



# 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.