steps, Including Possible Ordinance Adopting Local Regulations Regarding Commercial

ACTION MINUTES

Marijuana Activity, Outdoor Cultivation, and Marijuana Dispensaries. This Action is Exempt Under Section 15061(b)(3) of the California Environmental Quality Act.

MOTION: Vice Mayor Kniss moved, seconded by Chair Wolbach to recommend the City Council:

- A. Send a proposed Ordinance and zoning code amendments to the Planning and Transportation Commission for review during the summer; and
- B. Change the outdoor cultivation sunset provision in the Ordinance from indefinite to 2018; and
- C. Direct Staff to research maximum delivery size, regulations around delivery vehicle safety and business regulations, and information about sales and/or excise taxes.

MOTION PASSED: 3-0 DuBois absent

The Committee took a break from 7:49 P.M. until 7:56 P.M.

3. Request for Proposals for a Consulting Firm to Assist the City of Palo Alto and Palo Alto Unified School District With Master Planning of the Cubberley Community Center.

MOTION: Council Member Kou moved, seconded by Vice Mayor Kniss to recommend the City Council direct the Community Services Department to release a Request for Proposals (RFP) for a Consulting Firm to assist the City of Palo Alto and Palo Alto Unified School District with master planning of the Cubberley Community Center, including a negotiated cost sharing agreement.

INCORPORATED INTO THE MOTION WITH THE CONSENT OF THE MAKER AND THE SECONDER to add to the Motion "and that the negotiation will not cause a delay to the RFP."

MOTION RESTATED: Council Member Kou moved, seconded by Vice Mayor Kniss to recommend the City Council direct the Community Services Department to release a Request for Proposals for a Consulting Firm to assist the City of Palo Alto and Palo Alto Unified School District with master planning of the Cubberley Community Center, including a negotiated cost

ACTION MINUTES

sharing agreement, and that the negotiation will not cause a delay to the RFP.

MOTION PASSED: 3-0 DuBois absent

4. Staff Recommendation That the Policy and Services Committee Recommend the City Council Accept the Status Update of the Audit for Contract Oversight: Trenching and Installation of Electric Substructure.

MOTION: Vice Mayor Kniss moved, seconded by Council Member Kou to recommend the City Council accept the Status of Audit Recommendations for the Contract Oversight: Trenching and Installation of Electric Substructure Audit.

MOTION PASSED: 3-0 DuBois absent

5. Utilities Department: Cross Bore Inspection Contract Audit.

MOTION: Vice Mayor Kniss, seconded by Chair Wolbach to recommend the City Council accept the Utilities Department: Cross Bore Inspection Contract Audit.

MOTION PASSED: 3-0 DuBois absent

Future Meetings and Agendas

ADJOURNMENT: Meeting was adjourned at 9:03 P.M.



City of Palo Alto

Policy and Services Committee Staff Report

(ID # 8180)

Report Type: Action Items**Meeting Date: 6/13/2017****Summary Title: City Ordinance on Surveillance Technologies****Title: Consideration of a City Ordinance Protecting Personal Privacy in the Acquisition and Use of Surveillance Technologies by the City****From: City Manager****Lead Department: City Manager****Recommendation**

Staff recommends the Policy & Services Committee discuss and recommend City Council adoption of an ordinance establishing criteria and procedures for protecting personal privacy when considering the acquisition and use of surveillance technologies by the City.

(Staff will return to Council after the Council break with an actual ordinance, following Council direction and approval on this Action Item).

Background

In April 2016, Councilmembers Wolbach, Berman and Scharff presented a Colleagues Memo to City Council proposing the adoption of a City Policy or Ordinance to increase transparency and oversight in the acquisition and deployment of surveillance technologies (Attachment A). At the April 25, 2016 Council Meeting, Council voted to refer this Colleagues Memo to the Policy and Services Committee to discuss and potentially make recommendations to Council, with a focus on technology that collects personally identifiable information.

In December 2016, City staff presented to the Policy and Services Committee research and in depth information on current surveillance technologies used within the City and outlined some methods other governmental agencies are using to balance transparency, innovation and public safety through the pursuit of smart city strategies. The Committee instructed staff to return to Policy and Services Committee with a potential ordinance that would establish department policies and practices in order to reinforce the protection of individual privacy. (Attachment B)

Discussion

Personally Identifiable Information as defined by the U.S. Department of Labor is, “any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.” As new

technologies emerge the City seeks to reaffirm the commitment to the privacy rights of its residents and community members by establishing an ordinance that will increase City Council Oversight and Transparency in the purchase and use of surveillance technologies.

City Staff have reviewed the landscape of laws and policies in place regarding surveillance technologies purchased and used by government agencies, and sought feedback from stakeholders. This led to the comprehensive information provided to the Policy & Service Committee in December. Informal feedback on this report indicated that a narrower focus would be preferable as a next step.

Given this, staff recommends an ordinance that focuses on the primary technologies of concern today, and allows for the inclusion of new surveillance technologies that may be developed in the future. This approach establishes reporting and approval processes that can increase transparency without compromising public safety, limiting local control, or requiring additional resources.

Proposed Ordinance Tenets

Defining Surveillance Technology: The breadth of what is considered surveillance technology under the ordinance will dictate the frequency of requests to Council and resources required to comply with reporting and approval tenets. Staff recommends a measured approach as a starting point from which to build. The following definition has been developed by the City Attorney to focus on current technologies and builds in flexibility as new technologies emerge.

“Surveillance Technology” means any device or system primarily designed and actually used or intended to be used to collect and retain audio, electronic, visual, location, or similar information associated with any specific individual or group of specific individuals, for the purpose of tracking, monitoring or analysis associated with that individual or group of individuals. Examples of surveillance technology include, but are not limited to, drones with cameras or monitoring capabilities, automated license plate readers, closed-circuit cameras/televisions, cell-site simulators, biometrics-identification technology, and facial-recognition technology.

Explicit Council Authorization: Any purchase or contractual agreement for use of surveillance technology, no matter the cost, would require prior City Council authorization. This ensures that even low-cost technology is given thorough review prior to the City purchase or deploying.

Public Oversight: Staff reports requesting authorization will be placed on the Council agenda to ensure public awareness and Council oversight. Reports will at a minimum include:

- a detailed description of the technology with an explanation of how it works and what information it captures;
- statutory and/or regulatory, rules governing use of the technology;

- measures that will be taken to protect private information;
- how data will be managed and retained; and,
- Existing and/or recommended City administrative policies and procedures regarding use of the technology and the information it produces.

Transparency and Ongoing Oversight: To continue oversight of the City's use of surveillance technology after the initial authorization, a report will be submitted to City Council annually.

This report will include:

- identification of the technology and date of City Council authorization;
- department(s) utilizing the technology;
- frequency of deployment during the year; and,
- purpose and outcome of the deployments.

These reports will be made easily accessible to reinforce transparency.

Potential Alternatives

It should be noted that examples provided by advocates for City Council adoption of an ordinance were significantly more elaborate than the ordinance proposed by staff. The alternatives would likely require significantly greater analysis on a broader and somewhat open-ended range of technologies. Staff also noted that the examples were designed to provide direction to individual departments, which would be more applicability within a county government structure than a council-manager structure. If the Council wished to reinforce direction to individual departments, an administrative policies and procedures format would be more appropriate.

Staff recommends that the Committee consider and provide direction on the elements of a proposed ordinance. Staff will use this feedback to return with a drafted ordinance for adoption.

Attachments:

- Attachment A_ID# 6876 Colleagues Memo
- ATTACHMENT B_12-14-16 P&S Final Action Minutes



City of Palo Alto

COLLEAGUES MEMO

DATE: April 25, 2016

TO: City Council Members

FROM: Council Member Berman, Vice Mayor Scharff, Council Member Schmid, Council Member Wolbach

SUBJECT: COLLEAGUES MEMO: DEVELOPING CITY POLICY ON ACQUISITION, USE, AND SAFEGUARDS FOR SURVEILLANCE AND INFORMATION-GATHERING TECHNOLOGIES

SUMMARY

In order to maintain public trust, ensure protection of privacy, and provide clarity for city staff, Palo Alto should proactively adopt an ordinance establishing a general policy governing consideration, adoption, and use of surveillance and information-gathering technologies by city departments, contractors, or partners.

RECOMMENDATION

We recommend the City Council refer this memo to the Policy and Services Committee to discuss (supported by appropriate staff) creation of an ordinance or other policy governing surveillance and information-gathering technology. Such an ordinance would establish a standard operating procedure (SOP) to be utilized prior to adoption or re-purposing of any technology for potential surveillance applications by City departments, contractors, or partners, as well as prior to seeking funding for such technologies. In addition, the ordinance would require annual reporting on uses of such technologies by the City. Policy and Services should consider the following:

1. Whether and when public hearings and other community engagement are appropriate prior to adoption of surveillance technology by the City, contractor, or partner;
2. The mechanism for Council approval prior to adoption of, re-purposing of, or seeking funding for surveillance technology;
3. Information, such as a Surveillance Impact Report or statement in a City Manager's Report, to be prepared by staff prior to approval which would include information on operations and management; data use; data minimization and limitation; secure data storage and transmission; data access; data retention; data sharing; handling of Public Records Act requests and any individualized policy recommendations;
4. The requirements of federal, state and local laws, regulations and programs that protect and/or regulate gathering, access, retention and use of personally identifiable information and surveillance technology (such as HIPPA, PCII, PII, VISA, VMS, PRA and

- Records Retention). The Committee should survey the existing field of regulation as part of its preparation for developing new regulations;
5. Measures to accommodate community interests in smart city initiatives and other innovations, data-gathering to support planning efforts and other policy development, use of technology to facilitate access to City services and programs, security of persons and property, and cost efficiency, to strike the right balance for Palo Alto;
 6. Information sharing between jurisdictions; and
 7. What type of oversight, evaluation, auditing, or enforcement are appropriate.

For further discussion of possible components, see the model ordinance by the American Civil Liberties Union (Attachment A, pages 22-25) and recommendations by the International Association of Chiefs of Police (Attachment B, pages 3-7).

BACKGROUND

Technology

Examples of technology with surveillance applications include but are not limited to: automated license plate readers (ALPRs), image and video recording, audio recording, unmanned aerial vehicles (aka "drones"), voice recognition, facial recognition, gait analysis, location tracking, automated social media monitoring, cell phone interceptors / cell phone tower emulators (international mobile subscriber identity catchers "IMSI", e.g. Stingrays), electronic communication surveillance (e.g. internet and phone interception), hacking, and data mining.

Palo Alto

Palo Alto currently uses audio recording, cameras in police vehicles, body-worn cameras for police officers, and received one ALPR through a County grant. The Council also recently (October 5, 2015) approved a contract to deploy low resolution cameras to count pedestrian and bicycle traffic (the City Manager added a privacy clause to the contract). For video recording in particular, Palo Alto has a staff-written policy that was revised as recently as January 2015. (See Attachment E).

Other Cities

Other municipalities around the state (see Attachment C) and country have adopted various other technologies, often without notification to the public or elected officials, and without robust policies governing data protection, data access, and data retention. Boston, it was recently revealed, collected ALPR data (tracking residents' locations) which was stored online and accessible by the public. Alameda, CA, recently adopted a policy for Stingrays which was transparent, and well received by privacy advocates and the community as a good example.

County

Santa Clara County recently rejected adoption of Stingray cell phone interceptors after concerns raised by Supervisor Joe Simitian, in particular due to concerns about transparency. (See attachment D). Santa Clara County is currently considering an ordinance governing surveillance technology use by county agencies.

State

In 2015, Governor Jerry Brown signed several bills regarding privacy and modern technology. Two by Senator Jerry Hill deal with ALPRs (SB 34) and cell phone interceptors (SB 741). SB 178 by Senators Mark Leno and Joel Anderson requires a warrant prior to searching cell phones, emails, etc. AB 856 by Assemblymember Ian Calderon restricts use of drones over private property. AB 1116 by Assemblymember Mike Gatto restricts uses of voice recordings by private companies.

Federal

The Northern California Regional Intelligence Center (aka NCRIC or Fusion Center) in San Francisco links local surveillance with federal, raising concerns for residents about how data collected by local agencies will be shared with federal agencies. Federal intelligence, military, and law enforcement have been the subject of much controversy regarding surveillance technology - the nature, adoption, use, security, and legal justification of which have been questioned.

DISCUSSION

Law enforcement and government depend on the trust of the community. Use of technologies which has the appearance, potential, or effect of violating privacy or civil liberties can diminish community trust in government, particularly when adopted and used without transparency. The City's contracting processes include security and other requirements for data and personal information, and the City has a video management procedure that applies to visual information gathering, such as at sensitive utility infrastructure facilities, public garages, etc.

Rapidly evolving surveillance technology raises concerns for the City including, but not limited to: privacy of residents and visitors; chilling effects on expression, research, travel, association, or other rights; misuse of data; data breach (access by unauthorized parties); and adoption, use, or expansion of capabilities without Council oversight.

Rather than attempt to predict or react to each piece of emerging technology, the proposed ordinance would proactively establish a high level policy to be followed prior to the City (or contractor or partner) seeking funding, adopting, or re-purposing any specific technology. This standard operating procedure would provide clarity and predictability for City departments, the City Council, and the community.

As technology advances in coming years, our Police Department in particular will benefit from the confidence of our community that such technologies will only be adopted and utilized in a transparent and responsible manner with clear oversight by the elected City Council and the public to whom they are accountable.

Staff Impact

Resources from the following departments will be needed to support a policy discussion in Policy & Services: Information Technology, Police Department, Planning & Community

Environment, Utilities, Public Works, Emergency Services, City Manager's Office, City Clerk's Office and City Attorney's Office.

Depending on its breadth and specific requirements, significant staff resources may be needed to administer and maintain any new program. As a result of the evolving landscape of technology and security threads, privacy issues and the value of well-conceived policies are not limited to police and public safety activities alone. Utilities, for example, are increasingly working with data that can be sensitive for customers, and this sensitivity will increase with the roll-out of smart meter and smart grid technologies. Similarly, the capability of traffic and parking technologies to collect granular data presents another opportunity to examine the need for balancing data analytics and privacy priorities, while advancing the City's smart city initiatives.

Staff is not suggesting that these issues be overlooked. To the contrary, this may be a topic in which Palo Alto is uniquely positioned to demonstrate leadership in thoughtful stakeholder engagement and policy development. It should be recognized, however, that this effort may be a significant undertaking requiring consummate resources and prioritization to address effectively.



MAKING
SMART
DECISIONS
ABOUT
SURVEILLANCE

A GUIDE FOR
COMMUNITIES

FROM THE ACLU
OF CALIFORNIA

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

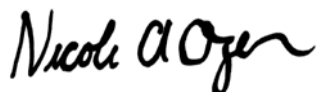
But surveillance can be both less effective and far more costly to local agencies and to the community at large than initially imagined, leaving communities saddled with long-term bills for surveillance that doesn't end up making the community safer. Surveillance can also be easily misused, leading to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

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

Instead, leaders and residents want to know when and why surveillance is being considered, what it is intended to do, and what it will really cost — both in dollars and in individual rights — before taking any steps to seek funding or acquire or deploy surveillance technology. They also want to craft robust rules to ensure proper use, oversight, and accountability if surveillance is used. Unfortunately, few resources exist to help communities make thoughtful decisions about surveillance. That's where this document comes in.

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

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



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



Peter Bibring
Police Practices Director
ACLU of California

CONTENTS

Technology Overview	2
Key Questions to Answer Before Moving Forward with Any Surveillance Proposal	3
Why It Matters: The Costs and Consequences of Surveillance	4
Surveillance Carries Both Immediate and Ongoing Financial Costs.....	4
Surveillance Carries Costs for the Community as a Whole	5
Surveillance Faces Increased Scrutiny from Public Officials.....	7
Key Steps when Considering a Surveillance Proposal	9
Collectively Evaluate the Effectiveness, Costs, and Alternatives Before Making Decisions about Surveillance	9
Establish a Surveillance Technology Use Policy to Mitigate Harms and Protect Rights ..	15
Ensure Accountability by Enforcing Policies and Encouraging Ongoing Public Engagement	19
Conclusion	21
Appendix: Model Surveillance & Community Safety Ordinance	22
Endnotes	216

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

Contributing Writers: Addison Litton & Thomas Mann Miller

Design & Layout: Gigi Pandian & Daniela Bernstein

Printing: InkWorks Press

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

**PUBLISHED BY THE ACLU OF CALIFORNIA
NOVEMBER 2014**

TECHNOLOGY OVERVIEW

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

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

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

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

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

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

AUTOMATED SOCIAL MEDIA MONITORING: Software tools that 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

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

A. SURVEILLANCE CARRIES BOTH IMMEDIATE AND ONGOING FINANCIAL COSTS

The fiscal impact of surveillance can far exceed initial purchase prices for equipment. Modifying current infrastructure, operating and maintaining systems, and training staff can consume limited time and money even if federal or state grants fund initial costs.¹ Surveillance technologies may also fail or be misused, resulting in costly lawsuits. Looking beyond the sticker price is essential.

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

The hidden costs of infrastructure, training and staffing, operations, and maintenance can dwarf the cost of acquiring surveillance technology in the first place. Communities that have failed to accurately estimate the full financial cost of a surveillance system have dealt with massive cost overruns and programs that fail to

“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 Department²

accomplish their stated purpose. For example, Philadelphia planned to spend \$651,672 for a video surveillance program featuring 216 cameras. Instead, it spent \$13.9 million on the project and wound up with only 102 functional cameras after a year, a result the city controller described as “exceedingly alarming, and outright excessive — especially when \$13.9 million is equivalent to the cost of putting 200 new police recruits on our streets.”³ To avoid a similar incident in your community, it is essential to identify all of the costs required to install, use, and maintain surveillance technology before making a decision about whether to do so.

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

Surveillance can carry a number of legal risks. Programs that fail to include proper safeguards for freedom of expression, association, and religion, or that inadequately enforce such safeguards, can lead to expensive litigation. For example, Muslim residents in Orange County filed a discrimination lawsuit when it was revealed that state agents were sending informants into mosques to collect information on the identities and activities of worshippers.⁴ Even technical glitches can create the potential for costly lawsuits and other expenses: the City of San Francisco is still embroiled in a multi-year civil rights lawsuit after wrongly pulling over, handcuffing, and holding at gunpoint an innocent woman due to an error by its ALPR system.⁵

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

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

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

3. FUNDS SPENT ON SURVEILLANCE MAY BE WASTED DUE TO COMMUNITY BACKLASH

Failing to thoroughly discuss surveillance proposals and listen to community concerns early in the process can result in massive backlash and wasted time and funds when plans have to be suspended or even cancelled.

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

Renee Domingo, Oakland Emergency Services Coordinator⁸

Oakland was forced to scrap most of the planning for its Domain Awareness Center and scale the project back considerably after community members protested the misleading mission statement and lack of transparency for the project.⁹ Engaging with the

community before deciding whether to go forward with a surveillance proposal can help your community avoid a similar mistake.

B. SURVEILLANCE CARRIES COSTS FOR THE COMMUNITY AS A WHOLE

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

1. SURVEILLANCE CAN INTRUDE UPON COMMUNITY MEMBERS’ RIGHTS

Unfortunately, there are many examples demonstrating how readily surveillance can be misused to target individuals based on their associations or religious or political activities. Police in Santa Clara used a GPS device to track a student due to his father’s association with the local Muslim Community Association.¹¹ Police in Michigan sought “information on all the cell phones that were congregating in an area where a labor-union protest was expected.”¹² The NSA specifically monitored the email of several prominent Muslim-Americans with no evidence whatsoever of wrongdoing.¹³ And in Germany, drones that were supposed to be used only for traffic monitoring and for serious kidnapping situations were later used to monitor an anti-nuclear protest.¹⁴

“It is essential that big data analysis conducted by law enforcement outside the context of predicated criminal investigations be deployed with appropriate protections for individual privacy and civil liberties. The presumption of innocence is the bedrock of the American criminal justice system. To prevent chilling effects to Constitutional rights of free speech and association, the public must be aware of the existence, operation, and efficacy of such programs.”

- Big Data: Seizing Opportunities, Preserving Values (White House Report)¹⁵

Surveillance programs that do not focus on individual targets can be particularly problematic. “Dragnet” surveillance of the entire public creates the potential for all sorts of abuse, from NSA analysts tracking romantic partners¹⁶ to a Washington, D.C. police lieutenant blackmailing patrons of a gay bar.¹⁷ And surveillance targeted at specific groups, such as members of a religious congregation or attendees at a political rally or gun show, can discourage participation in community activities and alienate the group from the rest of

the community. Even if specific members of the group are legitimate targets of investigation, tracking the entire group extends “guilt by association” to those who have done nothing wrong. And once members of the group are tainted with such suspicion, it becomes easy to justify prying into their private lives, or even threatening them with further consequences, such as placement on the No-Fly List, if they do not cooperate with additional surveillance efforts.¹⁸

SURVEILLANCE AND POLITICAL ACTIVISM

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

- o The California Office of Homeland Security collected detailed information about political demonstrations, including a rally outside a Canadian consulate office in San Francisco to protest seal hunting, a demonstration in Walnut Creek at which government officials spoke against the war in Iraq, and a Women’s International League for Peace and Freedom gathering at a courthouse in support of a 56-year-old Salinas woman facing federal trespassing charges.¹⁹
- o Local police have monitored peaceful political events, including a Code Pink antiwar protest on Mother’s Day²⁰ and even a lecture on veganism at Cal State Fresno.²¹
- o Undercover Oakland police officers infiltrated a group planning a peaceful protest against police brutality and even took a leadership role in directing the course of the march.²²
- o Santa Cruz police officers infiltrated planning meetings for a proposed alternative New Year’s Eve march, leading to a media firestorm and a report from the Santa Cruz police auditor concluding that the department “violated ... [parade] organizers’ rights to privacy, freedom of speech and freedom of assembly.”²³

Intelligence reforms born from lawsuits and congressional inquiries have led many law enforcement agencies to bar the collection of information about political activism and other First Amendment-protected activities without good reason to suspect that a particular individual is or has been involved in criminal activity. There need to be similar restrictions on the use of surveillance technology to ensure that it is not used to chill or undermine political activism.

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

Surveillance carries privacy and free speech threats even if it is conducted solely in public places. This is particularly true when surveillance information is aggregated to build a robust data profile that can “reveal much more in combination than any isolated record.”²⁵ As Supreme Court Justice Sonia Sotomayor has noted, “a precise, comprehensive record of a person’s public movements ... reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” In addition, “[a]wareness that the Government may be watching chills associational and expressive freedoms.”²⁶

2. SURVEILLANCE CAN ERODE TRUST IN LAW ENFORCEMENT

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

This fear that surveillance could be used in a discriminatory fashion is well-founded. In the years after the September 11th attacks, the New York Police Department created a secretive intelligence wing that infiltrated Muslim neighborhoods with undercover officers, where they monitored the daily lives and compiled dossiers about Muslim-Americans engaging in constitutionally protected activities in cafes, bookstores, and private residences with no evidence of illegal activity.²⁸ And in Britain, where video surveillance is pervasive, a European Parliament study showed that “the young, the male and the black were systematically and disproportionately targeted, not because of their involvement in crime or disorder, but for ‘no obvious reason.’”²⁹ Acquiring and using surveillance technologies without recognizing these concerns can reinforce distrust of law enforcement, hindering rather than aiding the protection of public safety.

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

C. SURVEILLANCE FACES INCREASED SCRUTINY FROM PUBLIC OFFICIALS

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

One of the most dramatic shifts in the legal landscape has been an increasing recognition that legal protections for individual rights must take into account the impact of modern technology. As a result, a majority of the Supreme Court has suggested that using technology to track an individual’s location — even in public — over an extended period of time triggers constitutional scrutiny.³¹ Similarly, a federal judge declared the NSA’s warrantless collection of telephone metadata unconstitutional, criticizing its “almost Orwellian” scope.³² Surveillance programs that fail to account for this trend may well be held unconstitutional, and criminal investigations based on evidence from those programs could be jeopardized.

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

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

The California Constitution is even more protective of community members' privacy, including in public spaces. The state right to privacy expressly gives Californians a legal and enforceable "right to be left alone" that protects interests in privacy beyond the home.³⁴ The California Supreme Court has held that covertly "infiltrating" and monitoring the activities of students and professors at classes and public meetings without any indication of criminal activity violated the California Constitution,³⁵ as did warrantless aerial surveillance of a resident's backyard.³⁶ Californians' right to free expression also extends outside of the home, even to privately-owned areas like shopping centers.³⁷

There are also bipartisan legislative efforts to rein in surveillance at the federal and state level. Federal lawmakers are evaluating proposals aimed at reining in the NSA³⁸ and updating the Electronic Communications Privacy Act.³⁹ As of October 2014, 6 states have enacted laws restricting law enforcement access to location information, with 14 other states considering similar legislation.⁴⁰ 43 states have introduced legislation aimed at curbing the use of drones for surveillance purposes.⁴¹ And in communities from Menlo Park to Seattle, local ordinances are placing specific restrictions on the use of surveillance technologies.⁴²

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

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

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

Key Steps when Considering a Surveillance Proposal

Surveillance can end up being very costly, both in dollars and in personal freedom. That’s why it is essential to publicly and thoroughly evaluate surveillance proposals. The following section will help your community — including public officials, law enforcement and diverse community members — work together to determine whether surveillance really makes sense and put in place robust rules to ensure proper use, oversight and accountability if your community decides to move forward with a surveillance proposal.

The Department of Homeland Security (DHS) Privacy Office and Office for Civil Rights and Civil Liberties issued *CCTV: Developing Privacy Best Practices*, a report that encourages government agencies to build privacy, civil rights, and civil liberties considerations into the design, acquisition, and operations of video surveillance systems. An appendix highlights the need to follow the Fair Information Practice Principles of Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability, and Auditing.⁴³

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

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

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

The best way to consider whether surveillance is the right choice and avoid costly mistakes is to engage the entire community — including law enforcement, local lawmakers, and members of the public — in a thorough discussion about any surveillance proposal. Different segments of your community are likely to bring valuable perspectives to the process of evaluating whether to acquire and use surveillance technology. And the time to engage with your community is at the very beginning of the process, *before* any funding is sought, technology is acquired or system is used.

“We need to have discussions with the public about new technologies and the robust privacy policies adopted to protect privacy. This lessens the pushback we get [and] benefits us in the long run.”

Chief Art Acevedo, Austin (TX) Police Department⁴⁴

➤ How is the community engaged in an informed debate about a surveillance proposal?

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

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

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

In 2013 the City of Oakland tried to expand its "Domain Awareness Center," originally focused on the Port of Oakland, into a citywide surveillance network linking together video cameras from local streets and schools, traffic cameras, and gunshot microphones. Instead of soliciting early public input about the expanded system, Oakland tried to move forward without any meaningful engagement with the community. Residents were outraged and the City Council voted against expanding the system.⁴⁵

An informed debate also requires that your community has access to a wide range of information in order to assess how surveillance would work in practice and whether it would advance local goals. Hosting community meetings with various speakers representing different perspectives (not just law enforcement and the technology vendor) can help the community understand how the surveillance technology actually works and its potential implications. Your community should also prepare and release a Surveillance Impact Report to help everyone understand the scope and potential costs of the proposal and a draft Surveillance Use Policy that details the safeguards that would be put in place if the proposal were approved. Your community may also consider convening an ad-hoc committee of local residents, experts and advocates who can work together to make recommendations or help complete these documents.

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

Several cities considering proposals to introduce or expand surveillance have found it useful to actively engage community members through working groups and ad-hoc committees to shape policy and provide oversight. The Redlands Police Department convened a Citizens' Privacy Council, open to any resident of the city, to provide advice on policy for surveillance cameras and oversee police use of the cameras.⁴⁶ Richmond formed an ad-hoc committee to evaluate policies for its video surveillance program.⁴⁷ And in 2014, following community backlash and the vote not to expand Oakland's Domain Awareness Center, the City Council created a Privacy and Data Retention Ad Hoc Advisory Committee comprised of diverse community members to create safeguards to protect privacy rights and prevent the misuse of data for a scaled-back system to be used at the Port of Oakland.⁴⁸

USE A SURVEILLANCE IMPACT REPORT TO MAKE AN INFORMED DECISION

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

- 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/smartabouts-surveillance.

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

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

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

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

San Jose residents were outraged when they learned that their police department had purchased a drone without any public debate. Amid critical media coverage and protests from community groups, civil-rights advocates, and local residents, police apologized and said they would ground the drone until they could conduct adequate public outreach.⁴⁹

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

Your community cannot determine whether surveillance is an appropriate solution if you have not first identified the problem. Defining the specific purpose or issues that surveillance is intended to address is essential to evaluate the likely effectiveness of surveillance and to identify alternatives that might provide a better fit for your needs and budget. It can help highlight the individuals or communities who are likely to be most impacted by surveillance and ensure that their thoughts and concerns are fully understood. It also

provides a starting point for crafting a Surveillance Use Policy by defining specific objectives for which surveillance is appropriate and barring its use outside of those purposes.

SURVEILLANCE AT THE “BORDER”

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

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

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

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

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

CASE STUDY: OAKLAND SPENDS \$2M ON “HARDLY-USED” POLICE TECHNOLOGY

The cash-strapped city of Oakland learned the hard way that acquiring new police technology without a clearly-defined purpose can be a waste of time and money. A city audit revealed that the city had squandered almost \$2 million on hardly-used police technology between 2006 and 2011. The auditor recommended steps to ensure that technology purchases were intended to fulfil specific strategic objectives and regular evaluation of their effectiveness.⁵¹

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

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

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

In 2005, San Francisco set out to deter violent crime and provide police with an investigative tool by installing video cameras in the City's high-crime, high-traffic areas. However, post-installation crime statistics published by mandate under a city ordinance revealed that the cameras neither reduced crime nor assisted in solving them in any meaningful way. In fact, the cameras only led to six suspects being charged by the SFPD between 2005 and 2008. As a result, the Police Commission reconsidered its plans to expand the program.⁵²

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

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

In particular, you should compare the effectiveness and costs of technology-based solutions with non-technology-oriented approaches to address the problem. For example, multiple studies have shown that traditional approaches such as increased lighting and foot patrols significantly reduce crime.⁵³ You should not automatically assume that surveillance technology will be more effective.

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

California cities are increasingly shutting down red light cameras as evidence mounts that the cameras increase, rather than decrease, traffic accidents. For example, in Walnut, CA, a study found that red light cameras resulted in dramatic increases in "red light running collisions" (400%), "rear end collisions" (71%) and "broadside collisions" (100%)" and that "no argument can be made that photo enforcement has improved safety . . . within the city of Walnut. In fact, the use of red light cameras appears to have decreased safety and put roadway users at increased risk." In light of this evidence, more than half of the California cities that once used red light cameras have ended their programs, turning instead to alternatives that have proven more effective at preventing accidents such as longer yellow lights at dangerous intersections.⁵⁴

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

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

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

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

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

- Police Executive Research Forum, “How Are Innovations in Technology Affecting Policing?”⁵⁵

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

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

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

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

The FBI had installed approximately 3,000 GPS trackers on cars without a warrant throughout the United States when the U.S. Supreme Court ruled in 2012 that their use implicated the Fourth Amendment.⁵⁶ As a result, the FBI deactivated the warrantless trackers and its agents had to physically retrieve them.⁵⁷ Obtaining warrants before using those GPS trackers would have ensured the constitutionality of obtained evidence and saved the FBI considerable time and effort.

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

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

CASE STUDY: REDLANDS DEPLOYS INSECURE CAMERA NETWORK

The surveillance camera network in the city of Redlands made the news for the wrong reasons when computer security experts demonstrated how easily they could take control of the cameras. Although the police department expressed concern about “people with criminal intent using the public camera feed to case homes or businesses or track the police force,” the network was deployed with no security at all. Even after the story broke, the network was secured with an outdated encryption protocol that a researcher described as “putting a diary lock on your front door.”⁵⁸

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

If after careful consideration and public debate your community decides that a particular surveillance technology is worth adopting, you need to ensure that policies are in place so that it is used properly. A clear, legally enforceable Surveillance Use Policy that provides guidance about when and how to use surveillance can safeguard individual rights while protecting local law enforcement and your entire community from costly lawsuits, bad press, loss of community trust, and more. Recognizing the necessity of use policies, Seattle and Spokane, Washington recently passed ordinances requiring police to develop use guidelines for new surveillance equipment before using it.⁵⁹

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

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

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

1. USE APPROPRIATELY: PLACE CLEAR LIMITS ON SURVEILLANCE

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

➤ *When is surveillance permitted or prohibited?*

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

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

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

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

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

In many cases, the best way to ensure that legal requirements are satisfied is to require a search warrant prior to conducting surveillance, allowing the court system to play a role in overseeing the program. With the streamlined modern warrant process, officers can seek a judge's approval quickly and easily by simply placing a phone call or using a mobile device.⁶¹

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

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

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

“All of our officers receive First and Fourth Amendment training before they're allowed to access the system in any way.”
- Jonathan Lewin, Chicago Police Department Office of Emergency Management and Communications⁶²

➤ *Are you only collecting necessary data?*

Ensuring that surveillance technology is used in a way that accomplishes its stated purpose without collecting additional data is a straightforward way to reduce the risk of privacy invasions. That's why the federal statute authorizing wiretaps has from its inception required “minimization” — an effort to make sure that even after a warrant has issued and collection is underway, police only intercept communications relevant to the investigation, not every communication made by the target.⁶³

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

CASE STUDY: OHIO STATE HIGHWAY PATROL RETAINS ONLY ALPR HITS

The Ohio State Highway Patrol policy for automated license plate readers (ALPRs) states that “all ‘non-hit’ captures shall be deleted immediately.” The ALPR program is intended to detect stolen vehicles, Amber Alerts, and persons with outstanding warrants. As a result, retaining data about “non-hit” vehicles does not further that purpose, and a policy of deleting that data immediately protects the community from unnecessary risks.⁶⁴

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

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

➤ *How will surveillance data be secured?*

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

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

CASE STUDY: MONTEREY COUNTY SUFFERS DATA BREACH DUE TO “TOTALLY OBSOLETE” DATA PRACTICES

Monterey County’s computer systems were breached in 2013 and the personal information of over 140,000 local residents was stolen. A subsequent grand jury investigation concluded that the breach stemmed from “totally obsolete” data practices and a failure to follow privacy laws. The grand jury warned of “serious financial consequences” if the county failed to change its practices.⁶⁵

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

In addition to technical safeguards to protect data, you should also limit the circumstances under which it can be legitimately accessed or used. These limits should be based on the specific purposes your community agreed to when it adopted the technology. For example, if the purpose of the technology is to address specific violent crimes, your policy might allow database searches only as part of an official investigation of a violent crime, and only for data that is related to that investigation. Data access and use

policies that are consistent with the articulated purposes for the system will provide guidance to operators and engender community trust by deterring abuses that can follow unfettered access to surveillance data.

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

CASE STUDY: LAX POLICIES LEAD TO “LOVEINT” ABUSE

Without strong policies limiting access to data, the temptation to misuse the system for personal interests can be hard to resist. The NSA even has a specific term, LOVEINT, for employees who monitor their significant others,⁶⁶ and two Fairfield officers could face criminal charges after using a statewide police database to screen women from online dating sites.⁶⁷

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

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

If data can be shared, your community must also determine how to ensure that the entity receiving the data lives up to your community's standards. This may require contractual language binding the third party to your data policies and safeguards. For example, the city of Menlo Park, California specifically requires by ordinance that any agreement with Northern California's fusion center demand compliance with the City's own retention policy.⁶⁸ If a potential recipient of your data cannot agree with your policies or conditions, the best choice is to not share your data.

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

The longer you retain information, the greater the potential privacy and security risks. The easiest way to minimize these risks is to retain only the information you need and only for as long as you need it.

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

To maximize the usefulness of your technology and minimize civil liberties concerns, your retention period should not be longer than necessary to directly advance community purposes. For instance, deploying automated license plate readers to locate stolen or Amber Alert vehicles is not aided by the collection of historical data. Retaining data “just in case it becomes useful” increases the risk that data will be used contrary to the purpose agreed upon by the community or wind up in the hands of a bad actor. Retaining data can also increase the costs of surveillance by requiring expensive storage solutions and making it harder to effectively use the system. Focusing on the specific objective that surveillance is intended to accomplish can help you determine a retention period that balances that objective with the costs and risks associated with data retention.

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

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

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

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

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

- Commander Steven Caluris, Chicago Police Department⁶⁹

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

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

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

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

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

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

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

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

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

“[A]ll usage is supervised. All camera and operator actions are logged and can be tracked later.”

- Jonathan Lewin, Chicago Police Department Office of Emergency Management and Communications.⁷⁰

CASE STUDY: FRESNO ADOPTS ANNUAL AUDIT OF VIDEO SURVEILLANCE

When the Fresno Police Department proposed a citywide video-policing program using live-feed cameras, the city council required an annual independent audit to ensure that all of the privacy and security guidelines for the system’s use are being followed. Fresno Police Chief Jerry Dyer said he supported the audit: “I have no doubt the audit will be very helpful to our ongoing video policing operations.” The city’s auditor, a retired federal district court judge with deep experience on civil rights cases, examined current use of the system and made specific policy recommendations.⁷¹

➤ *What legally enforceable sanctions exist against misuse and abuse of this technology?*

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

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

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

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

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

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

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

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

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

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

Conclusion

Communities increasingly understand the need to make smart choices about surveillance technology and ensure that time, energy, and resources are not spent on systems that cost more, do less, and have a greater impact on the rights of community members than you expect. And following public outcry about NSA spying and the use of military equipment by local police, community members demand — and deserve — both a voice in any decision to deploy surveillance technology and reassurance that robust safeguards and public oversight will be in place if surveillance is going to be used. Make sure that your entire community is engaged in asking and answering the right questions about surveillance technology by adopting a Surveillance & Community Safety Ordinance and following the other recommendations in this guide.

Appendix: Model Surveillance & Community Safety Ordinance

A. KEY PRINCIPLES OF THE MODEL ORDINANCE

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

B. MODEL ORDINANCE TEXT

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

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

Section 1. Title

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

Section 2. [Council/Board] Approval Requirement

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

Section 3. Information Required

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

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

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

Section 5. Compliance for Existing Surveillance Technology

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

Section 6. Oversight Following [Council/Board] Approval

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

Section 7. Definitions

The following definitions apply to this Ordinance:

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

- d. The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
 - e. Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - f. Statistics and information about public records act requests, including response rates; and
 - g. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.
- 2) “[City/County] entity” means any department, bureau, division, or unit of the [City/County].
 - 3) “Surveillance technology” means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group.
 - 4) “Surveillance Impact Report” means a publicly-released written report including at a minimum the following: (a) Information describing the surveillance technology and how it works, including product descriptions from manufacturers; (b) information on the proposed 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) for the surveillance technology.
 - 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 identifying personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy

Section 8. Enforcement

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

Section 9. Severability

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

Section 10. Effective Date

This Ordinance shall take effect on [DATE].

Endnotes

- ¹ See Darwin Bond Graham & Ali Winston, *The Hidden Costs of Oakland's Surveillance Center*, East Bay Express, Jan. 22, 2014, available at <http://www.eastbayexpress.com/oakland/controversial-the-hidden-costs-of-oaklands-surveillance-center/Content?oid=3816398>; Nancy La Vigne et al., Urban Institute, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention* (2011), available at http://www.cops.usdoj.gov/Publications/e071112381_EvalPublicSurveillance.pdf.
- ² Police Executive Research Forum, *How Are Innovations in Technology Transforming Policing?* 26 (Jan. 2012) [hereinafter PERF Report], available at http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.
- ³ Press Release, Office of the Controller, *Butkowitz Alarmed by Police Camera Program*, June 20, 2012, <http://www.philadelphiacontroller.org/page.asp?id=792>.
- ⁴ See *Fazaga v. FBI*, 844 F.Supp.2d 1022 (C.D. Cal. 2012).
- ⁵ See Tim Cushing, *Another Bogus Hit from a License Plate Reader Results in Another Citizen Surrounded by Cops with Guns Out*, TechDirt (May 23, 2014), <https://www.techdirt.com/articles/20140513/07404127218/another-bogus-hit-license-plate-reader-results-another-citizen-surrounded-cops-with-guns-out.shtml>.
- ⁶ Cal. Civil Code § 1798.29 (2014).
- ⁷ Ponemon Inst. & Symantec, *2011 Cost of Data Breach Study: United States* (2012), available at <http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us-en-us.pdf>.
- ⁸ Symposium, *The Value of Privacy*, U. Cal.-Hastings School of L. Const. L. Q., Apr. 7, 2014 (oral remarks), available at <http://livestre.am/4P7Lk>.
- ⁹ See Will Kane, *Oakland to Limit Surveillance Center to Port, Airport, S.F. Gate*, Mar. 6, 2014, available at <http://www.sfgate.com/bayarea/article/Oakland-to-limit-surveillance-center-to-port-5290273.php>.
- ¹⁰ For example, the San Francisco Police Department's Mission Statement states that "policing strategies must preserve and advance democratic values" and that "police must respect and protect the rights of all citizens as guaranteed by the state's Constitution." Police Department, Mission Statement, <http://sf-police.org/index.aspx?page=1616>.
- ¹¹ Terrence O'Brien, *Caught Spying, FBI Asks Student to Return GPS Tracker*, SWITCHED (Oct. 8, 2010), <http://www.switched.com/2010/10/08/caught-spying-fbi-asks-student-to-return-gps-tracker/>.
- ¹² Michael Isikoff, *FBI Tracks Suspects' Cell Phones Without a Warrant*, Newsweek, Feb. 18, 2010 (updated Mar. 13, 2010), available at <http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099>.
- ¹³ David Kravets, *Rights Groups Decry New NSA Leak: Snooping on Muslim-Americans' E-mail*, Ars Technica (July 9, 2014), <http://arstechnica.com/tech-policy/2014/07/rights-groups-decry-new-nsa-leak-snooping-on-muslim-americans-e-mail/>.
- ¹⁴ Christian Watien, *5 Uses for Drones that Don't Involve Fighting Terrorists*, Epoch Times (Nov. 10, 2012), www.theepochtimes.com/n2/world/5-uses-for-drones-that-don-t-involve-fighting-terrorists-313051-print.html.
- ¹⁵ Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 66 (2014), available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
- ¹⁶ Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, Wash. Post, Aug. 24, 2013, available at <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/>.
- ¹⁷ See Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, Wall St. J., Sep. 29, 2012, available at <http://online.wsj.com/news/articles/SB10000872396390443995604578004723603576296>.
- ¹⁸ See *Tanvir v. Holder*, Case No. 13-CV-6951 (S.D. N.Y. Apr. 22, 2014) (First Amended Complaint), available at <http://apps.washingtonpost.com/g/documents/world/lawsuit-accusing-us-of-putting-people-on-no-fly-list-after-they-say-they-wont-spy/941/>.
- ¹⁹ Peter Nicholas, *State Tracked Protesters in the Name of Security*, L.A. Times, July 1, 2006, available at <http://articles.latimes.com/2006/jul/01/local/me-security1..>
- ²⁰ Camille T. Taiara, *Monitoring Malcontents: Why Do the Governor's Critics Keep Findings Themselves Targets of Strange Police Scrutiny?*, S.F. Bay Guardian, http://www.sfbg.com/39/41/news_governator.html.
- ²¹ See Mike Rhodes, *Students at CSUF Are Starving for Civil Liberties*, Indybay (Apr. 27, 2005), <https://www.indybay.org/newsitems/2005/04/27/17351181.php>.
- ²² *Local 10 ILWU v. City of Oakland*, No. 3:03-cv-02962 (N.D. Cal. Apr. 28, 2005) (Jordan Dep. at 24:11-24).
- ²³ See Bradley, *Santa Cruzans Speak Out Against Police Infiltration and for an Independent Investigation*, Indybay (Jan. 25, 2006), <https://www.indybay.org/newsitems/2006/01/25/17981451.php>.
- ²⁴ Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (March 24, 2014), <http://ssrn.com/abstract=2412564>.
- ²⁵ *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

- ²⁶ United States v. Jones, 132 S.Ct. 945, 955, 56 (2012).
- ²⁷ Angel Jennings, Richard Winston & James Rainey, *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>.
- ²⁸ Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, Huffington Post (Feb 25, 2012), http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html; Adam Goldman & Matt Apuzzo, *New York Drops Unit That Spied on Muslims*, N.Y. Times, April 15, 2014, available at <http://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html>.
- ²⁹ European Parliament Directorate General Internal Policies, *A Review of the Increased Used of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe* 15 (2009).
- ³⁰ See Press Release, Leadership Conference, *Civil Rights Principles for the Era of Big Data*, <http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html>.
- ³¹ U.S. v. Jones, 132 S.Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, Ginsberg, Breyer, and Kagan, J., concurring in the judgment).
- ³² Klayman v. Obama, Civ. No. 13-0851 (D.D.C. Dec. 16, 2013).
- ³³ U.S. v. Jones, 132 S.Ct. at 956 (quoting U.S. v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).
- ³⁴ Ballot Pamphlet., Proposed Amendments to Cal. Const. with Arguments to Voters, Gen. Elec. (Nov. 7, 1972).
- ³⁵ White v. Davis, 533 P.2d (Cal. 1975).
- ³⁶ People v. Cook 41 Cal. 3d 373 (1985).
- ³⁷ Robins v. Pruneyard Shopping Center, 592 P.2d 899 (Cal. 1979) (holding that, under the California Constitution, members of the public have a legal right to pass out pamphlets and seek signatures in a privately-owned shopping center), *aff'd*, 447 U.S. 74 (1980).
- ³⁸ U.S.A. Freedom Act, H.R. 3361, 113th Cong. (2013).
- ³⁹ Email Privacy Act, H.R. 1852, 113th Cong. (2013).
- ⁴⁰ Allie Bohm, *Status of Location Privacy Legislation in the States*, ACLU Free Future (April 8, 2014), <https://www.aclu.org/blog/technology-and-liberty-national-security/status-location-privacy-legislation-states> (as of May 6, 2014).
- ⁴¹ Allie Bohm, *Status of 2014 Domestic Drone Legislation in the States*, ACLU Free Future (April 22, 2014), <https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states> (as of May 6, 2014).
- ⁴² See Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, available at http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approves-ordinance-regulating-police-use; *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), <http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/>.
- ⁴³ U.S. Dep't of Homeland Security, *CCTV: Developing Best Practices* (2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.
- ⁴⁴ PERF Report, *supra* note 2, at 35.
- ⁴⁵ Ali Winston, *Oakland City Council Rolls Back the Domain Awareness Center*, East Bay Express (Mar. 5, 2014), <http://www.eastbayexpress.com/SevenDays/archives/2014/03/05/oakland-city-council-rolls-back-the-dac>.
- ⁴⁶ Redlands Police Department, *Citizen Privacy Council*, <http://www.cityofredlands.org/police/CPC>.
- ⁴⁷ Memorandum, *Establishing Ad Hoc Committee to Review the Community Warning System and Industrial Safety Ordinance* (Sept. 18, 2012), http://64.166.146.155/agenda_publish.cfm?mt=ALL&get_month=9&get_year=2012&dsp=agm&seq=12339&rev=0&ag=241&ln=23604&nscq=0&nrev=0&pseq=12303&prev=0.
- ⁴⁸ See Memorandum, *City Administrator's Weekly Report* (Apr. 25, 2014), <http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak046804.pdf>.
- ⁴⁹ Robert Salonga, *San Jose: Police Apologize for Drone Secrecy, Promise Transparency*, San Jose Mercury News, Aug 5, 2014, available at http://www.mercurynews.com/crime-courts/ci_26279254/san-jose-police-apologize-secret-drone-purchase-promise.
- ⁵⁰ See ACLU, *Know Your Rights: The Government's 100-Mile "Border" Zone — Map*, <https://www.aclu.org/know-your-rights-governments-100-mile-border-zone-map>.
- ⁵¹ See Oakland City Auditor, *Police Technology Performance Audit: FY 2006–07 through 2010–11* (2012), available at <http://www.oaklandauditor.com/images/oakland/auditreports/0pd%20tech.pdf>.
- ⁵² See Citris, *Citris Study on SF Public Cameras Released* (Jan. 9, 2009), <http://citris-uc.org/citris-study-on-sf-public-cameras-released/>.

- ⁵³ See David P. Farrington & Brandon C. Welsh, *Effects of Improved Street Lighting on Crime: A Systematic Review*, Home Office Research Study 251 (Aug. 2002), p. 42; Ronald V. Clarke, U.S. Department of Justice, Office of Community Oriented Policing Services, *Improving Street Lighting to Reduce Crime in Residential Areas* (Dec. 2008), available at <http://cops.usdoj.gov/Publications/e1208-StreetLighting.pdf>; Jay Beeber, *Collision Analysis of the Photo Enforced Intersection in Walnut, CA*, <http://www.thenewspaper.com/rlc/docs/2014/ca-walnut.pdf>.
- ⁵⁴ See Steve Scauzillo, *Red Light Cameras Being Stopped*, L.A. Daily News. (Jan. 21, 2014), <http://www.dailynews.com/general-news/20140121/red-light-cameras-being-stopped>.
- ⁵⁵ PERF Report, *supra* note 2, at 44.
- ⁵⁶ *United States v. Jones*, 132 S. Ct. 945 (2012).
- ⁵⁷ Joann Pan, *FBI Turns Off 3000 GPS Devices After Ruling*, Mashable (Feb. 27, 2012), <http://mashable.com/2012/02/27/fbi-turns-off-3000-gps-devices/>.
- ⁵⁸ Kashmir Hill, *Whoops, Anyone Could Watch California City's Police Surveillance Cameras*, Forbes.com (Aug. 21, 2014), <http://www.forbes.com/sites/kashmirhill/2014/08/11/surveillance-cameras-for-all/>.
- ⁵⁹ *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), <http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/>; Jamela Debelak, ACLU of Washington, *Surveillance: Spokane Acts to Protect Privacy and Provide Transparency* (Aug. 21, 2013), <https://aclu-wa.org/blog/surveillance-spokane-acts-protect-privacy-and-provide-transparency>.
- ⁶⁰ Erika Aguilar, *LAPD Body Cameras: 90-Day Test Seeks to Answer Key Questions to Create New Policy*, 89.3 KPCC (Feb. 4, 2014), <http://www.scpr.org/news/2014/02/04/41855/lapd-body-cameras-90-day-test-seeks-to-answer-key/>.
- ⁶¹ Terry McFadden, *Technology Helping Police to Receive Warrants Faster*, WNDU.com (July 8, 2013), <http://www.wndu.com/news/specialreports/headlines/Technology-helping-police-to-receive-search-warrants-faster--214651051.html>.
- ⁶² PERF Report, *supra* note 2, at 14.
- ⁶³ 18 U.S.C. § 2518(5) (2014).
- ⁶⁴ Ohio State Highway Patrol Policy No. OSP-103.29 (revised Dec. 23, 2008).
- ⁶⁵ Julia Reynolds, *Monterey County Grand Jury Finds Computer Data Risks*, Monterey Herald, Aug. 21, 2014, available at http://www.montereyherald.com/news/ci_26009592/monterey-county-grand-jury-finds-computer-data-risks.
- ⁶⁶ Dianne Feinstein, *NSA Officers Spy on Love Interests*, Wall St. J., Aug. 23, 2013, available at <http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/>.
- ⁶⁷ Anjali Hemphill, *Dating on Duty: Officers Accused of Screening Dates Using Police System*, CBS 13 Sacramento (Aug. 22, 2014), <http://sacramento.cbslocal.com/2014/08/22/dating-on-duty-officers-accused-of-screening-dates-using-police-system/>.
- ⁶⁸ See Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, available at http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approves-ordinance-regulating-police-use.
- ⁶⁹ PERF Report, *supra* note 5, at 36.
- ⁷⁰ *Id.* at 14.
- ⁷¹ George Hostetter, *Former Judge Wanger Writes Far-Ranging Audit on Fresno Video Policing*, Fresno Bee, Jan. 7, 2014, available at <http://www.fresnobee.com/2014/01/07/3701754/judge-wanger-delivers-impressive.html>.



IACP TECHNOLOGY POLICY FRAMEWORK¹

January 2014

Introduction

New and emerging technologies increasingly play a crucial role in the daily work of police, equipping officers with enforcement and investigative tools that have the potential of making them safer, better informed, and more effective and efficient. Developing and enforcing comprehensive agency policies regarding deployment and use is a critical step in realizing the value that technologies promise, and is essential in assuring the public that their privacy and civil liberties are recognized and protected.

Technological advances have made it possible to monitor and record nearly every interaction between police and the public through the use of in-car and body-worn video, access to an expanding network of public and private video surveillance systems, and the increasing use of smartphones with digital recording capabilities by citizens and officers alike. Police can track suspects with the use of GPS tracking technologies and officers themselves can be tracked with automated vehicle location (AVL) systems. Automated license plate recognition (ALPR) systems can scan the license plates of vehicles within sight of officers in the field and quickly alert them if the vehicle has been reported stolen or is wanted. Identity can be remotely verified or established with biometric precision using mobile fingerprint scanners and facial recognition software. Crimes can be mapped as they are reported, gunshot detection technology can alert law enforcement almost instantaneously when a firearm is discharged, and surveillance cameras can be programmed to focus in on the gunshot location and stream live video to both dispatchers and responding officers. With these advancements come new opportunities to enhance public and officer safety. They also present new challenges for law enforcement executives.

The challenges include identifying which technologies can be incorporated by the agency to achieve the greatest public safety benefits, and defining metrics that will enable the agency to monitor and assess the value and performance of the technologies. Just because a technology *can* be implemented, does not mean that it *should* be. There are also challenges in integrating these technologies across different platforms, building resilient infrastructure and comprehensive security, providing technical support, and maintaining and upgrading applications and hardware. All of this can be confusing and technically demanding, underscoring the need for effective planning, strategic deployment, and performance management.

Addressing these challenges is paramount because of the broader issues that the use of this expanding array of technologies by law enforcement presents. A principal tenet of policing is the trust citizens grant police to take actions on their behalf. If that trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe.

The Policy Mandate

Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and civil liberties of individuals, as well as the privacy protections afforded to the data collected, stored, and used, is essential to ensure effective and sustainable implementation, and to maintain community trust. Policies function to reinforce training and to establish an operational baseline to guide officers and other personnel in proper procedures regarding its use. Moreover, policies help to ensure uniformity in practice across the agency and to enforce accountability. Policies should reflect the mission and values of the agency and be tightly aligned with applicable local, state, and federal laws, regulations, and judicial rulings.

Policies also function to establish transparency of operations, enabling agencies to allay public fears and misperceptions by providing a framework that ensures responsible use, accountability, and legal and constitutional compliance. The use of automated license plate recognition (ALPR) technologies, unmanned aerial systems, and body-worn video by law enforcement, for example, has generated substantial public discussion, increasing scrutiny, and legislative action in recent years.² Privacy advocates, elected officials, and members of the public have raised important questions about how and under what circumstances these technologies are deployed, for what purposes, and how the data gathered by these technologies are retained, used, and shared. Having and enforcing a strong policy framework enables law enforcement executives to demonstrate responsible planning, implementation, and management.

Agencies should adopt and enforce a technology policy framework that addresses technology objectives, deployment, privacy protections, records management, data quality, systems security, data retention and purging, access and use of stored data, information sharing, accountability, training, and sanctions for non-compliance. Agencies should implement safeguards to ensure that technologies will not be deployed in a manner that could violate civil rights (race, religion, national origin, ethnicity, etc.) or civil liberties (speech, assembly, religious exercise, etc.). The policy framework is but one of several critical components in the larger technology planning effort that agencies should undertake to ensure proper and effective use of automation.

Universal Principles

Given the privacy concerns and sensitivity of personally identifiable information and other data often captured and used by law enforcement agencies,³ and recognizing evolving perceptions of what constitutes a reasonable expectation of privacy,⁴ the

technology policy framework should be anchored in principles universally recognized as essential in a democratic society.

The following universal principles should be viewed as a guide in the development of effective policies for *technologies that can, or have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time, date, and geographic location where the data were captured.*⁵

1. *Specification of Use*—Agencies should define the purpose, objectives, and requirements for implementing specific technologies, and identify the types of data captured, stored, generated, or otherwise produced.
2. *Policies and Procedures*—Agencies should articulate in writing, educate personnel regarding, and enforce agency policies and procedures governing adoption, deployment, use, and access to the technology and the data it provides. These policies and procedures should be reviewed and updated on a regular basis, and whenever the technology or its use, or use of the data it provides significantly changes.
3. *Privacy and Data Quality*—The agency should assess the privacy risks and recognize the privacy interests of all persons, articulate privacy protections in agency policies, and regularly review and evaluate technology deployment, access, use, data sharing, and privacy policies to ensure data quality (i.e., accurate, timely, and complete information) and compliance with local, state, and federal laws, constitutional mandates, policies, and practice.
4. *Data Minimization and Limitation*—The agency should recognize that only those technologies, and only those data, that are strictly needed to accomplish the specific objectives approved by the agency will be deployed, and only for so long as it demonstrates continuing value and alignment with applicable constitutional, legislative, regulatory, judicial, and policy mandates.
5. *Performance Evaluation*—Agencies should regularly monitor and evaluate the performance and value of technologies to determine whether continued deployment and use is warranted on operational, tactical, and technical grounds.
6. *Transparency and Notice*—Agencies should employ open and public communication and decision-making regarding the adoption, deployment, use, and access to technology, the data it provides, and the policies governing its use. When and where appropriate, the decision-making process should also involve governing/oversight bodies, particularly in the procurement process. Agencies should provide notice, when applicable, regarding the deployment and use of technologies, as well as make their privacy policies available to the public. There are practical and legal exceptions to this principle for technologies that are

lawfully deployed in undercover investigations and legitimate, approved covert operations.⁶

7. *Security*—Agencies should develop and implement technical, operational, and policy tools and resources to establish and ensure appropriate security of the technology (including networks and infrastructure) and the data it provides to safeguard against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. This principle includes meeting state and federal security mandates (e.g., the FBI’s CJIS Security Policy⁷), and having procedures in place to respond if a data breach, loss, compromise, or unauthorized disclosure occurs, including whether, how, and when affected persons will be notified, and remedial and corrective actions to be taken.⁸
8. *Data Retention, Access and Use*—Agencies should have a policy that clearly articulates that data collection, retention, access, and use practices are aligned with their strategic and tactical objectives, and that data are retained in conformance with local, state, and/or federal statute/law or retention policies, and only as long as it has a demonstrable, practical value.
9. *Auditing and Accountability*—Agencies and their sworn and civilian employees, contractors, subcontractors, and volunteers should be held accountable for complying with agency, state, and federal policies surrounding the deployment and use of the technology and the data it provides. All access to data derived and/or generated from the use of relevant technologies should be subject to specific authorization and strictly and regularly audited to ensure policy compliance and data integrity. Sanctions for non-compliance should be defined and enforced.

Developing Policies and Operating Procedures

The universal principles provide structural guidance for the development of specific agency policies and operating procedures that comport with established constitutional, legal, and ethical mandates and standards. Agency policies and procedures specify the operational components of each individual technology implementation, deployment, and management, and should typically include and address the following factors:⁹

1. Purpose
 - a. A general discussion of the purpose of a specific agency policy to include the agency’s position on protecting privacy.
2. Policy
 - a. A discussion of the overarching agency policy regarding the deployment and use of a specific technology, its application to members of the agency, and reference to relevant laws, policies, and/or regulations that authorize the agency to implement a technology, or that relate to the use and deployment of a technology.
3. Definitions

- a. A description of the technology, its components, and functions.
 - b. Definitions and acronyms associated with the technology.
4. Management
- a. Strategic Alignment: Describe how the technology aligns and furthers the agency's strategic and tactical deployment objectives.
 - b. Objectives and Performance: Identify objectives for the deployment and conditions for use of a technology, and a general strategy for assessing performance and compliance with the agency's policy.
 - c. Ownership: Clearly specify that the hardware and software associated with the technology is the property of the agency, regardless whether it has been purchased, leased, or acquired as a service, and that all deployments of a technology are for official use only (FOUO). All data captured, stored, generated, or otherwise produced by a technology are the property of the agency, regardless where the data are housed or stored. All access, use, sharing, and dissemination of the data must comply with the policies established and enforced by the agency.
 - d. Classification of Data: Clearly specify the data classification and its level of sensitivity (e.g., top secret, secret, confidential, restricted, unclassified, private, public, etc.), whether the data captured, stored, generated, or otherwise produced by a technology are considered public information, and whether it is subject to applicable public records act requests and under what circumstances.
 - e. Privacy Impact: Develop or adopt and use a formal privacy impact assessment (PIA)¹⁰ or similar agency privacy assessment on technology and the data it captures, stores, generates, or otherwise produces.
5. Operations
- a. Installation, Maintenance, and Support: Require regular maintenance, support, upgrades, calibration, and refreshes of a technology to ensure that it functions properly.
 - b. Deployment: Identify who is authorized to officially approve the deployment and use of a technology, and the conditions necessary for deployment and use, if applicable.
 - c. Training: Require training, and perhaps certification or other documented proficiency, if applicable, of all personnel who will be managing, maintaining, and/or using a technology. Training should also cover privacy protections on the use of the technology, and the impact and sanctions for potential violations.
 - d. Operational Use: Identify specific operational factors that must be addressed in deployment and use of a technology. (For example, for ALPR, the officer should i) verify that the system has correctly "read" the license plate characters; ii) verify the state of issue of the license plate; iii) verify that the "hot list" record that triggered the alert is still active in the state or NCIC stolen vehicle or other file, and confirm the

hit with the entering agency; and iv) recognize that the driver of the vehicle may not be the registered owner).

- e. Recordkeeping: Require recordkeeping practices that document all deployments of the technology, including who authorized the deployment; how, when, and where the technology was deployed; results of deployments; and any exceptions. Recordkeeping will support efforts to properly manage technology implementation, ensure compliance with agency policies, enable transparency of operations, enable appropriate auditing review, and help document business benefits realization.

6. Data Collection, Access, Use, and Retention

- a. Collection: Define what data will be collected, how data will be collected, the frequency of collection, how and where data will be stored, and under what authority and conditions the data may be purged, destroyed, or deleted in compliance with applicable local, state, and/or federal recordkeeping statutes and policies, court orders, etc. Identify the destruction/deletion methods to be used.
- b. Access and Use: Define what constitutes authorized use of data captured, stored, generated, or otherwise produced by a technology. Define who is authorized to approve access and use of the data, for what purposes and under what circumstances.
- c. Information Sharing: Specify whether data captured, stored, generated, or otherwise produced by a technology can be shared with other agencies, under what circumstances, how authorization is provided, how information that is shared is tracked/logged, how use is monitored, and how policy provisions (including privacy) will be managed and enforced. Any agency contributing and/or accessing shared information should be a signatory of a data sharing Memorandum of Understanding (MOU). Dissemination of any shared information should be governed by compliance with applicable state and federal laws, standards, agency privacy policies, and procedures as agreed in the MOU.
- d. Security: Define information systems security requirements of the technology and access to the data to ensure the integrity of the systems and confidentiality of the data. The security policy should address all state and federal mandated security policies, and clearly address procedures to be followed in the event of a loss, compromise, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data, including how and when affected persons will be notified, and remedial and corrective actions to be taken.
- e. Data Retention and Use: Establish data retention schedules in accordance with state or federal law or policy, access privileges, purge,

and deletion criteria for all data captured, stored, generated, or otherwise produced by a technology. Agencies should consider differentiating between data that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion or direct investigative focus. Agencies may wish to limit the retention of general surveillance data. Empirical research assessing the performance of a technology may assist in determining an appropriate retention schedule.

7. Oversight, Evaluation, Auditing, and Enforcement
 - a. Oversight: Establish a reporting mechanism and a protocol to regularly monitor the use and deployment of a technology to ensure strategic alignment and assessment of policy compliance.
 - b. Evaluation: Regularly assess the overall performance of a technology so that it can i) identify whether a technology is performing effectively, ii) identify operational factors that may impact performance effectiveness and/or efficiency, iii) identify data quality issues, iv) assess the business value and calculate return on investment of a technology, and v) ensure proper technology refresh planning.
 - c. Auditing: Audit all access to data captured, stored, generated, or otherwise produced by a technology to ensure that only authorized users are accessing the data for legitimate and authorized purposes, and establish regular audit schedules.
 - d. Enforcement: Establish procedures for enforcement if users are suspected of being or have been found to be in noncompliance with agency policies.

Conclusion

Realizing the value that technology promises law enforcement can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all resources and tools available to law enforcement, the use of new technologies must be carefully considered and managed. Agencies must clearly articulate their strategic goals for the technology, and this should be aligned with the broader strategic plans of the agency and safety needs of the public. Thorough and ongoing training is required to ensure that the technology performs effectively, and that users are well versed in the operational policies and procedures defined and enforced by the agency. Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system, and reassure the public that their privacy interests are recognized and protected. The development of these policies is a proven way for executives to ensure they are taking full advantage of technology to assist in providing the best criminal justice services, while protecting the privacy, civil rights, and civil liberties of citizens.

¹ This Technology Policy Framework was developed by an ad-hoc committee of law enforcement executives and subject matter experts representing IACP Divisions, Committees, Sections, the IACP National Law Enforcement Policy Center, and other organizations and groups, including the Criminal Intelligence Coordinating Council, Major Cities Chiefs Association, National Sheriffs' Association, Major County Sheriffs' Association, Association of State Criminal Investigative Agencies, the Institute for Intergovernmental Research (IIR), the Integrated Justice Information Systems (IJIS) Institute, and federal partners.

² The American Civil Liberties Union (ACLU) recently released two reports addressing law enforcement technologies—ALPR and body-worn video. Both reports discuss the value of the technology to law enforcement operations and investigations, and both call for policies addressing deployment, operations, data retention, access, and sharing. Catherine Crump, *You are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, (New York: ACLU, July 2013), at <https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record>, and Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All*, (New York: ACLU, October 2013), at <https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all>. Also see, Massachusetts Senate Bill S.1648, *An Act to Regulate the Use of Automatic License Plate Reader Systems*, Cynthia S. Creem, Sponsor, at <https://malegislature.gov/Bills/188/Senate/S1648>; Cynthia Stone Creem and Jonathan Hecht, "Check it, then chuck it," *The Boston Globe*, December 20, 2013, at <http://www.bostonglobe.com/opinion/2013/12/20/podium-license/R1tKQerVOYAPLW6VCKodGK/story.html>; Shawn Musgrave, "Boston Police halt license scanning program," *The Boston Globe*, December 14, 2013, at <http://www.bostonglobe.com/metro/2013/12/14/boston-police-suspend-use-high-tech-license-plate-readers-amid-privacy-concerns/B2hy9UizC7KzebnGyQ0JNM/story.html>; Ashley Luthern and Kevin Crowe, "Proposed Wisconsin bill would set rules for license-plate readers," *Milwaukee Journal Sentinel*, December 3, 2013, at <http://www.jsonline.com/news/milwaukee/proposed-wisconsin-bill-would-set-rules-for-license-plate-readers-b99155494z1-234324371.html>; Dash Coleman, "Tybee Island abandons license plate scanner plans," *Savannah Morning News*, December 3, 2013, at <http://savannahnow.com/news/2013-12-02/tybee-island-abandons-license-plate-scanner-plans#.UqCAy8RDuNO>; Kristian Foden-Vencil, "Portland police are collecting thousands of license plate numbers every day," *Portland Tribune*, December 3, 2013, at <http://portlandtribune.com/pt/9-news/2013130-portland-police-are-collecting-thousands-of-license-plate-numbers-every-day>; Alicia Petska, "City Council split over how to handle license plate reader concerns," *The News & Advance*, (Lynchburg, VA), November 12, 2013, at http://www.newsadvance.com/news/local/article_5327dc78-4c18-11e3-bc28-001a4bcf6878.html; Jonathan Oosting, "Proposal would regulate license plate readers in Michigan, limit data stored by police agencies," *MLive*, (Lansing, MI), September 9, 2013, at http://www.mlive.com/politics/index.ssf/2013/09/proposal_would_regulate_licens.html; Katrina Lamansky, "Iowa City moves to ban traffic cameras, drones, and license plate recognition," *WQAD*, June 5, 2013, at <http://wqad.com/2013/06/05/iowa-city-moves-to-ban-traffic-cameras-drones-and-license-plate-recognition/>; Richard M. Thompson, II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, (Washington, DC: Congressional Research Service, April 3, 2013), at <http://www.fas.org/sgp/crs/natsec/R42701.pdf>; Somini Sengupta, "Rise of Drones in U.S. Drives

Efforts to Limit Police Use,” *New York Times*, February 15, 2013, at <http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?pagewanted=all>; Stephanie K. Pell and Christopher Soghoian, “Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact,” *Berkeley Technology Law Journal*, Vol. 27, No. 1, pp. 117-196, (2012), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845644; and Stephen Rushin, “The Legislative Response to Mass Police Surveillance,” *79 Brooklyn Law Review* 1, (2013), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344805. All accessed December 30, 2013.

³ Personally identifiable information (PII) has been defined as “...any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.” Government Accountability Office (GAO), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, (Washington, D.C.: GAO, May 2008), p. 1, at <http://www.gao.gov/new.items/d08536.pdf>. McCallister, *et. al.*, define “linked” information as “information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual.” Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology*, (Gaithersburg, MD: NIST, April 2010), p. 2-1, at <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>. McCallister, *et. al.*, go on to describe *linked* and *linkable* information: “For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.” *Id.* Both accessed December 30, 2013.

⁴ Justice Harlan first articulated a “constitutionally protected reasonable expectation of privacy” in *Katz v. United States*, 389 U.S. 347 (1967), at 361. Justice Harlan’s two-fold test is “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” *Id.* Many of the technologies being deployed by law enforcement capture information that is publicly exposed, such as digital photographs and video of people and vehicles, or vehicle license plates in public venues (i.e., on public streets, roadways, highways, and public parking lots), and there is little expectation of privacy. “A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” *United States v. Knotts*, 460 U.S. 276 (1983), at 281. Law enforcement is free to observe and even record information regarding a person’s or a vehicle’s movements in public venues. The U.S. Supreme Court, however, has ruled that the electronic compilation of otherwise publicly available but

difficult to obtain records alters the privacy interest implicated by disclosure of that compilation. *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989). Automation overwhelms what the Court referred to as the *practical obscurity* associated with manually collecting and concatenating the individual public records associated with a particular person into a comprehensive, longitudinal criminal history record. “[T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.” *Id.*, at p. 764. This has subsequently been referred to as the “mosaic theory” of the Fourth Amendment. *United States v. Maynard*, 615 F.3d 544 (D.C. Cir.) (2010). See also, Orin Kerr, “The Mosaic Theory of the Fourth Amendment,” *Michigan Law Review*, Vol. 111, p. 311, (2012), at <http://www.michiganlawreview.org/assets/pdfs/111/3/Kerr.pdf>. Accessed December 30, 2013.

⁵ These universal principles largely align with the Fair Information Practices (FIPs) first articulated in 1973 by the Department of Health, Education & Welfare (HEW). HEW, *Records, Computers and the Rights of Citizens*, July 1973, at <http://epic.org/privacy/hew1973report/default.html>. See, Robert Gellman, *Fair Information Practices: A Basic History*, Version 2.02, November 11, 2013, at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>. Comparable principles have been articulated by various governmental agencies, including the U.S. Department of Homeland Security, (Hugo Teufel, III, *Privacy Policy Guidance Memorandum, Number: 2008-01*, (Washington, DC: DHS, December 29, 2008), pp. 3-4, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf); the Home Office in the United Kingdom (Home Office, *Surveillance Camera Code of Practice*, (London, UK; The Stationery Office, June 2013), pp 10-11, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf); and the Information and Privacy Commissioner of Ontario, Canada (Ann Cavoukian, *Guidelines for the Use of Video Surveillance Cameras in Public Places*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, September 2007), pp. 5-6, at: http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf, and Ann Cavoukian, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigative Report (Privacy Investigation Report MC07-68)*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, March 3, 2008), p 3, at: http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf). Also see, National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, (The National Academies Press: Washington, D.C., 2008), at http://nap.edu/catalog.php?record_id=12452. All accessed December 30, 2013.

⁶ Law enforcement is not, for example, expected to notify the subjects of lawfully authorized wiretaps that their conversations are being monitored and/or recorded. These deployments, however, are typically subject to prior judicial review and authorization. See, e.g., *Katz v. United States*, 389 U.S. 347 (1967); *Berger v. New York*, 388 U.S. 41 (1967); *Title III, Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. §§ 2510-2522, as amended by the *Electronic Communications Privacy Act of 1986*.

⁷ Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.2, August 9, 2013, CJISD-ITS-DOC-08140-5.2, at <http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>. Accessed December 30, 2013.

⁸ Additional guidance regarding safeguarding personally identifiable information can be found in the Office of Management and Budget (OMB) Data Breach notification policy (M-07-16), at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>, and state data breach notification laws available from the National Conference of State Legislatures, at <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>. Accessed December 30, 2013.

⁹ See, e.g., International Association of Chiefs of Police, *Model Policy: License Plate Readers*, August 2010 <http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223>; Paula T. Dow, Attorney General, *Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data*, (Trenton, NJ: Office of the Attorney General, December 3, 2010), at <http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersI-120310.pdf>; Office of the Police Ombudsman, *2011 Annual Report: Attachment G: Body-Worn Video & Law Enforcement: An Overview of the Common Concerns Associated with Its Use*, (Spokane, WA: Spokane Police Ombudsman, February 20, 2012), at <http://www.spdombudsman.com/wp-content/uploads/2012/02/Attachment-G-Body-Camera-Report.pdf>; ACLU, *Model Policy: Mobile License Plate Reader (LPR) System*, (Des Moines, IA: ACLU, September 19, 2012), at <http://www.aclu-ia.org/iowa/wp-content/uploads/2012/09/Model-ALPR-Policy-for-Iowa-Law-Enforcement.pdf>. Many of these policy elements are also addressed in the National Research Council's report, *op. cit.*, specifically in chapter 2, "A Framework for Evaluating Information-Based Programs to Fight Terrorism or Serve Other Important National Goals," at pp. 44-67. All accessed December 30, 2013

¹⁰ A privacy impact assessment (PIA) is "a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme." Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review*, 25, 2 (April 2009), pp. 125-135, at <http://www.rogerclarke.com/DV/PIAHist-08.html>. Law enforcement agencies should consider using the Global Advisory Committee's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities* at <https://it.ojp.gov/gist/47/Guide-to-Conducting-Privacy-Impact-Assessments-for-State--Local--and-Tribal-Justice-Entities>. This resource leads policy developers through appropriate privacy risk assessment questions that evaluate the process through which PII is collected, stored, protected, shared, and managed by an electronic information system or online collection application. The IACP published *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, (Alexandria, VA: IACP, September 2009), at http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. For a list of PIAs completed by the U.S. Department of Justice, see <http://www.justice.gov/opcl/pia.htm>; Department of Homeland Security, see <https://www.dhs.gov/privacy-office-privacy-impact-assessments-pia>. All accessed December 30, 2013.



*State of Surveillance in California –
Findings & Recommendations
January 2015*

Executive Summary

In the wake of revelations about the National Security Agency’s rampant warrantless spying and local law enforcement’s use of military equipment in cities like Ferguson, Missouri, community members have been regularly contacting the ACLU with concerns about the proliferation of surveillance. Cities and counties have also increasingly reached out for guidance about how to approach the use of surveillance in ways consistent with civil liberties and civil rights. Yet very little information exists about surveillance technology in California or how to properly consider its acquisition or use. To address this, the ACLU of California conducted a first-of-its-kind assessment of surveillance technology in the state. We also released a new resource guide, *Making Smart Decisions About Surveillance: A Guide for Communities*, and developed a model ordinance designed to help policymakers ensure adequate transparency, oversight, and accountability.¹

The following document summarizes our findings about the state of surveillance in California and recommends several ways that the Attorney General and other state policymakers could take action to help address the widespread lack of transparency, oversight, and accountability for surveillance technology in California.

Methodology and Summary of Surveillance Survey Findings

From June to November 2014, the ACLU of California² examined thousands of publicly available³ records for California’s 58 counties and 60 selected cities.⁴ We researched the types of surveillance technology in communities, including automated license plate readers (ALPRs),⁵ body cameras,⁶ drones,⁷ facial recognition,⁸ “Stingrays,”⁹ and video surveillance.¹⁰ We investigated how much money has been spent to acquire and maintain surveillance technology and the source of those funds. We also examined any public processes in place to provide for transparency, oversight, and accountability for surveillance technology’s acquisition and use. What we discovered raised a number of significant concerns.

Across the state, there is widespread proliferation of surveillance, with at least 90 communities (40 counties, 50 cities) possessing some form of surveillance technology. Vast sums of money are being spent on surveillance, including over \$65 million in publicly available figures, a significant portion of which is federal grant dollars. While some communities are taking important steps to thoroughly consider surveillance technology and develop plans to promote public safety and safeguard citizen rights, we discovered that even basic transparency, oversight, and accountability has become the exception, not the rule. Many California communities lack the

guidance to make smart decisions about surveillance and are moving forward without public conversation, careful consideration of the costs and benefits, or adequate policies in place to prevent misuse and safeguard rights.

There is Widespread Proliferation of Surveillance Technology in California

California communities have acquired and deployed a wide array of surveillance technologies. Our research uncovered at least 90 California communities (40 counties, 50 cities) in possession of various surveillance technologies.¹¹ Video cameras are the most common form of surveillance technology in California - more than half of the cities and counties we examined have acquired them. ALPRs are a close second - 57 of the 118 counties and cities in our survey possess such devices.¹² Finally, at least 32 California communities had body cameras as of November 2014.¹³

Local law enforcement agencies are also acquiring newer, more powerful technologies like drones and Stingray cell phone tracking devices that can facilitate other forms of surreptitious surveillance.¹⁴ At least 3 communities (San Jose and Los Angeles and Alameda Counties) have acquired drones for law enforcement purposes. Information about Stingray purchases was nearly impossible to locate, yet we know from reporting and our research that they exist in at least 10 different communities, including Los Angeles, Oakland, San Jose, San Francisco, San Diego and Sacramento.¹⁵ While a lack of publicly available information about drones and Stingrays makes it difficult to discover which localities possess these tools and the legal basis for their use, it may be that other communities are either considering or already have these technologies as well.

Vast Sums of Money is Being Spent on Surveillance Technology

We found publicly available evidence documenting more than \$65 million dollars in spending on surveillance technology in California. We identified over \$20 million of spending on video surveillance alone.¹⁶ These funds come from multiple sources, including local,¹⁷ state,¹⁸ and federal funding streams.¹⁹ Law enforcement agencies have also obtained surveillance funding from private sources such as police foundations,²⁰ asset forfeiture proceeds,²¹ and other jurisdictions²² (LAPD received its two drones from Seattle police).²³

Federal dollars are a very common source of funding for California's surveillance technology. Federal funds constituted roughly 40 percent of the surveillance programs we examined with identifiable funding sources. Numerous localities have used federal funds to buy everything from automated license plate readers²⁴ to facial recognition technology.²⁵ Federal funds were also originally earmarked for San Jose's drone purchase.²⁶ In California, these federal funds are typically administered under programs operated by the Department Homeland Security Grant Programs that include the Urban Areas Security Initiative (UASI) and the Port Security Grant Program (PSGP). The California Emergency Management Association (CalEMA) also manages federal surveillance grants to local governments.²⁷

Yet with all of the funding we found for the acquisition of these technologies, surveillance technology's post-acquisition costs, including maintenance, replacement, staffing, and training were often not accounted for or reported in publicly available materials. We did not find a single surveillance program that was preceded by a comprehensive cost-benefit analysis that included information about current and future costs and an analysis of the potential impact on civil

liberties and civil rights. It is clear from the few public records that we located that these ongoing costs can be substantial. For example, Clovis was spending at least \$60,000 in maintenance costs for its network of video surveillance cameras by 2011²⁸ and Richmond was spending \$300,000 annually for maintenance by 2013.²⁹

Because our research was based solely on publicly available information about surveillance, the spending data noted is almost certainly just the tip of the iceberg. Very little information is easily and publicly accessible about local surveillance technology acquisitions. For example, although public records reflect that Riverside acquired ALPR units in 2011, the ACLU was unable to locate any other documents concerning the acquisition, funding or policies concerning these ALPR units.³⁰

Basic Transparency, Accountability and Oversight Is the Exception for Surveillance Technology in California, Not the Rule

Surveillance technology is often purchased without adequate community engagement

Our research also revealed that communities in California are also acquiring surveillance technology without first adequately engaging the public.³¹ And when information about surveillance technology is included in public documents at some point in the process, it may include language so vague that it is difficult for the public and even some policymakers to understand what is being considered and know to voice concern.

Community members were surprised to learn in 2014 about drone purchases in San Jose and Alameda County. In San Jose, the relevant city council meeting agenda only specified that the police and fire departments had sought authorization to receive \$983,000 from the federally funded Bay Area Urban Areas Security Initiative.³² The public did not learn about the purchase until months later when ACLU researchers discovered attached agenda documents with earmarked funds for an “unmanned aerial vehicle.”³³ There was immediate public outrage at this “secret” purchase.³⁴ The police soon apologized and have now initiated a public process to consider the potential use of the drone.³⁵ Unfortunately, this trend continues - in late 2014, the Alameda County Sheriff simply announced that he had bought two drones, providing no public notice despite the fact that widespread local concerns sidelined a similar proposal in 2012.³⁶

The purchase of invasive Stingray cell phone surveillance technology is another area where policymakers and the public appear to also be left in the dark. When Sacramento County approved over \$300,000 dollars in funding for what the ACLU believes to be Stingray equipment, the only information provided in public records was that law enforcement was seeking “wireless tracking equipment.”³⁷ In San Jose public documents, over \$300,000 in funding for what the ACLU also suspects to be Stingray technology was referred to as “law enforcement surveillance technology equipment.”³⁸

Public debate is rare and late in the process

Our research found that adequate public debate over surveillance technology is rare and if it happens at all, is very late in the process. We found evidence of public debate about the acquisition of surveillance technology for less than 15% of the programs we tracked. None of the 52 communities we identified with two or more surveillance technologies publicly debated every

technology.³⁹ For more than 100 of the 180 surveillance technology programs we identified in publicly available records, we either could not locate evidence of a public hearing or approval was via consent calendar. Consent calendar items are typically designated as routine in nature, are intended to have no discussion, and are often approved en masse with a single vote. We found only two occasions where surveillance technology proposals were removed from the consent calendar to entertain public debate: for body cameras in Fresno,⁴⁰ and for a mounted infrared video-surveillance camera and microwave transmission system in San Diego County.⁴¹

Even where there are public records disclosing the consideration or acquisition of a surveillance program, they are often incomplete, lacking basic information about the technology involved, costs, or potential impact on civil liberties. The result is that policymakers may not have the information they need to make an informed decision. For example, after the Santa Cruz City Council approved the use of federal funds to purchase ALPRs for the police department, one councilmember was asked what effect the scanners might have on community members, he replied, “I don’t know enough about the technology.”⁴² Another was unaware of privacy issues, admitting, “I was asleep at the wheel. The council didn’t get much correspondence about the potential for the erosion of civil rights that these kinds of devices can cause.... If I’d been better informed about [the ALPRs] I may have voted against the purchase....”⁴³

We also found that the timing of any public debate and policymaker approval is often late in the process – after law enforcement agencies apply and obtain funding for surveillance technology rather than before. The Santa Clara County Sheriff was awarded \$489,000 by the Urban Areas Security Initiative to purchase facial-recognition software prior to public process before the Santa Clara County Board of Supervisors.⁴⁴ In Placerville, police obtained a grant for \$26,000 in federal funds for a license-plate reader before City Council public process.⁴⁵ San Rafael police were awarded \$33,126 in federal funds for a license-plate reader before public process at the city council.⁴⁶ Recently, the San Jose police received federal funding approval and earmarked it to purchase a drone prior to public process at the city council.⁴⁷

While some California communities have taken important steps to ensure a more robust public process, there is a lack of consistency in the process between different surveillance technologies.⁴⁸ For example, before Ventura acquired a \$93,000 video monitoring system, its police department discussed the system’s intended uses with local community councils, addressed residents’ concerns, and explained the proposed internal use restrictions.⁴⁹ And while San Jose’s acquisition of a drone initially lacked public involvement, when considering acquisition of body cameras the city developed a robust 12-month work plan that included a diverse ad-hoc committee, an assessment of technological needs, and the drafting of a policy for Council consideration.⁵⁰ Although we could not locate a community with a policy that ensures consistent public engagement and debate for all surveillance technology, members of the board of supervisors in Santa Clara, San Francisco, and Santa Cruz counties have announced plans to introduce separate Surveillance Technology & Community Safety Ordinances.

Few surveillance technologies have adequate use policies

We found a publicly available use policy for fewer than 1 in 5 surveillance technology programs. None of the 52 communities with two or more surveillance technologies had publicly available use policies for every technology. Many cities had no use policy whatsoever for their surveillance technology – for example, only 3 of the 61 counties and cities we identified using

video surveillance had publicly available use policies. The publicly available policies that do exist largely fail to properly address all of the necessary issues including purpose specification, limited use, training, data security, data retention, auditing, and accountability discussed by the Department of Homeland Security Privacy Office, the International Association of Chiefs of Police Technology Policy Framework, or the ACLU of California guide and model ordinance.⁵¹

Many policies we looked at appear to be modified templates that do not properly address all of the necessary issues. The City of Alameda's 2013 proposal for an ALPR policy is a prime example of this.⁵² Produced by a company called Lexipol, that policy did not place clear limits on the technology's use, instead directing that the technology be used for "official and legitimate business." That policy also lacked detail about officer training, meaningful limits on retention or use of ALPR data, and enforceable consequences for violation of the use policy itself. After analyzing the policy last year, the ACLU urged Alameda to delay adoption of ALPR technology until the community revised and improved its use policy.⁵³

Other surveillance programs appear to have no policies in place except for those written by a federally connected fusion center, such as by the South Bay Information Sharing System (SBISS), the Southern California-based Automated Regional Justice Information System (ARJIS), or the Northern California Regional Intelligence Center (NCRIC).⁵⁴ These policies lack strong protections to prevent against misuse and infringements of constitutionally protected activities.⁵⁵ For example, NCRIC's ALPR policy only prohibits monitoring of First Amendment activities where those activities are the sole reason for monitoring. The ARJIS policy lacks a detailed set of acceptable and prohibited uses.⁵⁶ While NCRIC expressly permits law enforcement agencies to set local retention policies, others, like ARJIS, do not, and once a community decides to share surveillance data with this fusion center, its control over what happens to community members' data diminishes.⁵⁷

We also found that few policies have clear and effective enforcement provisions for violations. The need for enforceable policies is illustrated by Oakland's officer body camera policy, which contains specific directives to officers' use of the equipment, prohibitions on conduct, and instructions for the storage and access to data. However, Oakland's policy does not contain a mechanism ensuring its enforcement⁵⁸ and it appears that Oakland police have repeatedly violated the department's body camera policy without consequence.⁵⁹

Not having a proper use policy can also lead to significant legal problems for communities. San Francisco learned this lesson the hard way when it adopted license plate readers without a formal policy that required officers to confirm plate reads visually to safeguard civil rights. In March 2009, an ALPR unit misread the plate of Denise Green, a 47 year-old African American woman, erroneously flagging her burgundy Lexis as a stolen gray truck. The police stopped Green, handcuffed her, and held her at gunpoint while a search took place.⁶⁰ In early 2014, a federal appeals court authorized a constitutional rights suit by Green against the SFPD, the City, and the patrol officers.

While no community has a surveillance use policy in place that comprehensively addresses all of the necessary issues, several community policies have integrated important building blocks that others can replicate.

- In 2006, the San Francisco Board of Supervisors passed the Community Safety Camera ordinance (CSC).⁶¹ The CSC includes a specific purpose for the cameras and limits use of camera data, requires public notice when new cameras are being considered, a public hearing, a vote of the police commission, approval only if benefits outweigh concerns and community support exists, and annual reporting.
- In 2006, the Fresno Police Department adopted a Video Policing Project Policy and Guidelines Manual.⁶² This extensive manual describes the system and its purpose, includes guidance and specific prohibitions on racial profiling, details access limits for collected data, addresses primary and secondary uses of data, strictly limits retention of footage, addresses the public's right of access to footage obtained by the city's cameras, and requires independent auditing.
- In 2014, Menlo Park's City Council passed an ordinance consisting of a use policy for ALPRs and video surveillance.⁶³ This enforceable policy includes provisions setting forth specific prohibited uses of each technology, quarterly auditing of the use and efficacy of ALPR, and constraints on how data can be shared with third parties including the area fusion center, NCRIC.
- In 2014, a citizens' committee appointed by the Oakland City Council drafted a proposed policy for the City's DHS-funded Port Domain Awareness Center (DAC) that places clear limits on allowable uses, provides guidance to operators with regards to constitutionally protected activities, requires comprehensive auditing, and sets forth enforceable consequences for misuse.⁶⁴

Oversight of surveillance technology after deployment is virtually non-existent

Necessary provisions for oversight of surveillance technology after initial use, including audits, fiscal and civil liberties reviews, and evaluation of program efficacy are few and far between. Two programs we found that planned for more than minimal periodic oversight are Fresno's citywide video-policing program and San Francisco's Community Safety Camera Program.⁶⁵

In Fresno, the city council required an annual independent audit of the police department's citywide, live-feed, video-policing program to ensure that all of the privacy and security guidelines for the system's use are being followed.⁶⁶ The auditor is specifically instructed to report to the city council on police compliance with Fresno's video-policing policies.⁶⁷ The first comprehensive audit was completed in 2014 by a former federal judge.⁶⁸ Fresno Police Chief Jerry Dyer expressed support for the auditing process, saying "I have no doubt the audit will be very helpful to our ongoing video policing operations."⁶⁹

San Francisco's CSC requires that the San Francisco Police Department prepare a report every year on all cameras in the City and County.⁷⁰ The annual report is designed to assess the cameras' effectiveness, effect on crime, and to help the community determine whether any changes to the program should be made.⁷¹ In 2008, researchers at the University of California, Berkeley, comprehensively evaluated San Francisco's surveillance cameras. The resulting report found that the existing camera program had not addressed its intended purpose of preventing or reducing violent crime.⁷² This report informed subsequent public debate amongst the Board of Supervisors regarding a proposal to expand the program.⁷³

Finally, Menlo Park’s ALPR and video surveillance ordinance requires NCRIC (the entity that stores the City’s ALPR data) to provide a quarterly report to the city that summarizes the number of license plates captured by the ALPR in the city, how many of those license plates were “hits” (on an active wanted list), the number of inquiries made by Menlo Park personnel along with the justifications for those inquiries, and information on any data retained beyond six months and the reasons for such retention. In November 2014, Menlo Park published its first quarterly ALPR review. The data indicated that only about .05% of the plate reads were “hits,” most of which were false reads.⁷⁴

Policy Recommendations

Surveillance technology is proliferating in California’s communities largely without mechanisms that ensure transparency, accountability, and oversight for its acquisition and use. Local law enforcement lacks clear guidance and direction from state policymakers on how to promote public safety while safeguarding civil liberties and civil rights. As the state’s chief law officer and defender of liberty for Californians, the Attorney General is well-positioned to work to address these growing concerns in a variety of ways:

1. Issue Attorney General Best Practices for Surveillance Technology

With growing community concern about policing, the Attorney General should use the opportunity to issue clear guidance to law enforcement in the state about the basic mechanisms for public transparency, accountability, and oversight that should be in place at the earliest stage of the process – when surveillance technology is being considered and well before it is purchased or deployed. Best Practices issues by the Attorney General’s Office would be very helpful to communities throughout California. The ACLU of California’s guide for communities, *Making Smart Decisions About Surveillance*, and resources also developed by The International Association of Chiefs of Police, Police Executive Research Forum, and the Department of Homeland Security Privacy Office would hopefully all be helpful to the development of Attorney General Best Practices.⁷⁵

2. Encourage Law Enforcement Support of Local Ordinances

The Attorney General could also encourage local law enforcement to support local Surveillance Technology & Community Safety Ordinances and create mechanisms that facilitate consistent transparency, accountability, and oversight at the local level. Policymakers in Santa Clara County, San Francisco County, and Santa Cruz County have already committed to introducing the ordinance, the Oakland Ad Hoc Advisory Committee on Privacy and Data Retention has also recommended its adoption,⁷⁶ and several other large and small communities throughout California are also considering next steps. Key principles for local ordinances include:

- **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.

3. Support State Legislation to Create Consistent Transparency, Oversight, and Accountability Mechanisms for California Law Enforcement

The Attorney General might also consider state legislation that also incorporates these key principles and ensures proper and consistent transparency, oversight, and accountability when surveillance technology is being considered by any California law enforcement entity.

4. Develop & Periodically Issue California State of Surveillance Report

The ACLU of California’s extensive research on surveillance in California also highlighted just how difficult it is to identify what is happening in the state. It would be very helpful for the Attorney General to streamline transparency about surveillance in California, both to increase public awareness and facilitate oversight. As a recommendation in Best Practices or a provision in a potential state law, the Attorney General’s Office should consider mechanisms to compile and release regularly-updated information about surveillance technology in the state, including what is being used and where, funding sources, and what processes are in place to provide for transparency, accountability, and oversight.

¹ The *Making Smart Decisions About Surveillance* guide, an interactive map of findings, and additional resources are available at <https://www.aclunc.org/smartaboutsurrveillance>.

² Thank you to legal researchers Matt Cagle, Thomas Mann Miller, Molly Caldwell, Tony Huynh, Lauren Harriman, and Leighanna Mixter.

³ For purposes of this document, “publicly available” information is that which a resident with Internet access could obtain online without the assistance of a request under the California Public Records Act. Our search included but was not limited to publicly available agendas, minutes, and staff reports of city councils and county boards of supervisors; documents of regional quasigovernmental entities; government statements; and news reports.

⁴ We researched the following California cities: Anaheim, Bakersfield, Beverly Hills, Burbank, Blythe, Chico, Chula Vista, Clovis, Concord, East Palo Alto, El Centro, Elk Grove, Escondido, Eureka, Fontana, Fremont, Fresno, Gilroy, Glendale, Hayward, Huntington Beach, Inglewood, Irvine, Long Beach, Los Angeles, Martinez, Merced, Menlo Park, Modesto, Moreno Valley, Napa, Oakland, Oceanside, Ontario, Oxnard, Pasadena, Placerville, Rancho, Cucamonga, Redding, Redlands, Richmond, Riverside, Roseville, Sacramento, Salinas, San Bernardino, San Diego, San Jose, San Rafael, Santa Ana, Santa Clara, Santa Cruz, Santa Maria, Santa Monica, Santa Rosa, Stockton, Turlock, Ukiah, Vallejo, Ventura, Visalia, Yuba City.

⁵ **Automated license plate readers** are 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 all vehicles that drive by.

⁶ **Body cameras** are small cameras worn by police that record audio and video. These cameras can record everything 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.

⁷ **Drones** are 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. Often quieter than traditional aircraft, drones are capable of surreptitious surveillance.

⁸ **Facial recognition** is software that identifies a person in photos or videos based on various characteristics of the person’s face. Facial recognition software may be applied to photos or videos captured by an array of devices or contained in government databases.

⁹ **“Stingrays,” or International Mobile Subscriber Identity (“IMSI”) Catchers** are devices that emulate a cell phone tower in order to interact with nearby cell phones. Stingrays identify nearby devices, operate in a dragnet fashion that affects every phone in range, and can also be configured to intercept and capture the contents of communications including calls, text messages, or Internet activity.

¹⁰ **Video surveillance camera** systems that allow the 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 investigations or prosecutions.

¹¹ A summary of the ACLU of California’s surveillance findings is located at the following URL:
<http://www.aclunc.org/surveillancemap>.

¹² We located approximately \$7.8 million in funding allocated for automated license plate readers.

¹³ We located approximately \$8.2 million in funding allocated for officer body cameras.

¹⁴ See Jennifer Valentino-Devries, *‘Stingray’ Phone Tracker Fuels Constitutional Clash*, Wall Street Journal, Sept. 22, 2011, available at: <http://www.wsj.com/articles/SB10001424053111904194604576583112723197574>.

¹⁵ We located publicly available information suggesting the following localities possess Stingrays: San Bernardino, Los Angeles Police Department, Los Angeles Sheriff Department, Oakland Police Department, San Jose Police Department, San Francisco Police Department, San Diego Police Department, San Diego County, Sacramento Police Department, and the Sacramento County Sheriff’s Department.

¹⁶ We located approximately \$21.5 million in funding allocated for video surveillance technology. Cities have spent the most local money on video surveillance programs, totaling almost \$10 million across 12 cities. Fresno spent over \$3 million on its live-feed cameras between 2006 and 2013, and has resorted to staffing the cameras with volunteers, rather than sworn officers as originally intended. Oliver Wanger, “Video Policing Unit Audit” (Nov. 30, 2013), 3–6, available at <http://www.wjhattorneys.com/assets/files/VPU-Audit-00449144.pdf> and <https://s3.amazonaws.com/s3.documentcloud.org/documents/1003257/wanger-report.pdf> (\$870,000 in 2007, \$1,016,477.95 in 2008, \$547,803 in 2009, \$124,200 in 2010, \$103,600 in 2011, \$111,400 in 2012, \$148,320 in 2013, and \$135,200 in 2014, totaling \$3,057,000.95). Richmond and the Port of Richmond spent \$4 million on 34 CCTV cameras in “high-crime” Richmond neighborhoods and 79 cameras at the Port of Richmond, in 2007. Richmond City Council, Meeting Minutes (July 31, 2007), 1–2, available at <http://www.ci.richmond.ca.us/ArchiveCenter/ViewFile/Item/1253> (the City of Richmond contributed \$1,538,244, the Port of Richmond contributed \$3,833,279, and the City of Richmond reserved \$166,721 for contingencies). Oakland has most likely spent millions of dollars on surveillance cameras, but there is no clear record of total spending. In 2008, Oakland police proposed spending \$5.8 million for a wireless mesh system with 20 surveillance cameras and a monitoring center, with expected annual recurring costs of \$800,000, and another \$1.5 million on cameras around public schools. Oakland currently has 35 CCTV cameras and 40 live-feed cameras in the city, 135 cameras at the Oakland Coliseum complex, and over 700 cameras around public schools. Memo from Wayne Tucker, Chief of Police, to the Office of the City Administrator, regarding a report on crime fighting strategies to the Public Safety Committee (Jul. 8, 2008), at 1, Port of Oakland, Board of Port Commissioners Meeting Agenda (May 23, 2013), Item 3.1, at 12, available at http://www.portofoakland.com/pdf/about/meetings/2013/boar_shee_130523.pdf.

¹⁷ For example, in September 2014 the City of Anaheim allocated over \$1.15 million of local funds for the purchase of officer body cameras. The specific source of funds was the Police Dept. 2014/2015 Budget for Civil Liabilities Investigator in the General Fund. See Ana Venagas, *Anaheim police officers to wear cameras*, OC Register, Sept. 9, 2014, available at <http://www.ocregister.com/articles/cameras-634334-video-police.html>; see also http://www.anaheim.net/docs_agend/questys_pub/MG47522/AgendaFrame.htm; http://www.anaheim.net/docs_agend/questys_pub/MG47522/AS47561/AS47565/AI47816/DO47817/DO_47817.pdf.

¹⁸ For example, video surveillance in Roseville was paid for in part with CA Prop. 1b funds.
http://roseville.granicus.com/MetaViewer.php?view_id=2&clip_id=2358&meta_id=88314

¹⁹ For example, the Department of Homeland Security (DHS) funneled \$35,546,960 to local governments in the Bay Area as part of the Urban Area Security Initiative (UASI) between May 1, 2012, and November 30, 2013. From those funds, Oakland received \$1,200,730 during that period, San Jose received \$1,548,879, Santa Clara County

received \$4,143,890, and Santa Cruz received \$345,800, totaling \$7,239,299. While not all UASI funds are allocated to surveillance technology, a significant portion are: *See* Memo from Tristan Levardo, CFO of the Bay Area Urban Area Security Initiative, to the Bay Area Urban Area Security Initiative Approval Authority regarding FY2011 UASI Spending Report (June 12, 2014), *available at* <http://bayareauasi.org/sites/default/files/resources/061214%20Agenda%20Item%207%20FY2011%20UASI%20Spending%20Report.pdf>; Bay Area Urban Areas Security Initiative, Project Proposal Guidance for Fiscal Year 2015 (Interim) (Sept. 11, 2014), at 9, *available at* <http://bayareauasi.org/sites/default/files/resources/091114%20Agenda%20Item%204%20Appendix%20A%20FY15%20Project%20Proposal%20Guidance%20%26%20Sample%20Form.pdf> (marked draft for Approval Authority review).

²⁰ The Chico Police Department Business Support Team funded a license-plate reader in Chico. *See, e.g.*, Chico City Council, Meeting Minutes (Feb. 19, 2013), Consent Agenda Item 2.2 (unanimously approving donation of license-plate reader from Chico Police Department Business Support Team), *available at* http://chico-ca.granicus.com/MinutesViewer.php?view_id=2&clip_id=370&doc_id=9db34992-d762-1030-9122-24b3144c4264;

²¹ Our research uncovered multiple purchases of surveillance technology made with asset forfeiture funds, including officer body cameras in Hayward and El Centro, video surveillance in Santa Barbara and Bakersfield, and ALPRs in Inglewood. *See* Hayward City Council Agenda, July 1, 2014, *available at* <http://www.hayward-ca.gov/CITY-GOVERNMENT/CITY-COUNCIL-MEETINGS/2014/CCA14PDF/cca070114full.pdf>; City of El Centro Council Agenda Report, Oct. 2, 2012, *available at* <http://www.cityofelcentro.org/userfiles/10-02-12%20-%20Item%209%281%29.pdf>; City of Santa Barbara City Council Minutes, Sept. 20, 2011, *available at* http://services.santabarbaraca.gov/cap/MG100814/AS100818/AS100825/AS100826/AI101983/DO102015/DO_102015.PDF; Gretchen Wenner, *Downtown surveillance cameras will bring Big Brother to Bakersfield*, *The Californian*, Aug. 12, 2010, *available at* <http://www.bakersfieldcalifornian.com/local/x1415295660/Downtown-surveillance-cameras-will-bring-Big-Brother-to-Bakersfield>; City of Inglewood Minutes, July 19, 2011, *available at* <http://www.cityofinglewood.org/civica/filebank/blobdload.asp?BlobID=7045>; *see also* Dave Maass, *Asset Forfeiture and the Cycle of Electronic Surveillance Funding*, Electronic Frontier Foundation, Jan. 16, 2015, <https://www.eff.org/deeplinks/2015/01/asset-forfeiture-and-cycle-electronic-surveillance-funding>.

²² In February 2014, the Modesto police announced they were sending a surveillance vehicle—called an “Armadillo”—equipped with eight live-feed, wide-angle, high-definition cameras to monitor “high-crime” neighborhoods. There was no decision by local leaders to approve the transfer; the police department had received the vehicle as a donation from neighboring Ceres. Modesto Police Department, *Police Armadillo Hits High Crime Areas* (Feb. 25, 2014), <http://www.ci.modesto.ca.us/newsroom/releases/police/prdetail.asp?ID=1872>; Tim Daly, *Modesto cops add “armadillo” to force*, *News 10*, Feb. 26, 2014, *available at* <http://www.news10.net/story/news/local/modesto/2014/02/26/modesto-armadillo-police-camera/5848819/>. In another example, several Native American tribes funded license-plate readers for the San Diego County Sheriff. 2011 ALPR funding \$78,673.25, San Diego County Meeting Agenda, *available at* http://www.sdcounty.ca.gov/lueg/iglcbc/meetingdocs/4-8-11_IGLCBC_MeetingAgenda.pdf.

²³ Joel Rubin, *LAPD adds drones to arsenal, says they’ll be used sparingly*, *LA Times*, May 30, 2014, *available at* <http://www.latimes.com/local/lanow/la-me-ln-lapd-adds-drones-to-arsenal-20140530-story.html> (“[T]he department announced that it had acquired two “unmanned aerial vehicles” as gifts from the Seattle Police Department.”)

²⁴ Numerous California localities have used federal funding to purchase automated license plate readers and include Chula Vista, Clovis, East Palo Alto, Marin County, Roseville, San Diego, Tulare County, and Elk Grove.

²⁵ *See* Memo from Assistant Attorney General Regina B. Schofield to Dr. Pamela Scanlon regarding federal funding in the amount of \$418,000 for the Automated Regional Justice Information System (ARJIS) which includes a “query system based on facial recognition.” *Available at*: https://www.eff.org/files/2013/11/07/01_-_tacids_award_letter_2.pdf; *see also* Jennifer Lynch & Dave Maass, *San Diego Gets in Your Face With New Mobile Identification System*, Electronic Frontier Foundation, Nov. 7, 2013, <https://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system>.

²⁶ Memo from Larry Esquivel, San Jose Chief of Police, to the Mayor and City Council (Nov. 1, 2013), at 3, *available at* <http://sanjoseca.gov/DocumentCenter/View/23693> (requesting permission to purchase an unmanned aerial vehicle with \$8,000 of \$354,000 in DHS funding); City of San Jose, City Council Meeting Minutes (Nov. 19, 2013), Item 2.12, at 9, (authorizing execution of agreement with the City and County of San Francisco to accept \$983,000 in funding from the Urban Areas Security Initiative); *see also* Shawn Musgrave, *Despite Repeated Denials, San Jose Police Definitely Have a Drone*, *Vice* (July 29, 2014), *available at* motherboard.vice.com/read/despote-repeated-denials-san-jose-police-definitely-have-a-drone; Robert Salonga, *San*

Jose police drone inflames surveillance-state rumblings, San Jose Mercury News (July 30, 2014), available at http://www.mercurynews.com/crime-courts/ci_26253376/san-jose-surveillance-state-rumblings-inflamed-by-sjpd.

²⁷ For example, the Alameda County Sheriff originally planned to purchase a drone in 2012 with part of a larger \$1.2 million grant dispersed through the California Emergency Management Agency. Angela Woodall, *Alameda County puts the brakes on purchasing drone*, Oakland Tribune, Dec. 4, 2012, available at http://www.mercurynews.com/breaking-news/ci_22122536.

²⁸ City of Clovis, Report to the City Council (Sept. 19, 2011), available at <https://www.ci.clovis.ca.us/Portals/0/Documents/CityCouncil/Agendas/2011/20110919/CC-D-1.pdf>; see also Demian Bulaw, *Future Fuzzy for Government Use of Surveillance Cameras/Still Some Bay Area Cities Hope to Follow Clovis' Lead*, SFGate, July 23, 2006, available at <http://www.sfgate.com/news/article/Future-fuzzy-for-government-use-of-public-2515607.php>.

²⁹ See City of Richmond, Human Resources Management Dept. Meeting Minutes (Apr. 25, 2013), at 1–3, available at <http://www.ci.richmond.ca.us/Archive/ViewFile/Item/5178>.

³⁰ ALPR units were mentioned in a community update newsletter, RPD Happenings, available at <http://www.riversideca.gov/rpd/community/newsletters/rpd-2011-05.pdf>.

³¹ There are many examples of surveillance technology purchases without public notice or involvement. For example, a 2009 report to the Salinas city council listed a video surveillance system as having been acquired “recently” despite the fact that the ACLU could not locate publicly available City Council records mentioning the initial purchase. Salinas Police Department, 180-day Report to the Community, October 20, 2009, available at <http://www.ci.salinas.ca.us/services/police/pdf/180-DayReport-102009.pdf>.

³² Matt Bigler, *Bay Area's first cop drone sparks worry, outrage from civil-rights group*, KCBS Bay Area, <http://sanfrancisco.cbslocal.com/2014/11/13/san-jose-police-hear-residents-concerns-about-surveillance-drone/>; Thom Jensen, Mike Bott, *Is sheriff's department using tracking and data-collecting device without search warrants?*, CBS News 10, June 23, 2014, <http://www.news10.net/story/news/investigations/2014/06/23/is-sacramento-county-sheriff-dept-using-stingray-to-track-collect-data/11296461/>.

³² City of San Jose, City Council Meeting Agenda (Nov. 19, 2013), at 6 (Consent Calendar Item 2.12), available at <http://sanjoseca.gov/DocumentCenter/View/23727>.

³³ When the San Jose City Council gave approval to police to purchase a drone, the description on the city council meeting agenda specified only that the police and fire departments sought authorization to receive \$983,000 from the Bay Area Urban Areas Security Initiative. The description provided only a link to a memo from the police and fire chiefs and the budget director with more information about what the funds would be used for, including \$8,000 for an unmanned aerial vehicle. See City of San Jose, City Council Meeting Agenda (Nov. 19, 2013), at 6 (Consent Calendar Item 2.12), available at <http://sanjoseca.gov/DocumentCenter/View/23727>; Memo from Larry Esquivel, San Jose Chief of Police, to the Mayor and City Council (Nov. 1, 2013), at 3, available at <http://sanjoseca.gov/DocumentCenter/View/23693> (requesting permission to purchase an unmanned aerial vehicle with \$8,000 of \$354,000 in DHS funding).

³⁴ Scott Herhold, *Big Brother, begone: The San Jose police should get rid of their drone*, San Jose Mercury News, Aug. 2, 2014, available at http://www.mercurynews.com/scott-herhold/ci_26264766/big-brother-begone-san-jose-police-should-get; San Jose Peace & Justice Center, *Rally Against the Drone! And Militarization of the Police* (last accessed Jan. 20, 2015), <http://www.sanjosepeace.org/article.php/20141001152838137>.

³⁵ 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

³⁶ In November 2014 the Alameda County Sheriff purchased two drones with over \$97,000 in funds from the county's Office of Homeland Security and Emergency Services. See Matt O'Brien, *Alameda County sheriff buys two drones*, Dec. 4, 2014, available at http://www.mercurynews.com/crime-courts/ci_27059034/alameda-county-sheriff-buys-two-drones.

³⁷ Sacramento County, Board of Supervisors Agenda (Nov. 5, 2013), Item 14, available at <http://www.agendanet.saccounty.net/sirepub/cache/2/uwdlotm54esv3znz0pwsbzy/1131109042014035517303.htm>; Memo from the Sheriff's Department to the Sacramento County Board of Supervisors for the Agenda of Nov. 5, 2013, at 2, available at <http://www.agendanet.saccounty.net/sirepub/cache/2/uwdlotm54esv3znz0pwsbzy/649263409042014035719458.PDF> (spending authorization request includes \$300,075 for “Wireless Tracking Equipment”) (in a response to a public-records request from the ACLU of Northern California about documents related to IMSI catchers, Sacramento County returned a document with the same budget line, \$300,075, with the description, apparently “Wireless Tracking Equipment,” redacted); Kim Minugh, *Sacramento County sheriff acknowledges possession, use*

of cellphone surveillance technology, Sacramento Bee (Jul. 31, 2014), available at <http://www.sacbee.com/2014/07/31/6596112/sacramento-sheriff-acknowledges.html>.

³⁸ Memo from Christopher M. Moore, Chief of Police, to the San Jose Mayor and City Council (July 30, 2014), at 3 (requesting authorization to enter into agreement with City and County of San Francisco to allocate UASI funds to San Jose, including \$250,000 for “law enforcement surveillance technology equipment”); Agreement Between the City and County of San Francisco and the City of San Jose for the Distribution of FY 2011 UASI Grant Funds (May 1, 2012), at A-3, available at http://www3.sanjoseca.gov/clerk/Agenda/20120821/20120821_0802acon.pdf (\$250,000 to purchase “law enforcement surveillance technology equipment”). The equipment number included in the agreement description, AEL#: 13LE-00-SURV, is used by DHS. See Department of Homeland Security, Equipment, Law Enforcement Surveillance, AEL / SEL Number 13LE-00-SURV, available at <https://www.llis.dhs.gov/knowledgebase/authorizedequipmentlist/equipment-law-enforcement-surveillance> (accessed Sept. 4, 2014) (equipment description: “Surveillance equipment and related accessories, including but not limited to: audio, data, and visual equipment. Includes electronic equipment such as Pen registers (equipment capable of capturing incoming and outgoing phone numbers, along with the duration of calls, without listening to the actual conversations.)”); City of San Jose, Early Distribution Council Packet for May 14, 2013 (Apr. 30, 2013), at 12 (including memo from San Jose Chief of Police Larry Esquivel regarding proposed spending for 2012 UASI funding); Agreement Between the City and County of San Francisco and the City of San Jose for the Distribution of FY 2012 UASI Grant Funds (Dec. 1, 2012), at A-2, available at <http://sanjoseca.gov/DocumentCenter/View/15909> (\$172,000 to purchase “law enforcement surveillance equipment,” AEL# 13LE-00-SURV); The two expenditures of \$250,000 and \$172,000 match records San Jose released in response to a public-records request, including proposals to UASI (for the same amounts) and purchase agreements with Harris Corp. (totaling \$432,485.31), which produces the most well-known IMSI catchers. See KXTV News 10, *9 Calif. law enforcement agencies connected to cellphone spying technology*, Mar. 6, 2014, available at <http://www.news10.net/story/news/investigations/watchdog/2014/03/06/5-california-law-enforcement-agencies-connected-to-stingrays/6147381/>.

³⁹ In at least one instance, local officials did not debate acquisition but did debate policy: the Chico City Council authorized the purchase of a license-plate reader on the consent calendar, in 2013, but directed staff to draft a use policy, which it did debate. City of Chico, City Council Meeting Minutes (Sept. 3, 2013), available at http://chico-ca.granicus.com/MinutesViewer.php?view_id=2&clip_id=416&doc_id=d8a860c2-67dd-1031-9668-843478bb431f; City of Chico, City Council Meeting Agenda (Sept. 3, 2013), available at http://chico-ca.granicus.com/MetaViewer.php?view_id=2&clip_id=416&meta_id=36829.

⁴⁰ City of Fresno, City Council Meeting Minutes (Jul. 31, 2014), available at <https://fresno.legistar.com/LegislationDetail.aspx?ID=1852287&GUID=833F6193-0CCE-45C7-86CC-3C0194672568>.

⁴¹ San Diego County, Board of Supervisors Meeting Agenda (Jan. 26, 2010), Item 2, available at http://sdcountry.granicus.com/DocumentViewer.php?file=sdcountry_673669eb2e688fc71ef2bec80221ad8c.pdf&view=1; Memo from William D. Gore, San Diego County Sheriff, to the San Diego County Board of Supervisors (Jan. 26, 2010) (request for sole source authority to purchase surveillance equipment), available at http://www.sdcountry.ca.gov/bos/supporting_docs/012610ag02t.pdf.

⁴² John Malkin, *Surveillance City?* GoodTimes, Jan 29, 2014, <http://www.gtweekly.com/index.php/santa-cruz-news/good-times-cover-stories/5386-surveillance-city.html>.

⁴³ *Id.*

⁴⁴ Santa Clara Board of Supervisors, Minutes, Sept. 11, 2012, available at <http://sccgov.iqm2.com/Citizens/FileOpen.aspx?Type=12&ID=4131&Inline=True> (approving grant of UASI federal funds); see also Memo from Laurie Smith, Santa Clara County Sheriff, to the Santa Clara County Board of Supervisors regarding Integrated Regional Law Enforcement Information Sharing System (Coplink) (Feb. 12, 2013) (requesting authorization to spend \$489,000 from the Department of Homeland Security to upgrade regional database with facial recognition software), available at sccgov.iqm2.com/Citizens/FileOpen.aspx?Type=30&ID=13873.

⁴⁵ Memo from George Nielson, Chief of Police, to the Placerville City Council, Aug. 20, 2008, available at <http://www.cityofplacerville.org/civicax/filebank/blobload.aspx?blobid=3962> (“[A]pproximately \$26,000.00 has been approved by the Approval Authority Board for the City's use, for the purchase of an Automated License Plate Recognition system.”)

⁴⁶ City of San Rafael, City Council Agenda Report, prepared by Lt. Raffaello Pata, Captain (Mar. 19, 2012).

⁴⁷ See Memo from Larry Esquivel, San Jose Chief of Police, to the Mayor and City Council (Nov. 1, 2013), at 3, *available at* <http://sanjoseca.gov/DocumentCenter/View/23693> (requesting permission to purchase an unmanned aerial vehicle with \$8,000 of \$354,000 in DHS funding).

⁴⁸ The Redlands Police Department convened a Citizens' Privacy Council, open to any resident of the city, to provide advice on policy for surveillance cameras and oversee police use of the cameras. Richmond formed an ad-hoc committee to evaluate policies for its video surveillance program. 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. Redlands Police Department, Citizen Privacy Council, <http://www.cityofredlands.org/police/CPC>; 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; see Memorandum, Oakland City Administrator's Weekly Report (Apr. 25, 2014), <http://www2.oaklandnet.com/oakcal/groups/cityadministrator/documents/report/oak046804.pdf>.

⁴⁹ City of Ventura Administrative Report (Dec. 14, 2011), *available at* http://www.cityofventura.net/files/file/meetings/city_council/2012/01-09-12/item%2004.pdf

⁵⁰ Memo from Larry Esquivel, Chief of Police, to the San Jose Mayor and City Council (Mar. 20, 2014), regarding body worn cameras (detailing work plan for Body Worn Camera Committee), *available at* <http://www.piersystem.com/external/content/document/1914/2126242/1/03-21-14Police.PDF>.

⁵¹ 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; International Association of Chiefs of Police, Technology Policy Framework (2014), *available at* www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.

⁵² See, e.g., Draft ALPR Policy 462 for the use of Automated License Plate Readers, Alameda City website, http://alamedaca.gov/sites/default/files/department-files/2013-12-26/draft_alpr_policy.pdf.

⁵³ Analysis of Alameda's Draft Policy Manual for Automated License Plate Readers, Jan. 29, 2014, *available at* http://alamedaca.gov/sites/default/files/department-files/2014-02-04/aclu_analysis_of_alameda_alpr_policy.pdf.

⁵⁴ For example, San Diego, Chula Vista, Oceanside, and Escondido share all data they collect with ALPRs through a regional data-sharing system called ARJIS. In the Bay Area alone, several regional data-sharing systems aggregate and analyze ALPR data, including SBISS for the South Bay (Santa Clara and Gilroy), NCRIC for the North Bay (Menlo Park, San Mateo County), and the UASI's West Node Regional Data Sharing in Marin County.

⁵⁵ NCRIC Automated License Plate Reader Policy, *available at* <https://ncric.org/html/NCRIC%20ALPR%20POLICY.pdf> ARJIS LPR Regional Guidelines (Jan. 2015 draft), *available at* <http://www.arjis.org/Portals/0/PortalDocuments/DRAFT%20ARJIS%20LPR%20Acceptable%20Use%20Policy%20OpSC%2001%2002%202015%20ps.pdf>; SBISS Memorandum of Understanding, http://www3.sanjoseca.gov/clerk/Agenda/20100330/20100330_0210mou.pdf.

⁵⁶ SBISS MOU mentions no set limit. NCRIC has a default length of one year, but allows shorter limits set by contributing cities or counties to trump its retention period. ARJIS has a retention period of one year for fixed cameras and two years for portable cameras regardless of limit set by contributor. City of Palo Alto City Council Staff Report (May 5, 2014), *available at* <https://www.cityofpaloalto.org/civica/x/filebank/documents/40191>; NCIRC Automated License Plate Reader Policy, *available at* <https://ncric.org/html/NCRIC%20ALPR%20POLICY.pdf>; LPR Regional Guidelines (Jan. 2015 Draft), *available at* <http://www.arjis.org/Portals/0/PortalDocuments/DRAFT%20ARJIS%20LPR%20Acceptable%20Use%20Policy%20OpSC%2001%2002%202015%20ps.pdf>; The City of Novato California Staff Report (Oct. 8, 2013), *available at* http://ci.novato.ca.us/agendas/pdfstaffreports/cc100813_F-3.pdf; Memorandum of Understanding, *available at* http://apps.co.shasta.ca.us/BOS_Agenda/MG69199/AS69205/AS69234/AI69367/DO69369/13.PDF.

⁵⁷ A data sharing agreement in one jurisdiction may affect residents in another. For example, when the Santa Clara County Board of Supervisors approved, via consent calendar, a request from the county sheriff to upgrade a regional database with facial-recognition software, the decision also affected dozens of other cities that cooperate with the county sheriff and contribute information to the database—including every city in Santa Clara, Santa Cruz, Monterey, and San Benito counties. See Memo from Laurie Smith, Santa Clara County Sheriff, to the Santa Clara County Board of Supervisors regarding Integrated Regional Law Enforcement Information Sharing System (Coplink) (Feb. 12, 2013) (requesting authorizing to spend \$489,000 from the Department of Homeland Security to

upgrade regional database with facial recognition software); Santa Clara County Board of Supervisors, Board of Supervisors Meeting Minutes (Feb. 12, 2013) (approving request from Laurie Smith on consent calendar).

⁵⁸ Oakland Police Department, Portable Video Management System, Departmental General Order, Effective Date Mar. 5 2014, *available at* <https://www.muckrock.com/foi/california-52/oakland-police-dept-body-cam-policy-emails-and-complaints-13459/#files>.

⁵⁹ *See, e.g.*, Sixteenth Monitoring Report of Robert S. Warshaw, Monitor of the Negotiated Settlement Agreement (NSA) in the case of *Delphine Allen, et al., vs. City of Oakland, et al.*, in the United States District Court for the Northern District of California, at 45, *available at* <http://www.cand.uscourts.gov/filelibrary/1350/2014-01%20monitoring%20report.pdf>.

⁶⁰ Matt Cagle, *San Francisco - Paying the Price for Surveillance Without Safeguards*, ACLU-NC Blog, May 22, 2014, <https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards>.

⁶¹ Community Safety Camera Ordinance, Chapter 19 of the San Francisco Administrative Code, *available at* <http://administrative.sanfranciscocode.org/19/>.

⁶² For complete Video Policing Project Policy Guidelines and Manual, *see* Memo from Jerry Dyer, Fresno Police Chief, to Fresno City Council, Oct. 21, 2008, 13–24, *available at* <http://www.fresno.gov/NR/rdonlyres/77999966-4ABA-45C5-9519-42E4E29657A4/0/HonorableBrettDorianVideoPolicingAuditorServices.pdf>.

⁶³ City of Menlo Park, City Council Special and Regular Meeting Agenda (June 3, 2014), Item #D-1, An Ordinance Regarding the Use of Automated License Plate Readers and Neighborhood Surveillance Cameras, *available at* <http://www.menlopark.org/ArchiveCenter/ViewFile/Item/1658>.

⁶⁴ The Ad Hoc committee’s draft, dated January 15, 2015, is available here: <https://oaklandprivacy.files.wordpress.com/2015/01/1-13-15-dac-privacy-and-data-retention-policy-draft-011515.pdf>.

⁶⁵ Cities and counties have occasionally required that surveillance technologies be reviewed within a certain time period after deployment, but these requirements are rare and incomplete where they exist. For example, while San Bernardino maintains a city website listing statistics about the use of ALPR, including stolen cars recovered, publicly available statistics have not been published for any year following 2010. *See* ALPR Statistics, City of San Bernardino website (last visited Jan. 20, 2015), http://www.ci.san-bernardino.ca.us/cityhall/police_department/public_safety/traffic_safety_programs/alpr/default.asp. Roseville’s City Council required that the Roseville Police Department report the benefits and costs of bus cameras to a city commission one year after installation. In the case of Roseville, the ACLU found no record that the post-deployment report was ever conducted. City of Roseville, Transit On-Board Video Cameras Purchase (May 31, 2012), *available at* http://roseville.granicus.com/MetaViewer.php?view_id=2&clip_id=2358&meta_id=88314.

⁶⁶ Fresno City Council Minutes, Sep. 20, 2012, *available at* <http://www.fresno.gov/CouncilDocs/agenda9.20.2012/1b.pdf>.

⁶⁷ *Id.*; City of Fresno, City Council Meeting Minutes, Aug. 22, 2006, *available at* <http://www.fresno.gov/NR/rdonlyres/CE8889CD-A095-40D1-968B-B50237558584/0/August222006CityCouncilMinutes.pdf> (amending policy to include annual audit); City of Fresno, City Council Meeting Minutes, Sep. 26, 2006, *available at* <http://www.fresno.gov/NR/rdonlyres/2D40AAED-5A45-4FD1-8316-1EE714F42D78/0/September262006CityCouncilMinutes.pdf> (amending policy to include greater protections for individuals participating in demonstrations or other lawful gatherings).

⁶⁸ Hon. Oliver W. Wanger, *Annual Audit for the Fresno Police Department Video Policing Unit for the Period Ending November 30, 2013* (December 30, 2013), *available at* <http://www.wjhattorneys.com/assets/files/VPU-Audit-00449144.pdf>; George Hostetter, *Former Judge Wanger Writes Far-Ranging Audit on Fresno Video Policing*, in *The Fresno Bee* (Jan. 7, 2014), *available at* <http://www.fresnobee.com/2014/01/07/3701754/judge-wanger-delivers-impressive.html>.

⁶⁹ Judge Wanger: Fresno video policing done right, needs money, *Fresno Bee*, Jan 8, 2014, *available at* <http://cqcengage.com/mmajority/app/document/1354649;jsessionid=ocJiPHEyGHZ19bsd440Xgp5B.undefined>

⁷⁰ Ordinance No. 127-06, Sec. 19.4(d), *available at* <https://sfgov.legistar.com/View.ashx?M=F&ID=2592763&GUID=E040FBD1-E991-425A-AE5B-0A4449FFD108>.

⁷¹ *Id.* The report must “identify the camera locations, the crime statistics (or the vicinity surrounding each camera both before and after the camera is installed, crime statistics from surrounding vicinities, the number of times the Police Department requested copies of the recorded images, the number of times the images were used to bring criminal charges, the types of charges brought, and the results of the charges.”

⁷² *See* Citris, Citris Study on SF Public Cameras Released (Jan. 9, 2009), <http://citris-uc.org/citris-study-on-sf-publiccameras-released/>.

⁷³ Andrew Dudley, *Lights, Camera, Inaction: San Francisco's Broken Surveillance System*, Hoodline, Oct. 19, 2014, <http://hoodline.com/2014/10/lights-cameras-inaction-san-francisco-s-broken-surveillance-state>.

⁷⁴ Quarterly Review of Data Captured by Automated License Plate Readers (ALPR) for the Period Beginning July 1, 2014 through October 1, 2014, Menlo Park City Council Meeting, Nov. 18, 2014, *available at* <http://menlopark.org/DocumentCenter/View/5786>.

⁷⁵ See *Making Smart Decisions About Surveillance: A Guide for Communities*, <https://www.aclunc.org/publications/making-smart-decisions-about-surveillance-guide-communities>; Map: State of Surveillance in California, ACLU of Northern California, <https://www.aclunc.org/article/map-state-surveillance-california>; 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; Police Executive Research Forum, How Are Innovations in Technology Transforming Policing? 26 (Jan. 2012), *available at* http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf; International Association of Chiefs of Police, Technology Policy Framework (2014), *available at* www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.

⁷⁶ The DAC Ad Hoc Advisory Committee's recommendations supplementing its privacy policy include a recommendation that Oakland adopt a citywide surveillance technology ordinance. <https://oaklandprivacy.files.wordpress.com/2015/01/1-13-15-dac-privacy-and-data-retention-policy-draft-011515.pdf>.



HOME MAIN MENU MY STORIES: 24 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

Ars Technica has arrived in Europe. [Check it out!](#)

LAW & DISORDER / CIVILIZATION & DISCONTENTS

In rare move, Silicon Valley county gov't kills stingray acquisition

Santa Clara county executive tells Ars what Harris wanted was "on the silly side."

by Cyrus Farivar - May 7, 2015 6:00am PDT

Share Tweet 32



Jhaymesiviphotography

The Santa Clara County Board of Supervisors has halted a plan to approve the purchase of a cell-site simulator, better

FURTHER READING

LAT



SEC Sw "re sm



LAT



FEAT G1 to

known as a stingray.

The secretive surveillance devices can be used to determine a phone's location, but they can also intercept calls and text messages. During the act of locating a phone, stingrays also sweep up information about nearby phones—not just the target phone. Earlier this year, Ars reported on how the **FBI is actively trying to "prevent disclosure"** of how these devices are used in local jurisdictions across America.

The move, happening in one of the primary counties in Silicon Valley, marks an unusual occasion that a local government has turned away from federal funds that would be used to acquire such a device. The device was **approved** initially during a February 24, 2015 meeting, despite a **testy exchange** between the Santa Clara Sheriff's Office and Supervisor Joe Simitian, a former state senator with a penchant for an interest in privacy issues. Simitian's office didn't immediately respond to Ars' request for comment.

Staying mum

James Williams, the deputy county executive, **wrote in a Tuesday letter** to his boss Jeffrey Smith:

After negotiations regarding contract terms, including business and legal issues, the County and Harris have been unable to reach agreement on a contract for the purchase of the System. Accordingly, the System will not be purchased at this time.

Harris Corporation is the Florida-based defense contractor that is the manufacturer of the device produced under the StingRay trademark. As the dominant maker of cell-site simulators, stingray has also become the generic name for this class of devices. Both the FBI and the Harris Corporation have previously declined to answer Ars' specific questions.

Smith told Ars that Harris wanted to impose overly strict restrictions as to what could be disclosed through the public records process.

"What happened was, we were in negotiations with Harris, and we couldn't get them to agree to even the most basic criteria we have in terms of being responsive to public records requests," he said.

"After many hours of back and forth it became clear that they weren't going to consent to a contract in an attempt to keep everything secret and non-discoverable and that's not something we could live with as a public agency. The negotiations are going to be terminated and the grant money will go to other purposes."



STINGRAY PHONE TRACKERS COMING TO SANTA CLARA AFTER "15 MINUTES" OF REVIEW

Vote this week comes after community given little chance to object.

FURTHER READING



ROBBERY SUSPECT PULLS GUILTY PLEA AFTER STINGRAY DISCLOSURE, CASE DROPPED

"What's the point of gathering evidence if you're not going to use it?"

pe

The
New

WA

Ha

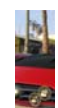
G4

LG
Sna

STA



LAT



WH.

AB
th

DOZ

He said that the FBI was not involved in the discussions, and that Santa Clara County did not even get to the stage of the onerous non-disclosure agreement along the lines of a previously published one **revealed** in a court case in Erie County, New York.

In that case, a **rare unredacted form** demonstrated the full extent of the FBI's attempt to quash public disclosure of stingray information. The most egregious example from the document showed that the FBI would prefer to drop a criminal case in order to protect secrecy surrounding the stingray.

In St. Louis, a defense lawyer who represented a woman who had pleaded guilty to being involved in a series of robberies recently told Ars that prosecutors **dropped charges** rather than expose the use of a stingray. Last year, **prosecutors in Baltimore** did the same thing during a robbery trial.

"The best I can get into is that [Harris has] been convinced by somebody, maybe by themselves, that federal law prohibits them saying anything to anybody about their technology unless that person has a badge or is a criminal investigation in the criminal justice system," Smith added.

"So if we're buying this as civilians we would have to guarantee that we would never tell anybody that it was being bought. It was a little on the silly side. They're claiming that everything is a trade secret, but the reality is that the public is quite well-aware that this is a wireless wiretapping and it's not a secret, I can't understand where they're coming from."

Bringing sunlight to the process

Civil liberties and legal experts hope that the newfound scrutiny that has come from various cities around the country, including Tacoma, Washington, and Erie County, New York, are beginning to reach those in government.

"With more scrutiny of these deals and the strings that are attached to them, I am hopeful that more counties will negotiate more aggressively," **Brian Owsley**, a former federal judge who is now a law professor at Indiana Tech, told Ars.

"As Harris Corporation is in the business of selling its products, if enough local law enforcement agencies object to the 'standard' agreement, then Harris Corporation may have to change its standard language."

Relatively little is known about how, exactly, stingrays, known more generically as cell-site simulators, are used by law enforcement agencies nationwide, although new documents have recently been released showing how they have been purchased and **used in some limited instances**. However, it has been well-established that **cops have lied to courts** about their use. Typically, police deploy them without first obtaining a search warrant.

A local privacy activist who has closely followed stingrays from nearby San Leandro, California, Mike Katz-Lacabe, told Ars this was the first time he had ever heard of a county resisting acquisition of a stingray.

"Much, if not all, of the credit goes to Supervisor Joe Simitian and his push for transparency," he told

FURTHER READING



NEW CALIFORNIA BILL WOULD REQUIRE LOCAL APPROVAL FOR STINGRAY USE

Berkeley law prof: "Communities ought to have a say in decisions like this."

An
get

wo
Tw
fin

Ars by e-mail. "In addition, this is one of the few times that there has been a public discussion BEFORE the acquisition of a stingray. There were no public discussions in Oakland, San Jose, or San Francisco when each of those police departments acquired a stingray, and they may not have even appeared on an agenda of the respective City Councils."

"I hope that this is a sign that sunlight is finally piercing the veil of the secrecy surrounding the use of this equipment," he added. "Use of this equipment is specifically kept hidden from judicial authority and the courts under the terms of the non-disclosure agreement that police departments must sign before they can buy a Stingray. 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."

Smith, the county executive, for his part was surprised to learn that Santa Clara may be the first local entity to refuse Harris' demands.

"We're not focused on being the only one to do something, but we had to do what we thought was right in terms of negotiations," he added. "If it's the only time it's happened, I'm surprised."

READER COMMENTS 32

Share Tweet Google+ Reddit



Cyrus Farivar / Cyrus is the Senior Business Editor at Ars Technica, and is also a radio producer and author. His first book, *The Internet of Elsewhere*, was published in April 2011.

[@cfarivar on Twitter](#)

← OLDER STORY

NEWER STORY →

YOU MAY ALSO LIKE

SITE LINKS

- [About Us](#)
- [Advertise with us](#)
- [Contact Us](#)
- [Reprints](#)

SUBSCRIPTIONS

- [Subscribe to Ars](#)

MORE READING

- [RSS Feeds](#)
- [Newsletters](#)

CONDE NAST SITES

- [Reddit](#)
- [Wired](#)
- [Vanity Fair](#)
- [Style](#)
- [Details](#)

[Visit our sister sites](#)

[Subscribe to a magazine](#)

CONDÉ NAST

© 2015 Condé Nast. All rights reserved

Use of this Site constitutes acceptance of our [User Agreement](#) (effective 1/2/14) and [Privacy Policy](#) (effective 1/2/14), and [Ars Technica Addendum](#) (effective 1/2/14) and [Your California Privacy Rights](#)

The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.

[Ad Choices](#)

City of Palo Alto Policy on Video Management

Revised January 2015

I. INTRODUCTION

The purpose of this Policy is to provide guidelines for the use of City-owned video management systems (VMS) and accompanying cameras that are permanently installed. Mobile, portable, wearable and other such audio/video systems are outside the scope of this Policy.

II. POLICY STATEMENT

The City of Palo Alto is committed to enhancing the quality of life of employees and residents of Palo Alto by integrating security practices with available technology. To enhance security of City property and aid investigatory capability, it may be appropriate to permanently install stationary video devices that are owned by the City of Palo Alto, and to ensure that the video systems currently in existence are governed by a single City-wide policy. The City remains committed to ensuring that all video systems are used in a manner that respects and balances the privacy interests of employees and residents.

Video systems will be used by various departments to monitor critical infrastructure that support on-going City services, prevent acts of vandalism, theft and other crimes, provide real-time situational awareness in the event of natural disasters or other critical incidents, assist with response to public safety incidents in the City, and, where appropriate, the investigation of criminal activity.

III. DEFINITIONS

“General Monitoring” refers to viewing recorded images from stationary cameras and monitors that have been approved under this Policy for the purpose of complying with City policies and laws and regulations.

“Specific monitoring,” for purposes of this Policy, refers to a more focused type of observation on an individual or group of individuals that involves: (1) realtime or live monitoring; (2) a closer degree of scrutiny related to the reasonable grounds to believe the person(s) who are the target of the monitoring are engaging in or have engaged in prohibited activity and (3) is designed to be investigatory and generally conducted over a longer timeframe. Specific monitoring does not include incidental observation or inadvertent discovery. For any specific monitoring activity to occur, there must be some connection between the information collected and unlawful activity.

“Operators” are those persons provided with access to any part of the VMS. Current staffing precludes the routine monitoring of cameras. Accordingly, operators may be capable of viewing live (real-time) or recorded video and other information, depending on their level of access.

“VMS Administrator” refers to the designee(s) of the City Manager, who shall oversee this Policy, as defined herein. As of January 2015, the designee(s), who are to form a committee and work collaboratively, are as follows: (1) the Director of Emergency Services; (2) a representative from the Palo Alto Utilities Department; and (3) a representative of the City Attorney’s Office.

IV. USE OF PERMANENTLY INSTALLED STATIONARY VIDEO EQUIPMENT

A. Rules

- 1) Application: The head of a City department (“applicant”) wishing to permanently install video cameras shall submit a written request (form) to the VMS Administrator with a statement justifying the benefit of installing such equipment. The application must include the proposed number and location of the device(s), the purpose of the installation, whether the location of the cameras involves recording of activity by employees or the general public or both, and the names and titles of the individuals who will be the operators. The source of funding for the installation must be specifically identified as part of the request.
- 2) Review: The VMS Administrator will review the request and advise the applicant of the decision within ninety (90) business days after receipt. The applicant may appeal the decision of the VMS Administrator by submitting an appeal to the City Manager or his/her designee, who will consult with the City Attorney’s Office and respond to the request within thirty (30) business days after receipt. The decision of the City Manager or his/her designee is final.
- 3) Equipment Specifications: The VMS Administrator will develop a specification that provides guidance regarding the type of equipment City departments may purchase, compatibility, installation (contractors, etc.), and other such implementation details.
- 4) Changes: An applicant may file a written request to change the location or limit the visual range of a specific installation of video equipment based on a belief that it infringes on a reasonable expectation of privacy or other protected rights. The request shall be submitted to the VMS Administrator and shall (a) identify the location, (b) identify the concern or issue, and (c) provide the suggested changes. The VMS Administrator shall respond to the request within ninety (90) business days after receipt. The response will be based on a reconsideration of the initial request to install the devices in light of the concerns. The appeal process is the same as paragraph 2, above.
- 5) Retroactive Provisions: Within twelve (12) months of the effective date of this Policy and the Equipment Specifications, all existing City-owned systems shall be brought into compliance with all aspects of this Policy. Those which do not conform shall be removed, unless a waiver is granted by the VMS Administrator.
- 6) Security: Operators shall exercise due care to ensure that video displays shall not be viewable by unauthorized persons.
- 7) Signage: Any area in which a video system is permanently installed shall have signage prominently displayed indicating the fact of monitoring. In cases in which there is an ongoing investigation, monitoring shall be governed by usual legal or City procedures, which may not require signage.

In the event third parties (such as private businesses and other non-government entities) desire to share their video feeds with the City, the following rules will apply:

- 1) Except for exigent circumstances or temporary (less than 90 days) access, the third party shall submit a written authorization form to the VMS Administrator, specifying which City department is to be granted access, for what duration (if any), and any other conditions or limitations.
- 2) The VMS Administrator shall maintain a registry of such third parties which have authorized the City of Palo Alto to have access to their video systems.

B. Training

- 1) Operators shall be trained in the technical, legal and ethical parameters of appropriate system use.
- 2) Operators shall receive a copy of this policy and provide written acknowledgement that they have read and understood its contents.
- 3) Certain operators, such as those in the 911 Communications Center and the Emergency Operations Center, may require additional training.

C. Operation

- 1) Monitoring will be conducted in a professional, ethical and legal manner. The system will not be used to invade the privacy of individuals or otherwise utilized in areas where the reasonable expectation of privacy exists. Monitoring shall not be used to harass, intimidate or discriminate against any individual or group.
- 2) Duties of Department Heads.
 - (a) Each Department Head shall designate the Operators and provide the list of staff to the VMS Administrator;
 - (b) Each Department Head shall keep this list of Operators up-to-date and ensure staff completes the required training (per Section B) and completes the VMS Employee Statement and other forms;
 - (c) Department Operators may engage in General Monitoring for the purpose of enhancing compliance with City policies as described in Section I herein;
 - (d) Department Operators shall not engage in Specific Monitoring except in instances of suspected criminal activity, natural disaster, or threat to public property or safety, unless authorized by the VMS; and
 - (e) Every Department Head shall ensure that they or their staff notify the VMS Administrator as soon as practicable of any instances of or planned Specific Monitoring.
- 3) Duties of VMS Administrator.
 - (a) The VMS Administrator may engage in General Monitoring for the purpose of enhancing compliance with City policies as described in Section I herein;
 - (b) The VMS Administrator shall have City-wide system access and may engage in realtime and Specific Monitoring in the event of natural disaster, law enforcement

emergency, imminent threat situation, authorized law enforcement investigation, for the purpose of system-wide threat and safety assessments, and/or with the approval of the Chief of Police or his/her designee or City Manager or his/her designee;

- (c) The VMS Administrator shall prepare an annual report to the City Manager and the Chief of Police containing information regarding system use City-wide; and
- (d) All requests for recordings or other system use that are made in connection with internal investigations, disciplinary matters, or criminal investigation shall be made to the VMS Administrator.

D. Storage, Public Records

- 1) Both current and archived recordings will be secured in accordance with current state of art and best practices.
- 2) The volitional public release of video images shall be done only with the authorization of the VMS Administrator and only with a properly completed written request.
- 3) Video images needed for a criminal investigation or other official reason shall be collected and booked in accordance with current departmental evidence procedures.
- 4) Requests for recorded video images from other government agencies or by the submission of a court order or subpoena shall be promptly submitted to the Police Department Communications Manager, who will research the request and submit the results of such search through the VMS Administrator to the City Attorney's office for further handling. Every reasonable effort should be made to preserve the data requested until the request has been fully processed by the City Attorney's office.
- 5) Video images captured by the system that are requested by the public or media will be made available only to the extent required by law. Except as required by a valid court order or other lawful process, video images requested under the Public Records Act will generally not be disclosed to the public when such video images are evidence in an ongoing criminal investigation in which a disposition has not been reached.
- 6) Recordings shall be retained for one (1) year in accordance with California Government Code Section 34090.6(a) and then will be erased or recorded over unless retained as part of a criminal investigation, a civil or criminal court proceeding, pursuant to a Preservation Notice issued by the City Attorney's Office. No attempt shall ever be made to alter any recording, except to enhance quality for investigative purposes and to blur elements (such as uninvolved bystander faces) consistent with other policies and common practice to preserve privacy, to preserve evidence or other such lawful and valid reason. The VMS may have network video recorders (NVRs) or similar mechanisms where images are "buffered" for a period of time before they overwritten. Such data are not considered recordings. A recording occurs when images are exported to another medium (such as a DVD).
- 7) Retained recordings will be destroyed at the appropriate time, which will be determined and directed by the City Attorney's Office.

E. Destruction or Tampering with Cameras or System Components

Any person who tampers with or destroys a camera or any part of the video system may be prosecuted in the criminal justice system as well as subject to discipline, up to and including termination, in the case of staff.

F. Routine Audits

The video system shall be subject to regular audits. Any unauthorized use of the video system shall be reported to the VMS Administrator as well as the City Manager or his/her designee.



POLICY AND SERVICES COMMITTEE ACTION MINUTES

Special Meeting
Wednesday, December 14, 2016

Chairperson DuBois called the meeting to order at 6:04 P.M. in the Community Meeting Room, 250 Hamilton Avenue, Palo Alto, California.

Present: DuBois (Chair), Kniss, Scharff

Absent: Berman

Oral Communications

None.

Agenda Items

2. Directions to Staff Concerning Further Requirements and Restrictions Related to Basement Construction and Dewatering.

MOTION: Vice Mayor Scharff moved, seconded by Chair DuBois to recommend the City Council direct Staff to:

1. Modify the Pilot Construction Dewatering Program (per the list below) approved by Council (on February 1, 2016), to apply to new applications after adoption (to the extent possible, for the 2017 construction season); and
2. Draft an ordinance codifying and enhancing the Construction Dewatering Program, with a goal of bringing the ordinance to Council in 2017, in order to be in place for projects not having either their Conditions of Approval or Building Permits by July 1, 2017, for the 2018 construction season; and
3. Explore the implementation and incentives for using advanced construction techniques such as cut-off walls.

ACTION MINUTES

AMENDMENT: Chair DuBois moved, seconded by Council Member XX to add to the Motion "Have Staff evaluate and bring options to Council regarding additional incentives such as the mandatory cone test, allowing a longer construction season if you use a cutoff wall and the idea of a required draw down test."

AMENDMENT FAILED DUE TO THE LACK OF A SECOND

AMENDMENT: Chair Dubois moved, seconded by Council Member XX to add to the Motion "Ask Staff to evaluate the idea of a temporary moratorium with the exception for those that participate in the pilot program."

AMENDMENT FAILED DUE TO THE LACK OF A SECOND

MOTION RESTATED: Vice Mayor Scharff moved, seconded by Chair DuBois to recommend the City Council direct staff to:

1. Modify the Pilot Construction Dewatering Program (per the list below) approved by Council (on February 1, 2016), to apply to new applications after adoption (to the extent possible, for the 2017 construction season); and
2. Draft an Ordinance codifying and enhancing the Construction Dewatering Program, with a goal of bringing the ordinance to Council in 2017, in order to be in place for projects not having either their Conditions of Approval or Building Permits by July 1, 2017, for the 2018 construction season; and
3. Explore the implementation and incentives for using advanced construction techniques such as cut-off walls.

MOTION PASSED: 2-1 DuBois no, Berman absent

The Committee took a break from 8:37 P.M. to 8:44 P.M.

1. Discussion and Recommendations for Data Collection and Privacy Policy Guidelines.

MOTION: Chair DuBois moved, seconded by Council Member Kniss to recommend Staff return to the Policy and Services Committee with a

ACTION MINUTES

potential Ordinance that would establish department policies and practices in order to reinforce the protection of individual privacy.

MOTION PASSED: 3-0 Berman absent

3. Discussion and Recommendations for the 2017 City Council Priority Setting Process and Retreat Planning.

NO ACTION TAKEN

Future Meetings and Agendas

ADJOURNMENT: Meeting was adjourned at 9:18 P.M.