POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

City of Seattle

MASTER LIST OF SURVEILLANCE TECHNOLOGIES

11.30.2017

Seattle
Information Technology

CONTENTS

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
Total	**28**

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
Total		**28**

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
Binoculars/Spotting Scope	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
SensorLink Amp Fork	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
Check Meter Device	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
License Plate Readers	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. This information is collected under the authority of SMC 11.16.200 requiring SDOT to keep records of traffic volumes.	1
Closed Circuit Television Equipment	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 (http://web6.seattle.gov/Travelers/). The video is not archived. This information is collected under the authority of SMC 11.16.200 requiring SDOT to keep records of traffic volumes.	2
Acyclica	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. This information is collected under the authority of SMC 11.16.200, requiring SDOT to keep records of traffic volumes, as well as SMC 11.16.220 requiring an annual report on traffic.	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
Emergency Scene Cameras	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
Hazmat Camera	This wireless system transmits pictures related to hazardous materials sites to document and identify clean up and management requirements.	2
Computer-Aided Dispatch	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
Automated License Plate Recognition (ALPR)	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
Booking Photo Comparison Software (BPCS)	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 SPD Manual §12.045.	2
Forward Looking Infrared Real-time video (FLIR)	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
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: 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 (RCW 9A.73.200). • **Camera systems**: 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. • **Tracking devices**: 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.	4
Computer-Aided Dispatch (CAD)	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
CopLogic	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
Hostage Negotiation Throw Phone	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
Remotely Operated Vehicles (ROVs)	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
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	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
Video Recording Systems	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
Washington State Patrol (WSP) Aircraft	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
Washington State Patrol (WSP) Drones	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
Callyo	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
I2 iBase	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
Parking Enforcement Systems	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 SMC 11.35.	16
Situational Awareness Cameras Without Recording	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
Crash Data Retrieval	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
Maltego	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.