



**Privacy Advisory Commission**  
**May 3, 2018 5:00 PM**  
**Oakland City Hall**  
**Hearing Room 1**  
**1 Frank H. Ogawa Plaza, 3rd Floor**  
***Meeting Agenda***

---

**Commission Members:** *District 1 Representative: Reem Suleiman, District 2 Representative: Chloe Brown, District 3 Representative: Brian M. Hofer, District 4 Representative: Lou Katz, District 5 Representative: Raymundo Jacquez III, District 6 Representative: Clint M. Johnson, District 7 Representative: Robert Oliver, Council At-Large Representative: Saied R. Karamooz, Mayoral Representative: Heather Patterson*

---

*Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.*

1. 5:00pm: Call to Order, determination of quorum
2. 5:05pm: Review and approval of April meeting minutes
3. 5:10pm: Open Forum
4. 5:15pm: Surveillance Equipment Ordinance – discuss methodology and department outreach for survey of existing equipment.
5. 5:25pm: Streetline Status Report. Review and take possible action on report.
6. 5:30pm: Vehicle-mounted Automated License Plate Recognition (ALPR) for Parking Enforcement. Review and take possible action on use policy.
7. 6:10pm: Oakland Department of Transportation/Vendor use of UAV/Drones. Review and take possible action on use policy.
8. 7:00pm: Adjournment



**Privacy Advisory Commission**  
**April 5, 2018 5:00 PM**  
**Oakland City Hall**  
**Hearing Room 1**  
**1 Frank H. Ogawa Plaza, 3rd Floor**  
***Meeting Minutes***

---

**Commission Members:** *District 1 Representative: Reem Suleiman, District 2 Representative: Chloe Brown, District 3 Representative: Brian M. Hofer, District 4 Representative: Lou Katz, District 5 Representative: Raymundo Jacquez III, District 6 Representative: Clint M. Johnson, District 7 Representative: Robert Oliver, Council At-Large Representative: Saied R. Karamooz, Mayoral Representative: Heather Patterson*

---

*Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.*

1. 5:00pm: Call to Order, determination of quorum

*The meeting was called to order at 6:05. Members present: Hofer, Brown, Katz, Jaquez, Karamooz, Patterson. Members Absent: Suleiman, Johnson, Oliver.*

2. 5:05pm: Review and approval of February meeting minutes

*The minutes were approved with one minor correction to item 6.*

3. 5:10pm: Open Forum

*There were no Open Forum Speakers.*

4. 5:15pm: Introduction of new commissioners

*Members Chloe Brown who is the new appointee for District 2 and Heather Patterson who is the new appointee for the Mayor's Office had the opportunity to introduce themselves and share their motivation to be part of the Commission.*

5. 5:20pm: Presentation by UC Berkeley School of Information – CRIMS Privacy Assessment. Possible Action – Accept report; make recommendations to the City Council.

*Kimberly Fong and Steve Trush presented an overview of their report which carefully studied the Consolidated Records Information Management System maintained by Alameda County. Their findings indicated two major areas of concern: data sharing and the governance structure of CRIMS. The recommendations (included in the report in full) include developing a closer collaboration with Alameda County to determine data access issues, an assessment of the City's own Records Management System and how it interacts with CRIMS, and adding MOUs regarding data sharing to the soon to pass Surveillance Technology Ordinance.*

6. 5:45pm: Review and take possible action on Sanctuary City Contracting Ordinance

*The Commission reviewed the revised draft ordinance and approved it to be recommended to the City Council unanimously.*

7. 5:55pm: Review and take possible action on Cell Site Simulator Annual Report

*The Commission adopted a motion to accept the annual report and found the current uses to be valid.*

8. 6:10pm: Community Inquiry into Landlord Tax Audit/Business Revenue Data Requests (presentation by Strauss, Keenan). Possible Action – make recommendations to the City Council.

*Jonah Strauss of the Oakland Warehouse Coalition and David Keenan of Make Safe DIY Spaces presented their concern with a Citywide Audit of Commercial Landlords that was being conducted. The provided documentation displaying that the audit asks landlords to provide information about their commercial tenants that they find to be a violation of the tenants' privacy. They are concerned that in the wake of the Ghostship Fire, this effort is designed to cause the eviction of artists living in unpermitted commercial warehouses. They also raised concern that the City was not willing to provide them with a list of all landlords who received such a notice.*

*Joe DeVries told the Commission that the audit was developed in the wake of the Ghostship Fire but was one of several actions taken by the City after realizing that systems were not necessarily communicating with each other and there were gaps in information. Specific to this audit; it was sent to landlords who were paying taxes on commercial property but no business license existed on file for the address. This indicates a business operating without a license which is a violation. He also stated that the City would not provide the list of audited businesses as that information is protected.*

*The Commission decided to table any action on this item to a future meeting where a staff member from the Treasury Department could answer operational questions.*

# OAKLAND DEPARTMENT OF TRANSPORTATION

## [Proposed] Use Policy for Unmanned Aerial Vehicles (UAV)/Drones

### 1. Purpose

The unmanned aerial vehicles (UAV)/drones shall be used by city vendors for two purposes: 1) for project photography purposes to capture before and after impacts of transportation improvement projects in the public right of way, and 2) to rapidly assess roadway and infrastructure conditions without endangering city staff on public and private properties following a natural disaster (mudslide, flood, earthquake, fire, sinkhole, etc.).

### 2. Authorized Use

- Project photography (before and after images of street improvement projects)
- Assessment of conditions following a natural disaster
- All other uses not referenced above shall be prohibited.

### 3. Data Collection

The following data may be obtained through UAVs/Drones:

#### Camera

- Regular still images
- Regular video images
- Thermal still and video images
- 3D video images

The system's camera will be activated only when the UAV is operating in the project area to be photographed, or when there is a reasonable suspicion that a natural disaster may have caused unsafe conditions.

Any data obtained through the UAVs/drones must be used and handled pursuant to this policy.

### 4. Data Access

- Access to live mapping information and video image is limited to the pilots in command (PIC) and visual observers.
- Video footage/still images may be downloaded and viewed by relevant city staff.
- Video footage/still images may be released publicly in accordance with the Department's existing image sharing practices.

### 5. Data Protection

Vendors will be procured to operate UAVs/drones with specific project locations/emergency response locations identified.

Access to live data is limited to the following vendors:

- Pilots in command (PIC)
- Visual observers

Copies of video or still images shall be released to the project manager for project photography of street improvement projects and city staff assigned to respond to emergencies in the event of a natural disaster.

## **6. Data Retention**

Similar to existing project photographs and video footage/still images related to natural disasters, data may be retained by the Department of Transportation in perpetuity and shared publicly to increase awareness and understanding of the purpose and impacts of street design improvements and/or to notify the public of the severity of natural disasters.

## **7. Public Access**

The public may access photographs and videos that are not publicly shared by request.

## **8. Third-Party Data-Sharing**

Video footage or photographs may potentially be shared with the following:

- The public to increase awareness and understanding of transportation improvement projects and natural disasters
- Data on natural disasters may be shared with relevant utility companies (e.g. PG&E) and partner agencies (e.g. EBMUD, Caltrans)
- Investigating Officer
- District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence
- Parties in a civil litigation involving the County, in response to a subpoena
- Defendant in a traffic matter, in response to subpoenas issued by the defendant
- Pursuant to a Court Order

## **9. Training**

Training for operating the UAVs/drones will be provided by the vendor and will be limited to staff assigned as PIC and Visual Observers. Vendors shall be trained in UAV safety and privacy procedures.

## **10. Auditing and Oversight**

The PIC shall complete and submit a preflight checklist and risk assessment to the vendor each time the UAV/drone flies. Vendors shall ensure that these operations are met.

## **11. Maintenance**

Vendors will be required to maintain the integrity of the data captured and the safety of the UAV.

# Anticipated Impact Report for Unmanned Aerial Vehicles (UAV)/Drones

## 1. Information Describing the Integrated Helicopter Mapping System and How It Works

An Unmanned Aerial Vehicle (UAV) is an aircraft that is intended to navigate in the air without an on-board pilot. UAVs are alternatively called Remotely Piloted Aircraft (RPA), Remotely Operated Vehicle (ROV), or Drone. UAVs are part of Unmanned Aircraft Systems (UAS) that include the necessary equipment, network and personnel to control UAVs.

Sample Image of a street improvement project that would be captured with a UAV:



### Camera

All cameras will be equipped with regular view for capturing still images and video footage. Depending on the need and vendor capacity, UAV cameras may use a thermographic camera that senses infrared radiation

and/or 3-D video footage. The sensors installed thermal imaging cameras use detection of infrared radiation, typically emitted from a heat source (thermal radiation), to create a "picture" assembled for video output.

Thermal imaging cameras detect the heat given off by an object or person. Thousands of sensors on the array convert the infrared energy into electrical signals, which create a video image. The infrared camera measures and displays a “thermal profile” of objects in relation to the temperature of surrounding objects. So a person, warmer than the surrounding air, appears “white” while the cooler surrounding air or buildings will appear in varying shades of gray. The “white” images do not always show a clear silhouette and, as such, are subject to the observer’s interpretation.

Sample UAV Image of Earthquake Rescue (Beichuan, China)



Sample Thermal Image to Identify People in the Dark (San Diego)





## **2. Proposed Purpose**

UAVs/drones will be used by city vendors for two purposes: 1) for project photography purposes to capture before and after impacts of transportation improvement projects in the public right of way, and 2) to rapidly assess roadway and infrastructure conditions without endangering city staff on public and private properties following a natural disaster (mudslide, flood, earthquake, fire, sinkhole, etc.).

When vendors are deployed to use UAVs for these situations, a pilot in command (PIC) and visual observers trained and assigned by the vendor to view live footage. The camera to record video footage and still imagery is activated only when in the project area, such as:

- **Project Photography**

Once the UAV enters the project area, vendors will be assigned to take still images and/or video footage of public rights-of-way from specific angles that capture the local of proposed or completed transportation improvement projects. The purpose of these photographs is to communicate our work to the public.

- **Emergency Response**

The Department of Transportation responds to many natural disasters that endanger public safety and the safety of staff. UAVs would allow staff to quickly respond to natural disasters and assess conditions that may be inaccessible or unsafe for staff to enter.

## **3. Locations Where UAVs May Be Deployed**

Federal guidelines state that UAVs may fly no higher than 400 feet and remain below any surrounding obstacles when possible. They must remain thoroughly clear of and not interfere with manned aircraft operations and must avoid other aircraft and obstacles at all times.

## **4. Potential Impact on Civil Liberties & Privacy**

The Department of Transportation recognizes that all people have an inalienable right to privacy and is committed to protecting and safeguarding this right. The Department will not capture still or video footage of persons in areas where there is an expectation of privacy without the individual's permission, unless responding to a natural disaster.

The Police Department also recognizes that the integrated helicopter mapping system could raise concerns regarding real and/or perceived threats to civil liberties and privacy. In general, the public is concerned about police surveillance equipment using powerful zoom lenses and thermal cameras that may be used for discriminatory targeting or other purposes. It must be noted that these devices will not be used by law enforcement for surveillance purposes. These photographs and video recordings are similar to existing project photographs and emergency response photographs presently taken by Department of Transportation staff.



## 5. Mitigations

To be determined.

## 6. Data Types and Sources

### Camera

- Regular still images
- Regular video images
- Thermal still and video images
- 3D video images

## 7. Data Security

Video footage or photographs may potentially be shared with the following:

- The public to increase awareness and understanding of transportation improvement projects and natural disasters
- Data on natural disasters may be shared with relevant utility companies (e.g. PG&E) and partner agencies (e.g. EBMUD, Caltrans)

## 8. Fiscal Cost

### Initial Purchase Cost

None. The Department of Transportation will not acquire UAV equipment; we will procure vendors as needed.

### Personnel Costs

There are no additional personnel costs associated with the use of vendor-owned UAVs.

### Ongoing Costs

Staff will procure vendor for project photography and emergency response through a competitive process, following the City of Oakland's contracting procedures.

### Potential Sources of Funding

The integrated helicopter mapping system will be fully funded with grants from UASI (Urban Areas Security Initiative) and SHSGP (State Homeland Security Grant Program).

## 9. Third Party Dependence

Data will be processed and handled by a third party vendor who will share images and footage with the relevant Department of Transportation staff.

## 10. Alternatives

Project photography: an alternative that the Department of Transportation has employed is the use of electrical services "bucket" trucks, typically used to service traffic signals. This effort has proved an unsustainable use of staff time: rather than servicing broken signals and lights, electricians are deployed to project locations to take photographs. Capacity to complete this work has been limited.

Emergency response to natural disasters: presently, Department of Transportation staff

take photographs from ground level to capture impacts of natural disasters, and in certain circumstances, staff can't fully assess the scene of a natural disaster if conditions are unsafe to enter. Further, staff might enter an area believed to be safe from visual inspection, but may realize upon entry that there are hazards beyond their initial viewpoint that may endanger their safety.

## **11. Track Record**

We believe that the City of Oakland Department of Transportation would be the first transportation department to deploy the use of UAVs for the purposes outlined above.

City of Seattle

# MASTER LIST OF SURVEILLANCE TECHNOLOGIES



# CONTENTS

<b>EXECUTIVE SUMMARY.....</b>	<b>1</b>
<b>ABOUT THE MASTER LIST .....</b>	<b>2</b>
<b>SURVEILLANCE ORDINANCE .....</b>	<b>2</b>
<b>MASTER LIST REQUIREMENTS.....</b>	<b>2</b>
<b>NEXT STEPS.....</b>	<b>3</b>
<b>DEPARTMENT SUMMARY.....</b>	<b>4</b>
<b>MASTER LIST .....</b>	<b>1</b>
<b>SEATTLE CITY LIGHT .....</b>	<b>1</b>
<b>SEATTLE DEPARTMENT OF TRANSPORTATION .....</b>	<b>2</b>
<b>SEATTLE FIRE DEPARTMENT.....</b>	<b>3</b>
<b>SEATTLE POLICE DEPARTMENT .....</b>	<b>4</b>
<b>APPENDIX A: METHODOLOGY .....</b>	<b>8</b>
<b>APPENDIX B: SURVEILLANCE CRITERIA.....</b>	<b>9</b>

## EXECUTIVE SUMMARY

The Seattle City Council passed Ordinance [125376](#), known as the “Surveillance Ordinance”, to provide greater transparency to City Council and the public when the City acquires technology that meets the City’s definition of surveillance. The Surveillance Ordinance, which took effect on September 1, 2017, outlines requirements that include: surveillance technology review and approval by City Council before acquisition, Council review and approval via ordinance for existing technologies, and reporting about surveillance technology use and community impact.

Surveillance Ordinance section three requires the City’s Chief Technology Officer to compile a Master List of surveillance technologies in use by City departments as of the date the Surveillance Ordinance took effect (“Master List”), and to submit this report within 90 days of the Surveillance Ordinance’s effective date (November 30, 2017).

Department privacy champions worked with the Seattle IT Privacy Team to identify surveillance technologies in use. The list in this report represents the best effort of departments to identify existing technologies based on the definition and criteria outlined in the Surveillance Ordinance. Should additional technologies that were in use as of September 1, 2017 be discovered, this report will be amended and resubmitted.

The following departments currently use surveillance technology. These departments will complete the retroactive approval process for these technologies as required by the Surveillance Ordinance.

Department	Number of Technologies
Seattle City Light	3
Seattle Department of Transportation	3
Seattle Fire Department	3
Seattle Police Department	19
<b>Total</b>	<b>28</b>

## ABOUT THE MASTER LIST

This report was mandated as part the Surveillance Ordinance ([125376](#)) approved by City Council in August 2017. It was compiled with active input of all City departments. The Master List was compiled through the process detailed in Appendix A, using the criteria detailed in Appendix B.

## SURVEILLANCE ORDINANCE

Ordinance [125376](#), also referred to as the “Surveillance Ordinance”, took effect on September 1, 2017 and has implications for the acquisition of new technologies by the City, and technologies that are already in use that may fall under the new, broader definition of surveillance.


SMC 14.18.020.B.1 charges the City’s Executive with developing a process to identify surveillance technologies subject to the Ordinance. Seattle IT, on behalf of the Executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in [Seattle IT Policy PR-02](#), the “Surveillance Policy”.

## MASTER LIST REQUIREMENTS

Surveillance Ordinance section 3 requires the City’s Chief Technology Officer to compile a Master List of technologies in use as of September 1, 2017 that meets the definition of surveillance technology (“Master List”). Specifically, the Surveillance Ordinance states:

Section 3. Notwithstanding the provisions of Chapter 14.18 of the Seattle Municipal Code, each City department may use surveillance technology that has not received prior Council approval under Chapter 14.18 when the technology is, as of the effective date of this ordinance, (1) in the department’s possession or (2) in the execution or closeout phase of acquisition or has had a purchase order issued, pursuant to the Chief Technology Officer’s authority under subsection 3.23.030.C of the Seattle Municipal Code; provided, that the department complies with the procedures set forth in this section for Council approval.

Each City department shall compile a list of all surveillance technology that it controls and is utilizing as of the effective date of this ordinance that are not covered by an exemption or exception to the requirements of this Chapter 14.18 of the Seattle Municipal Code and submit it to the CTO, or submit an affirmative statement that there are no such technologies. The list shall identify for each technology whether the technology has received prior Council approval under Chapter 14.18, and if so, the ordinance number. The CTO shall compile a Master List that contains the information submitted by each department and a final list that identifies separately for each department the order in which the technology is recommended to be brought to the Council for ordinance approval. The Master List shall be filed within 90 days of the effective date of this ordinance with the City Clerk, with an electronic copy to the Chair of the committee responsible for public safety, the Director of Central Staff, the Chief Technology Officer, and the Inspector General for Public Safety. The CTO may make corrections to the master list, which must be timely filed with the City Clerk. Each City department shall submit requests for surveillance technology ordinance approval consistent with Chapter 14.18 of the Seattle



Municipal Code at a rate of at least one per month, or more when feasible, in list order, beginning no later than the end of the first quarter of 2018. The Council may revise or re-order the Master List by resolution.

Note that technologies exempted from Surveillance Ordinance compliance in SMC 14.18.030 are not included in the Master List.

## **NEXT STEPS**

After the submission of the Master List, departments will begin submitting Surveillance Impact Reports (SIRs) for Council approval at the rate of one per month, as required by the Surveillance Ordinance, starting no later than March 31, 2018.

If a department discovers a technology currently in place that is not enclosed in this Master List and meets the definition of surveillance as well as the requirements of the Surveillance Ordinance, it must be reported to the CTO immediately. At that time, the discovered technology will be added to the Master List and reported to Council.



## DEPARTMENT SUMMARY

Between September 1, 2017, and November 15, 2017, the Privacy Team, led by the City's Chief Privacy Officer, worked with departments to identify surveillance technologies that are currently in use. The table below notes if departments identified surveillance technologies in use within their department, and if so, how many.

Note the Surveillance Ordinance exempts the Seattle Municipal Courts and Seattle Public Library from compliance with the Surveillance Ordinance's requirements.

Department	Surveillance Technologies (Yes / No)	Number of Technologies
City Auditor	No	0
City Budget Office	No	0
Department of Education and Early Learning	No	0
Department of Neighborhoods	No	0
Finance and Administrative Services	No	0
Human Services Department	No	0
Legislative Department	No	0
Mayor's Office	No	0
Office of Arts and Culture	No	0
Office of Civil Rights	No	0
Office of Economic Development, Office of Film and Music	No	0
Office of Housing	No	0
Office of Immigrant and Refugee Affairs	No	0
Office of Intergovernmental Relations	No	0
Office of Labor Standards	No	0
Office of Planning and Community Development	No	0
Office of Sustainability and the Environment	No	0
Office of the Hearing Examiner	No	0
Retirement Office	No	0
Seattle Center	No	0
Seattle City Attorney	No	0
Seattle City Light	Yes	3
Seattle Department of Construction and Inspections	No	0
Seattle Department of Human Resources	No	0
Seattle Department of Transportation	Yes	3
Seattle Fire Department	Yes	3
Seattle Information Technology	No	0

Department	Surveillance Technologies (Yes / No)	Number of Technologies
Seattle Municipal Court	Exempt	N/A
Seattle Parks & Recreation	No	0
Seattle Police Department	Yes	19
Seattle Public Library	Exempt	N/A
Seattle Public Utilities	No	0
<b>Total</b>		<b>28</b>

## MASTER LIST

Technologies in use as of the effective date of this Surveillance Ordinance are listed below, organized by department. Each department ranked the order in which they will prepare Surveillance Impact Reports (SIRs) for submission to Council.

### SEATTLE CITY LIGHT

Seattle City Light (SCL) uses technology to ensure proper recording of electricity consumption, and is empowered by City of Seattle Ordinance [\(117490\)](#) to recover diverted power consumption. Additionally, federal regulatory requirements detail how SCL must monitor electrical usage. The tools and technologies listed below are used in the investigation of unbilled power usage as part of that obligation and as such meet the definition of surveillance and criteria for review.

Technology	Description	Proposed Review Order
<b>Binoculars/Spotting Scope</b>	The spotting scope is used to read meters from a distance when direct access to the meter is obstructed. Scopes are used by SCL's Current Diversion team to conduct investigations. Use of this technology may occur without informing a domicile's resident(s).	1
<b>SensorLink Amp Fork</b>	The SensorLink Amp Fork is used by SCL's Current Diversion team to measure the load on line-side entrance conductors, allowing SCL to determine the total amount of power being consumed at a service location. This tool provides an instantaneous reading to the group conducting the investigation. Use of this technology may occur without informing a domicile's resident(s).	2
<b>Check Meter Device</b>	This device measures the total amount of power being consumed at a service location where current diversion is confirmed or suspected. The device is set at the transformer and is used when a prolonged reading is desired by the Current Diversion team. Use of this technology may occur without informing a domicile's resident(s).	3

## SEATTLE DEPARTMENT OF TRANSPORTATION

The Seattle Department of Transportation is empowered by authority of Seattle Municipal Code ([SMC 11.16](#)) to monitor, record and optimize street use and traffic flow. The tools and technologies listed below are used in support of that mission, collecting and tracking identifiable individuals or vehicles and meet the definition and criteria for Council review. Ordinance and SMC authority for each technology is provide in the description field, below.

Technology	Description	Proposed Review Order
<b>License Plate Readers</b>	<p>License Plate Reader (LPR) cameras are a specialized CCTV camera with built in software to help identify and record license plates on vehicles. Travel times are generated by collecting arrival times at various checkpoints and matching the vehicle license plate numbers between consecutive checkpoints.</p> <p>This information is collected under the authority of <a href="#">SMC 11.16.200</a> requiring SDOT to keep records of traffic volumes.</p>	1
<b>Closed Circuit Television Equipment</b>	<p>SDOT has cameras installed throughout the City to monitor congestion, incidents, closures, and other traffic issues. The technology provides the ability to see roads, providing engineers with the necessary information to manage an incident and identify alternate routes. Every camera is available for live viewing by the public via our Traveler Information Web Map (<a href="http://web6.seattle.gov/Travelers/">http://web6.seattle.gov/Travelers/</a>). The video is not archived.</p> <p>This information is collected under the authority of <a href="#">SMC 11.16.200</a> requiring SDOT to keep records of traffic volumes.</p>	2
<b>Acyclica</b>	<p>Acyclica devices are in street furniture throughout the City and determine real time vehicle travel times in the City corridor by identifying WiFi-enabled devices in vehicles, such as smart phones, traveling between multiple sites. The identifying information is anonymized. Additionally, the data is deleted within 24 hours to prevent tracking devices over time.</p> <p>This information is collected under the authority of <a href="#">SMC 11.16.200</a>, requiring SDOT to keep records of traffic volumes, as well as <a href="#">SMC 11.16.220</a> requiring an annual report on traffic.</p>	3

## SEATTLE FIRE DEPARTMENT

Seattle Fire Department is committed to protecting life and property for Seattle residents. This requires the collection of photographic evidence and information at the scene of emergencies and other hazardous sites. This can include the capture of unidentifiable individuals and property as well as tracking of private inspection companies for compliance and documentation purposes.

Technology	Description	Proposed Review Order
<b>Emergency Scene Cameras</b>	Photos at incidents (not retained after transmission per department policy) are collected as part of the investigation and documentation of emergency responses and may include photographs of identifiable individuals and property.	1
<b>Hazmat Camera</b>	This wireless system transmits pictures related to hazardous materials sites to document and identify clean up and management requirements.	2
<b>Computer-Aided Dispatch</b>	Computer-aided dispatch (CAD) is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	3

## SEATTLE POLICE DEPARTMENT

Seattle Police Department (SPD) uses technologies to protect public safety and property and investigate and resolve crimes committed in the City of Seattle.

Note the Seattle City Council has mandated the submission of a Surveillance Impact Report for SPD's new records management system, Mark 43. This technology does not meet the criteria for a surveillance technology, and thus is not listed in the table below. In the of transparency on a project of public interest, SPD will complete the SIR and related community engagement requirements as directed.

Technology	Description	Proposed Review Order
<b>Automated License Plate Recognition (ALPR)</b>	ALPRs are computer-controlled, high-speed camera systems mounted on parking enforcement or police vehicles that automatically capture an image of license plates that come into view and converts the image of the license plate into alphanumeric data that can be used to locate vehicles reported stolen or otherwise sought for public safety purposes and to enforce parking restrictions.	1
<b>Booking Photo Comparison Software (BPCS)</b>	BCPS is used in situations where a picture of a suspected criminal, such as a burglar or convenience store robber, is taken by a camera. The still screenshot is entered into BPCS, which runs an algorithm to compare it to King County Jail booking photos to identify the person in the picture to further investigate his or her involvement in the crime. Use of BPCS is governed by <a href="#">SPD Manual §12.045</a> .	2
<b>Forward Looking Infrared Real-time video (FLIR)</b>	Two King County Sheriff's Office helicopters with Forward Looking Infrared (FLIR) send a real-time microwave video downlink of ongoing events to commanders and other decision-makers on the ground, facilitating specialized radio tracking equipment to locate bank robbery suspects and provides a platform for aerial photography and digital video of large outdoor locations (e.g., crime scenes and disaster damage, etc.).	3

Technology	Description	Proposed Review Order
<b>Undercover/ Technologies</b>	<p>The following groups of technologies are used to conduct sensitive investigations and should be reviewed together.</p> <ul style="list-style-type: none"> <li>• <b>Audio recording devices:</b> A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (<a href="#">RCW 9A.73.200</a>).</li> <li>• <b>Camera systems:</b> A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public.</li> <li>• <b>Tracking devices:</b> A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.</li> </ul>	4
<b>Computer-Aided Dispatch (CAD)</b>	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5
<b>CopLogic</b>	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
<b>Hostage Negotiation Throw Phone</b>	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7



Technology	Description	Proposed Review Order
<b>Remotely Operated Vehicles (ROVs)</b>	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
<b>911 Logging Recorder</b>	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
<b>Computer, cellphone and mobile device extraction tools</b>	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
<b>Video Recording Systems</b>	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
<b>Washington State Patrol (WSP) Aircraft</b>	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12
<b>Washington State Patrol (WSP) Drones</b>	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
<b>Callyo</b>	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14
<b>I2 iBase</b>	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15

Technology	Description	Proposed Review Order
<b>Parking Enforcement Systems</b>	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance <a href="#">SMC 11.35</a> .	16
<b>Situational Awareness Cameras Without Recording</b>	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
<b>Crash Data Retrieval</b>	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18
<b>Maltego</b>	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

## APPENDIX A: METHODOLOGY

The following steps were taken to complete the Master List requirement.

1. The Mayor's Office sent a City-wide email to notify City staff, department leaders, and privacy champions that the surveillance audit and inventory of technologies was required.
2. The Chief Privacy Officer presented the process and timeline to City executives and leaders to request resources and cooperation.
3. Privacy staff met with departments individually to discuss the overall process, discuss specific technologies, and make determinations about Master List technology inclusion.
4. Privacy champions and staff were provided with the surveillance checklist (see below) to assist in identifying surveillance technologies that meet Surveillance Ordinance requirements.
5. The list of technologies was validated against selection criteria and reviewed by the Chief Technology Officer prior to submission.

## APPENDIX B: SURVEILLANCE CRITERIA

### Surveillance Master List Questionnaire

#### Does the technology meet the following definition?

- ☐ Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.

#### Do any of the following exclusion criteria apply?

- ☐ Technology that is used to collect data where an individual knowingly and voluntarily provides the data.
- ☐ Technology that is used to collect data where individuals were presented with a clear and conspicuous opt-out notice.
- ☐ Technologies used for everyday office use.
- ☐ Body-worn cameras.
- ☐ Cameras installed in or on a police vehicle.
- ☐ Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of-way solely to record traffic violations.
- ☐ Cameras installed on City property solely for security purposes.
- ☐ Cameras installed solely to protect the physical integrity of City infrastructure, such as Seattle Public Utilities reservoirs.
- ☐ Technology that monitors only City employees in the performance of their City functions.

#### Do any of the inclusion criteria apply?

- ☐ The technology disparately impacts disadvantaged groups.
- ☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
- ☐ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
- ☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

To require a Surveillance Impact Review and inclusion on the Master List, the technology in question must meet the definition of surveillance, have no exclusion criteria and at least one inclusion criteria.

## County of Santa Clara

### Proposed Surveillance Use Policy Submission Schedule

<b>Group of Policies</b>	<b>Published on County Internet</b>	<b>Finance, Government, and Operations Committee (FGOC) Meeting</b>	<b>Board of Supervisors Meeting</b>
Yellow Group (see page 2)	Monday, April 30, 2018	Thursday, May 10, 2018	August 14, 2018 (1 <sup>st</sup> half of Yellow Group)
			August 28, 2018 (2 <sup>nd</sup> half of Yellow Group)
Orange Group (see page 3)	Monday, June 4, 2018	Thursday, June 14, 2018	September 11, 2018 (1 <sup>st</sup> half of Orange Group)
			September 25, 2018 (2 <sup>nd</sup> half of Orange Group)
Green Group (see page 4)	Monday, August 13, 2018	Thursday, August 23, 2018	October 16, 2018 (1 <sup>st</sup> half of Green Group)
			October 30, 2018 (2 <sup>nd</sup> half of Green Group)
Blue Group (see page 5)	Friday, August 31, 2018	Thursday, September 13, 2018	November 6, 2018 (1 <sup>st</sup> half of Blue Group)
			November 20, 2018 (2 <sup>nd</sup> half of Blue Group)

**Yellow Group**

<b>Department Name</b>	<b>Use Policy</b>
Office of the Sheriff	Automated License Plate Reader Technology
Office of the Sheriff	Ball Cameras
Office of the Sheriff	Callyo Mobile Bug
Office of the Sheriff	Command Vehicle Camera
Office of the Sheriff	Court Security and Safety Surveillance Equipment
Office of the Sheriff	Court Security Cameras
Office of the Sheriff	Crisis Negotiations Team ENT "Call Box" and Rescue Phone System
Office of the Sheriff	Digital Cameras and Video
Office of the Sheriff	Digital Voice Recorders
Office of the Sheriff	Facial Recognition Software
Office of the Sheriff	Flash Camera
Office of the Sheriff	L3 In-Car Video Recording System ("Dash Cam System")
Office of the Sheriff	Live Scan Machines and Mobile ID Fingerprint Machines
Office of the Sheriff	Live Trac PT-10 Plus Global Positioning System Tracking Devices
Office of the Sheriff	Trail Cameras
Office of the Sheriff	VideOversight Interview Recording and Case Management System
Office of the Sheriff Custody Bureau (DOC)	Safety and Security Surveillance Equipment

**Orange Group**

<b>Department Name</b>	<b>Use Policy</b>
Clerk of the Board	Audiovisual Recording Devices
Consumer & Environmental Protection Agency	Audio Recorders
Consumer & Environmental Protection Agency	Digital Cameras
Consumer & Environmental Protection Agency	Vector Control System Campus Security Cameras
County Communications Department	9-1-1 Audio Recording Equipment (NICE Logger System)
County Communications Department	Video Cameras Used for Facility Security
Countywide	Badge/Password-Access Technology for Multifunction Printer/Copying Machines
Countywide	Computers and Mobile Phones with Audiovisual Recording Capabilities
Countywide (by FAF)	Facility Access Control Technology
Dept. of Child Support Services	Exacq Video Security System
Dept. of Parks & Rec	Aerial Cameras and Global Positioning System Technologies
Dept. of Parks & Rec	Closed-Circuit Cameras
Dept. of Planning and Development	Audio Recorders
Dept. of Planning and Development	Digital Cameras
Facilities and Fleet	Security Cameras and Collected Data within the Facilities and Fleet Department
Facilities and Fleet	Telematics, a Vehicle Fleet Management Tool
Finance Agency - Clerk-Recorder	Security Cameras
Information Services Dept.	Security Cameras



**Green Group**

<b>Department Name</b>	<b>Use Policy</b>
Office of Pretrial Services	Electronic Alcohol Monitoring Devices
Office of Pretrial Services	Global Positioning System (GPS) Electronic Monitoring Devices
Office of the Assessor	Digital Cameras Used to Assess Property
Office of the Assessor	Video Cameras in the Assessor's Office
Office of the County Counsel	Digital Cameras and Audio Recorders
Office of the County Counsel	Network Server Camera
Office of the County Executive	Digital Camera
Office of the County Executive - Equal Opportunity Dept.	Audio Recorders
Office of the County Executive - Office of Emergency Services	Situational Awareness Tools
Office of the County Executive - Office of Reentry Services	Reentry Resource Center Security Cameras
Office of the Medical Examiner-Coroner	Digital Camera
Office of the Public Defender	Digital Cameras, Video Cameras, and Audio Recorders
Probation Dept.	Global Positioning System and Radio Frequency Devices
Probation Dept.	William F. James Ranch Video Security System
Procurement Dept.	Audio Recorders
Registrar of Voters	Security Cameras
Roads & Airports Dept.	Aircraft Noise and Operations Monitoring System
Roads & Airports Dept.	Facility Security Camera Systems
Roads & Airports Dept.	Telematics Technology
Social Services Agency	Call Center Phone Recording
Social Services Agency	Security Cameras

### Blue Group

Department Name	Use Policy
Office of the District Attorney	Data Extraction/Examination Equipment
Office of the District Attorney	Digital Recorders
Office of the District Attorney	Electric Binoculars
Office of the District Attorney	Global Positioning System (GPS) Tracker
Office of the District Attorney	Third-Party Surveillance Technology
Office of the District Attorney	Video Surveillance and Recording of Evidence Storage Facility
Office of the District Attorney - Crime Lab	Access Card and Biometric Fingerprint Systems
Office of the District Attorney - Crime Lab	Digital and Multimedia Evidence Unit Software and Tools
Office of the District Attorney - Crime Lab	Security Cameras
Office of the Sheriff Custody Bureau (DOC)	Booking Photograph Cameras
Office of the Sheriff Custody Bureau (DOC)	Handheld Digital Cameras
Office of the Sheriff Custody Bureau (DOC)	Inmate Telephone Monitoring
Office of the Sheriff Custody Bureau (DOC)	Portable Digital Audio Recorders
Santa Clara Valley Health & Hospital System	Baby Match Technology Used at Santa Clara Valley Medical Center
Santa Clara Valley Health & Hospital System	Badge and Biometric Readers
Santa Clara Valley Health & Hospital System	FairWarning Electronic Health Record Privacy Monitoring System
Santa Clara Valley Health & Hospital System	Mobile Audio and Visual Recording Devices
Santa Clara Valley Health & Hospital System	NicView Camera Technology Used at Santa Clara Valley Medical Center
Santa Clara Valley Health & Hospital System	Security Cameras Used at SCVHHS Facilities
Santa Clara Valley Health & Hospital System	Vocera Communication Technology
Santa Clara Valley Health & Hospital System - Emergency Medical Services Agency	Mobile Area Routing & Vehicle Location Information System (MARVLIS)