

Ordinance No. 5450
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 Criteria and Procedures to Protect Personal Privacy in the
Acquisition and Use of Surveillance Technology and Provide for Ongoing
Monitoring and Reporting

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 after the close of 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 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 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: September 10, 2018

PASSED: October 1, 2018

AYES: DuBois, Filseth, Fine, Holman, Kniss, Kou, Scharff, Tanaka, Wolbach

NOES:

ABSTENTIONS:

ABSENT:

ATTEST:



City Clerk

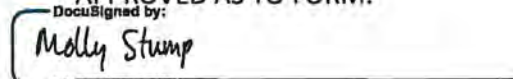
APPROVED:



Mayor
DocuSigned by:
Ed Shikada
E2DCA18CCC8D4F9

City Manager

APPROVED AS TO FORM:

DocuSigned by:


39AA73B853574A9
City Attorney

Certificate Of Completion

Envelope Id: 424B60F0D8334F279BFF5CDC3FF741AE	Status: Completed
Subject: Please DocuSign: ORD 5450 surveillance technology ordinance.docx	
Source Envelope:	
Document Pages: 5	Signatures: 2
Certificate Pages: 2	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Enabled	Beth Minor
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	250 Hamilton Ave
	Palo Alto , CA 94301
	Beth.Minor@CityofPaloAlto.org
	IP Address: 12.220.157.20

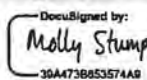
Record Tracking

Status: Original	Holder: Beth Minor	Location: DocuSign
10/17/2018 8:55:45 AM	Beth.Minor@CityofPaloAlto.org	
Security Appliance Status: Connected	Pool: City of Palo Alto	
Storage Appliance Status: Connected	Pool: City of Palo Alto	Location: DocuSign

Signer Events

Molly Stump
 molly.stump@cityofpaloalto.org
 City Attorney
 City of Palo Alto
 Security Level: Email, Account Authentication (None)

Signature



DocuSigned by:
 Molly Stump
 3DA473B853574A8

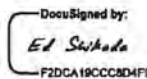
Signature Adoption: Pre-selected Style
 Using IP Address: 12.220.157.20

Timestamp

Sent: 10/17/2018 9:00:52 AM
 Resent: 10/18/2018 9:10:32 AM
 Viewed: 10/17/2018 11:44:50 AM
 Signed: 10/18/2018 1:56:41 PM

Electronic Record and Signature Disclosure: Not Offered via DocuSign

Ed Shikada
 ed.shikada@cityofpaloalto.org
 Assistant City Manager
 City of Palo Alto
 Security Level: Email, Account Authentication (None)



DocuSigned by:
 Ed Shikada
 F2DCA19CC8D4F9

Signature Adoption: Pre-selected Style
 Using IP Address: 12.220.157.20

Sent: 10/18/2018 1:56:42 PM
 Viewed: 10/23/2018 10:12:59 AM
 Signed: 10/23/2018 10:13:09 AM

Electronic Record and Signature Disclosure: Not Offered via DocuSign

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events

Status

Timestamp

Notary Events

Signature

Timestamp

Envelope Summary Events

Status

Timestamps

Envelope Sent	Hashed/Encrypted	10/18/2018 1:56:42 PM
Certified Delivered	Security Checked	10/23/2018 10:12:59 AM
Signing Complete	Security Checked	10/23/2018 10:13:09 AM

Envelope Summary Events	Status	Timestamps
Completed	Security Checked	10/23/2018 10:13:09 AM
Payment Events	Status	Timestamps