

2018 Surveillance Impact Report

PARKING ENFORCEMENT SYSTEMS (INCLUDING ALPR)

SEATTLE POLICE DEPARTMENT



CONTENTS

- SURVEILLANCE IMPACT REPORT OVERVIEW 4**
- HOW THIS DOCUMENT IS COMPLETED4**
- PRIVACY IMPACT ASSESSMENT 5**
- PURPOSE5**
- WHEN IS A PRIVACY IMPACT ASSESSMENT REQUIRED?.....5**
- 1.0 ABSTRACT 6**
- 1.1 PLEASE PROVIDE A BRIEF DESCRIPTION (ONE PARAGRAPH) OF THE PURPOSE AND PROPOSED USE OF THE PROJECT/TECHNOLOGY..... 6
- 1.1 CONTINUED... 8
- 1.2 EXPLAIN THE REASON THE PROJECT/TECHNOLOGY IS BEING CREATED OR UPDATED AND WHY THE PIA IS REQUIRED. 8
- 2.0 PROJECT / TECHNOLOGY OVERVIEW8**
- 2.1 DESCRIBE THE BENEFITS OF THE PROJECT/TECHNOLOGY..... 8
- 2.2 PROVIDE ANY DATA OR RESEARCH DEMONSTRATING ANTICIPATED BENEFITS. 8
- 2.3 DESCRIBE THE TECHNOLOGY INVOLVED 9
- 2.3 CONTINUED... 10
- 2.4 DESCRIBE HOW THE PROJECT OR USE OF TECHNOLOGY RELATES TO THE DEPARTMENT’S MISSION..... 10
- 2.5 WHO WILL BE INVOLVED WITH THE DEPLOYMENT AND USE OF THE PROJECT / TECHNOLOGY? 10
- 3.0 USE GOVERNANCE 11**
- 3.1 DESCRIBE THE PROCESSES THAT ARE REQUIRED PRIOR TO EACH USE, OR ACCESS TO/ OF THE PROJECT / TECHNOLOGY, SUCH AS A NOTIFICATION, OR CHECK-IN, CHECK-OUT OF EQUIPMENT. 11
- 3.2 LIST THE LEGAL STANDARDS OR CONDITIONS, IF ANY, THAT MUST BE MET BEFORE THE PROJECT / TECHNOLOGY IS USED..... 11
- 3.3 DESCRIBE THE POLICIES AND TRAINING REQUIRED OF ALL PERSONNEL OPERATING THE PROJECT / TECHNOLOGY, AND WHO HAS ACCESS TO ENSURE COMPLIANCE WITH USE AND MANAGEMENT POLICIES. 12

4.0 DATA COLLECTION AND USE	13
4.1 PROVIDE DETAILS ABOUT WHAT INFORMATION IS BEING COLLECTED FROM SOURCES OTHER THAN AN INDIVIDUAL, INCLUDING OTHER IT SYSTEMS, SYSTEMS OF RECORD, COMMERCIAL DATA AGGREGATORS, PUBLICLY AVAILABLE DATA AND/OR OTHER CITY DEPARTMENTS.....	13
5.0 DATA STORAGE, RETENTION AND DELETION	17
6.0 DATA SHARING AND ACCURACY	18
7.0 LEGAL OBLIGATIONS, RISKS AND COMPLIANCE.....	21
8.0 MONITORING AND ENFORCEMENT.....	22
FINANCIAL INFORMATION.....	23
PURPOSE	23
1.0 FISCAL IMPACT.....	23
EXPERTISE AND REFERENCES.....	25
PURPOSE	25
1.0 OTHER GOVERNMENT REFERENCES	25
2.0 ACADEMICS, CONSULTANTS, AND OTHER EXPERTS	25
3.0 WHITE PAPERS OR OTHER DOCUMENTS	26
RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET.....	27
PURPOSE	27
ADAPTION OF THE RET FOR SURVEILLANCE IMPACT REPORTS.....	27
RACIAL EQUITY TOOLKIT OVERVIEW	27
RACIAL EQUITY TOOLKIT: TO ASSESS POLICIES, INITIATIVES, PROGRAMS, AND BUDGET ISSUES	27
1.0 SET OUTCOMES.....	28
2.0 INVOLVE STAKEHOLDERS, ANALYZE DATA	30
3.0 DETERMINE BENEFIT AND/OR BURDEN	33

4.0 ADVANCE OPPORTUNITY OR MINIMIZE HARM 33

5.0 EVALUATE, RAISE RACIAL AWARENESS, BE ACCOUNTABLE 34

6.0 REPORT BACK..... 35

PRIVACY AND CIVIL LIBERTIES ASSESSMENT 36

PURPOSE 36

WORKING GROUP PRIVACY AND CIVIL LIBERTIES ASSESSMENT..... 36

APPENDIX A: GLOSSARY 37

**APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND
OVERVIEW 40**

APPENDIX C: PUBLIC MEETING NOTICE(S)..... 40

APPENDIX D: MEETING SIGN-IN SHEET(S) 40

APPENDIX E: MEETING TRANSCRIPT(S)..... 40

APPENDIX F: LETTERS FROM ORGANIZATIONS 40

APPENDIX H: EMAILS FROM THE PUBLIC 40

APPENDIX I: LETTERS FROM THE PUBLIC..... 40

SURVEILLANCE IMPACT REPORT OVERVIEW

The Seattle City Council passed Ordinance [125376](#), also referred to as the “Surveillance Ordinance”, on September 1, 2017. This Ordinance 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”.

HOW THIS DOCUMENT IS COMPLETED

As Seattle IT and department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only; all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

PRIVACY IMPACT ASSESSMENT

PURPOSE

A Privacy Impact Assessment (“PIA”) is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

WHEN IS A PRIVACY IMPACT ASSESSMENT REQUIRED?

A PIA may be required in two circumstances.

- 1) When a project, technology, or other review has been flagged as having a high privacy risk.
- 2) When a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

1.0 ABSTRACT

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Seattle Police Department (SPD) facilitates the flow of traffic, assists with the collection of revenue related to parking violations in the City of Seattle, and recovers stolen vehicles through a number of means. Among these is Parking Enforcement Systems technology, which is used by SPD as a necessary tool in the following ways:

1. Scofflaw – SPD employs three vehicles (two vans, and one truck) with ALPR systems to identify parked vehicles in violation of the City Scofflaw Ordinance. Vehicles in violation are subject to booting, pending payment of past due balances.
2. Time-Restricted Parking Areas – 47 sedans, 54 scooters, 2 vans, and 1 truck are utilized to monitor time-restricted parking within the City. Five of the sedans are equipped with ALPR systems and operated by civilian employees to digitally “chalk” vehicles parked in time-restricted zones. Utilizing GPS location and stem-valve comparison technology, the system alerts on those vehicles that are in violation of the time zone restriction upon a second pass. The remaining vehicles are used in traditional pay to park enforcement, and for manually chalking vehicle tires in time-restricted locations.
3. Restricted Parking Zones (“RPZ”) means a portion of the street commonly used for vehicular parking where vehicles properly displaying a permit or other authorization are exempt from the posted RPZ. Seattle Department of Transportation provides SPD with a list of vehicles permitted to park in an RPZ. Parking Enforcement Officers may use ALPR to determine that a vehicle does not have the appropriate permit or authorization to park in an RPZ.
4. Parking Enforcement Officers may use ALPR using a list of vehicles reported stolen or sought in connection with criminal investigation to identify those vehicles and report their location to Dispatch.
5. Parking in the City is also monitored by Parking Enforcement officers on bicycles, foot, and scooters. ALPR is not used in this capacity.

SPD has nineteen vehicles equipped with Automated License Plate Readers (ALPR). Eight of these are Parking Enforcement and eleven are Patrol vehicles. Although ALPR use for Parking Enforcement differs from ALPR use by Patrol in some respects as described in this Surveillance Impact Report and in the ALPR (Patrol) Surveillance Impact Report, all rules and policies that govern ALPR use by SPD as mentioned in the Surveillance Impact Report for ALPR (Patrol) are applicable in the same manner as they are when ALPR is utilized by Parking Enforcement.

The actual surveillance technology in this Surveillance Impact Report (SIR) is Genetec’s AutoVu ALPR hardware, which may only be used for the distinctly different purpose of parking enforcement when used with combined with the following (non-surveillance) technologies:

1. **Genetec’s Patroller software**, the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera “read” and “hit” data is accessible.

Continued on next page...

1.1 Continued...

2. **Samsung devices** allow Officers to access the software required to write tickets and enter ticket information.
3. **Gtechna software** prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

Among parking enforcement technologies, privacy concerns are probably most correlated with ALPR data collection in pursuit of parking enforcement. ALPR collects license plate information from vehicles, which could be correlated with other information to personally identify individuals' vehicles and determine where they were parked at a given time, track the movements of innocent individuals, or be pooled with ALPR data from other agencies. Parking enforcement technologies also have the potential to affect individuals residing in vehicles who park in areas where parking regulations apply.

2.0 PROJECT / TECHNOLOGY OVERVIEW

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

Drivers in Seattle spend almost 60 hours per year looking for parking in the City. This contributes to congestion and traffic flow concerns. Traffic congestion has increased with population growth and development, and is likely to continue to increase with Viaduct demolition and other future development. Parking Enforcement systems assist the City in managing traffic flow, parking assets, and recouping revenue lost to parking violations (Scofflaw, time-restricted parking enforcement, RPZ violations, and metered parking).

Patrol and Parking Enforcement ALPR assist the City in locating stolen vehicles. In 2017, 3613 motor vehicle thefts were reported in the City of Seattle. Using ALPR, Parking Enforcement identified 318 confirmed stolen vehicles. During the first nine months of 2018, 2600 motor vehicle thefts were reported in the City of Seattle. Using ALPR, Parking Enforcement identified 349 confirmed stolen vehicles during that period.

2.2 Provide any data or research demonstrating anticipated benefits.

Revenue collected from parking citations for two years:
2016: \$19,705,640
2017: \$20,909,278

2.3 Describe the technology involved.

SPD parking enforcement technologies include: Genetec's AutoVu ALPR hardware, Genetec's Patroller software, Paylock's Bootview software, Samsung handhelds, and Gtechna software. Parking Enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). (See ALPR: Patrol SIR for more detailed description of BOSS).

Parking enforcement ALPR hardware consists of high definition infrared digital cameras that are mounted on three vehicles designated for scofflaw enforcement (these boot vans carry boot devices that can be mounted to immobilize vehicles in violation of scofflaw), and five Parking Enforcement vehicles – for a total of eight ALPR-equipped vehicles that are utilized for Parking Enforcement. The other 39 ticketing vehicles are not equipped with ALPR.

In Time-Limited, no pay parking areas, the ALPR systems in the five sedans digitally “chalk” parked vehicles using GPS location and stem-valve comparison technology. The system alerts on those vehicles that are in violation of the time zone restriction upon a second pass. In RPZs, ALPR can be used to determine whether a vehicle is permitted to park in the RPZ based on the Seattle Department of Transportation-issued list of vehicles currently permitted to park in the RPZ.

The City contracts with Genetec for the AutoVu ALPR system used by Parking Enforcement. Genetec provides Patroller software that works in tandem with cameras, installed by PCS Mobile, Genetec's hardware and install partner. Patroller is the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera “read” and “hit” data is accessible.

Twice a day, the License Plate Reader File (known as the HotList) is uploaded from the State of Washington into the ALPR system. The license plate numbers compiled on the HotList “may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders” (WSP Memorandum of Understanding No. C141174GSC; March 11, 2014). While ALPR-equipped Parking Enforcement vehicles will receive notifications of any license plate “hits” on the HotList, Parking Enforcement officers radio these in to Dispatch and take no action themselves (see the Surveillance Impact Report for ALPR: Patrol for further information).

In addition to AutoVu, Parking Enforcement uses Paylock's Bootview software to assist SPD and Seattle Municipal Court enforce the [Scofflaw Ordinance](#), mandating the booting of vehicles in scofflaw (four or more unpaid violations). Municipal Court contracts with Paylock to assist with tracking the status of vehicles in violation of Scofflaw through its Bootview software program. SPD does not contract with Paylock or Bootview. Parking Enforcement Officers use the City of Seattle Municipal Court's [scofflaw list](#) - indicating those vehicles with four or more unpaid parking tickets subject to booting. Parking Enforcement Officers enforcing Scofflaw use this software to verify the current status of vehicles that are identified as being in violation of Scofflaw and to assist in determining whether a ticket should be issued.

Each configuration is designed so that the cameras capture the images and filter the reads through the linked software to determine if/when a hit occurs.

Continued on next page...

2.3 continued...

When the software identifies a hit, it issues an audible alert, and a visual notification informs the user as to what list the hit comes from –Scofflaw, time-restricted over time parking, or HotList.

- 1) If the user is utilizing the system to enforce Scofflaw violations, the user visually confirms the match and then verifies with Paylock’s Bootview (in-vehicle software linked to the Scofflaw list managed by Municipal Court) that the identified vehicle is in Scofflaw before taking further action.
- 2) In time-restricted parking enforcement, users rely on hits triggered by vehicles that have been digitally chalked and remain in time-restricted zones beyond allotted time. Once the user receives this hit, s/he visually verifies that the license plate read is accurate and, if so, does an image comparison of the tire to determine if the vehicle has moved since it was chalked at an earlier time before taking further action. Autovu’s patented tire valve stem technology assists users to make an accurate determination before issuing a violation. Hand-held devices, manufactured by Samsung, are used to 1) check the web-based Pay-by-Phone (contracted with SDOT) application, and parking meter data, to determine if vehicles in metered parking are in violation of their time limits, and 2) to issue citations for all parking infractions. Gtechna prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.
- 3) If a Parking Enforcement Officer receives notification of any license plate “hit” on the HotList, s/he radios it in to Dispatch and takes no further action themselves. SPD patrol or detectives assume responsibility for following up (see the SIR for ALPR: Patrol for further information).

2.4 Describe how the project or use of technology relates to the department’s mission.

Seattle Police Department utilizes Parking Enforcement Systems to uphold the law including Seattle’s [Traffic Code](#) and Seattle’s [Scofflaw Ordinance](#) and to ensure public safety by facilitating the flow of traffic and locating stolen vehicles.

2.5 Who will be involved with the deployment and use of the project / technology?

Parking Enforcement manages and oversees the deployment of ALPR-equipped vehicles for Scofflaw booting and time-restricted parking enforcement. Trained civilian Parking Enforcement Officers (PEOs) are authorized to operate the 101 vehicles, including the eight Parking Enforcement vehicles equipped with ALPR (3 boot vans; five sedans). A Parking Enforcement Supervisor monitors and manages access to the AutoVu ALPR system for parking enforcement purposes. Each shift, the Parking Enforcement Supervisor assigns deployment to Parking Enforcement Officers. Officers monitoring time-restricted parking focus their efforts solely on time-restricted zones (e.g., digital chalking), while officers enforcing Scofflaw with the boot vans canvas the City (these vehicles do not chalk).

Parking Enforcement ALPR data collected by Scofflaw enforcement boot vans is stored with Patrol ALPR data in the Neology Back Office System Software (BOSS). The BOSS ALPR administrator is a member of the Technical and Electronic Support Unit (TESU), a unit within SPD that maintains administrative control of much of SPD’s physical technology. The unit staff is knowledgeable about investigative and forensic technology. (See ALPR: Patrol SIR for more detailed description of BOSS).

3.0 USE GOVERNANCE

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

Prior to gaining access to the ALPR system, potential users must be trained by other trained SPD Parking Enforcement officers. Once this training has been verified with the Parking Enforcement Supervisor, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remain logged into the system the entire time that the ALPR system is in operation. The login is logged and auditable.

Parking Enforcement Officers are assigned the vehicles to use while on-shift, as well as a specific zone to monitor for time-restricted parking violations.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

For example, the purposes of a criminal investigation are supported by reasonable suspicion.

Parking Enforcement systems, including ALPR, can be used at any time.

Parking enforcement is governed by Seattle's [Traffic Code](#) and Seattle's [Scofflaw Ordinance](#). SPD ALPR systems can be used during routine patrol or specific to a criminal investigation (i.e., to locate a stolen vehicle), as per [SPD Policy 16.170](#). The policy specifies that the ALPR system administrator will be a member of the Technical and Electronic Support Unit (TESU). It further requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System ([ACCESS](#)) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only access ALPR data when that data relates to a specific criminal investigation. Records of these requests are purged after 90 days.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

Include links to all policies referenced.

[SPD Policy 16.170](#) addresses Automatic License Plate Readers. The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol (WSP) that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR.

Parking Enforcement officers are trained in the use of parking enforcement systems by trained Parking Enforcement Officers.

Compliance oversight is conducted by the Parking Enforcement supervisor.

DRAFT

4.0 DATA COLLECTION AND USE

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.

Data collected from ALPR include license plate image, computer-interpreted read of the license plate number, date, time, and GPS location. ALPR on Parking Enforcement vehicles, takes a burst of 26 pictures of each parked vehicle, for visual photo comparison when the same vehicle is later examined for time zone violation.

All ALPR-equipped vehicles upload a daily HotList that contains only license plate numbers, with the associated states, of stolen vehicles from NCIC and WASIC. The information downloaded will come from the NCIC hot file via ACCESS, currently managed by the Washington State Patrol (WSP). NCIC contains national stolen vehicle and plate data published daily by the FBI. The WSP places the NCIC file on a server available through ACCESS to those agencies that have a specific and signed agreement with WSP to access and use the information. SPD may supplement the list with additional information, such as vehicles sought in connection with an SPD criminal investigation.

Parking Enforcement vehicles equipped with ALPR are linked to the HotList; however, they take no action on hits generated from the list and request assistance from sworn officer(s). The Parking Enforcement Officer then returns to focusing on vehicles in violation of parking ordinances.

Boot van users connect to Bootview, a software program that contains information about individuals in Scofflaw. This list is created, and provided to Bootview, by Seattle Municipal Court. To be in scofflaw violation, a vehicle must have acquired four or more overdue, unpaid parking tickets and they must be found in the public-right-of-way. Booting is required whether a car is found parked illegally or legally.

When a user in a boot van receives a hit that a vehicle is in violation of scofflaw, s/he accesses Bootview to determine the most updated information about the scofflaw status. This system reports identifying information about the vehicle (license plate number, make, model, color) and information about past violations, as well as current information as to whether prior warnings or tickets have been issued. The hit from the Scofflaw list, coupled with the supporting information from Bootview helps users to determine whether to take action, which could include issuing a warning or booting a vehicle. Parking Enforcement also manages the Scofflaw Mitigation Program, in which officers assess scofflaw vehicles that appear to be lived-in vehicles and, in lieu of booting, provide contact information to assist individuals with payment of past-due fines, so as not to exacerbate a difficult situation.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

When the ALPR system registers a hit, the user must verify accuracy before taking any action. In Parking Enforcement, users verify first that a vehicle hit for Scofflaw violation is still actively in violation by checking for updated information in Bootview before booting a vehicle. Parking Enforcement Officers then visually verify that a vehicle suspected of time-zone restriction or metered parking violation is, in fact, in violation prior to issuing a ticket. Images captured serve as “evidence” that the system and the user are not in error.

Unless a hit has been exported for investigation and exported from the database for this purpose, all data captured by the five ALPR-equipped parking enforcement sedans is retained in the same database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days, per department retention policy (see ALPR Surveillance Impact Report).

Unless a hit has been exported for booting or investigation and exported for this purpose, all data captured by boot van ALPR is deleted when the Parking Enforcement Officer logs off the system at the end of shift.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Parking Enforcement is in operation Monday-Saturday, and with limited staffing on Sundays, for the purposes outlined above (see 1.0).

4.4 How often will the technology be in operation?

This technology may be used at any time, and on any day, during any given year.

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

Temporary – while in operation.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

In Parking Enforcement vehicles, ALPR cameras are in plain view, and the vehicle itself is advertised as a Parking Enforcement vehicle.

4.7 How will data that is collected be accessed and by whom?

Please do not include staff names; roles or functions only.

All data collected for Parking Enforcement systems are hosted on City SPD servers and are not accessible by vendors without knowledge and/or permission of City personnel. Unlike some ALPR systems, SPD's systems do not "pool" SPD's ALPR data with that collected by other agencies.

Only authorized users can access the data collected by ALPR for Parking Enforcement. Also, all activity by users in the AutoVu ALPR system is logged and auditable.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to authorized SPD personnel.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including [SPD Policy 12.040](#) - Department-Owned Computers, Devices & Software, [SPD Policy 12.050](#) - Criminal Justice Information Systems, [SPD Policy 12.080](#) – Department Records Access, Inspection & Dissemination, [SPD Policy 12.110](#) – Use of Department E-mail & Internet Systems, and [SPD Policy 12.111](#) – Use of Cloud Storage Services.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. that are applicable.

Access to the Parking Enforcement ALPR system is limited to ALPR-trained parking enforcement officers, the Parking Enforcement Supervisor, authorized SPD administrators, and authorized Seattle City IT administrators.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Users can only access the equipment and systems for purposes earlier outlined (see 1.0 above) – Scofflaw, parking enforcement, and criminal investigations.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (viewer logging, modification logging, etc.)?

Individuals can only access the Parking Enforcement AutoVu ALPR system via unique login credentials. Hardware systems can only be accessed in-vehicle (which are assigned by superiors for each shift), and Parking Enforcement software systems can only be accessed in-vehicle or on-site of SPD. As previously noted, all activity in the systems is logged and can be audited.

Further, City IT manages SQL on the system's backend that purges ALPR data at the required intervals (90 days). A record of the purge is generated and accessible at any time for verification of purges.

DRAFT

5.0 DATA STORAGE, RETENTION AND DELETION

5.1 How will data be securely stored?

All data collected from SPD's ALPR systems is stored, maintained, and managed on premises. Retention is automated, so that all ALPR data from the three ALPR-equipped Parking Enforcement boot vans is retained in the same BOSS database as ALPR data collected by ALPR-equipped patrol vehicles and is retained until automatically deleted after 90 days per department retention policy unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that citation or investigation (see ALPR: Patrol SIR for further detail). All data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift.

Unless a record is identified as being related to a parking violation or criminal investigation and exported in support of that matter, all data collected from the five ALPR-equipped Parking Enforcement sedans is deleted from the vehicle on-board system when the Parking Enforcement Officer logs off the at the end of the shift. No data from those sedans is retained by SPD except for records identified as being related to a parking violation or criminal investigation and exported during the shift it was captured.

Parking Enforcement systems that are contracted by SPD include only PCS Mobile's Patroller and Gtechna. Data collected by Patroller and Gtechna are hosted on City SPD servers.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

Systems utilized by Parking Enforcement keep logs of access and action. The Office of Inspector General may access all data and audit for compliance at any time.

5.3 What measures will be used to destroy improperly collected data?

Any citations issued by a Parking Enforcement Officer or booting for scofflaw violation can be contested by individuals. Users may make notes in records about license plate data captured that reflects that the hit is a misread, or that the hit was in error.

All information must be gathered and recorded in a manner that is consistent with [SPD Policy 6.060](#), such that it does not reasonably infringe upon "individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy."

All SPD employees must adhere to laws, City policy, and Department Policy ([SPD Policy 5.001](#)), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in [SPD Policy 5.002](#).

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Seattle City IT, in conjunction with SPD's Enforcement Supervisor, are responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG can review and ensure compliance, at any time.

6.0 DATA SHARING AND ACCURACY

6.1 Which entity or entities inside and external to the City will be data sharing partners?

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Seattle's [Scofflaw Ordinance](#) and [Traffic Code](#) require that SPD share information with Seattle Municipal Court.

Data may be shared without outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, [Chapter 42.56 RCW](#) ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department ([RCW 10.97.030](#), [SPD Policy 12.050](#)). Individuals can access their own information by submitting a public disclosure request.

Per [SPD Policy 12.080](#), the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by the parking enforcement systems may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by [SPD Policy 12.050](#) and [12.110](#). All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the [Mayor's Directive](#), dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by [SPD Policy 12.055](#). This sharing may include discrete pieces of data related to specific investigative files collected by the parking enforcement systems.

6.2 Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission as a law enforcement agency and to comply with legal requirements.

6.3 Are there any restrictions on non-City data use?

Yes No

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of [28 CFR Part 20](#). In addition, Washington State law enforcement agencies are subject to the provisions of [WAC 446-20-260](#), and [RCW Chapter 10.97](#).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies? Please describe the process for reviewing and updating data sharing agreements.

Research agreements must meet the standards reflected in [SPD Policy 12.055](#). Law enforcement agencies receiving criminal history information are subject to the requirements of [28 CFR Part 20](#). In addition, Washington State law enforcement agencies are subject to the provisions of [WAC 446-20-260](#), and [RCW Chapter 10.97](#).

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or way the parking enforcement systems may be used.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

Parking Enforcement systems technologies do not check themselves for errors. This is because the systems are unaware that they are gathering incorrect data. Instead, users are trained to visually verify accuracy (i.e., comparing a license plate hit from the system to the physical plate that the system read before taking any action). If they note a misread, they can enter a note into the system recognizing the read, as such. If they cannot verify visually, no action is taken.

Individuals can challenge citations, alleged scofflaw violations, or criminal charges and provide correct information.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals would not know that their information is collected inaccurately or erroneously in the normal course of ALPR data reading. This would only come to an individual's attention if a user acts on a hit received.

As it pertains to parking enforcement, individuals may contest booting action or a parking violation, and argue that the action was taken based on inaccurate or erroneous information, through the normal course of municipal proceedings.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department ([RCW 10.97.030](#), [SPD Policy 12.050](#)). Individuals can access their own information by submitting a public disclosure request.

DRAFT

7.0 LEGAL OBLIGATIONS, RISKS AND COMPLIANCE

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

ALPR use is not legally constrained at the local, state, or federal level. Instead, retention of data is restricted. Data collected by ALPR-equipped Parking Enforcement sedans other than that related to an alleged scofflaw violation or criminal investigation is deleted at the end of a Parking Enforcement Officer's shift. SPD has designated 90 days as the retention period for ALPR data from the three ALPR-equipped Parking Enforcement boot vans and the eleven ALPR-equipped patrol vehicles data that is not case specific (i.e., related to an investigation).

Parking Enforcement is authorized and mandated by Seattle's [Traffic Code](#) and Seattle's [Scofflaw Ordinance](#).

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

Users are trained in how to use the parking enforcement and ALPR systems and how to properly access data by other trained Parking Enforcement Officers. The Parking Enforcement Supervisor confirms the training before providing access to new users.

[SPD Policy 12.050](#) mandates that all employees, including Parking Enforcement Officers, who use terminals that have access to information in WACIC/NCIC files, must be certified by completing complete Security Awareness Training (Level 2) with recertification testing required every two years, and all employees also complete City Privacy Training. Failure to comply with ACCESS/NCIC/WACIC user requirements can result in termination of the right to continue using ACCESS services.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

As it relates to ALPR, each component of data collected, on its own, does not pose a privacy risk. Paired with other known or auditable information, however, an individual may be able to personally identify owners of vehicles, and then use that information to determine, to a certain degree, where specific vehicles have been located. Because SPD's ALPR cameras are not fixed in location, vehicles equipped with ALPR generally do not follow the same routes, and records are only retained for 90 days, this privacy risk is mitigated somewhat, as vehicle patterns more difficult to identify.

Per [SPD Policy 16.170](#), all users of ALPR are restricted from accessing the data, except as it relates to a specific criminal investigation. Appropriate SPD personnel can access the data (assuming it is within the 90-day retention period) as it relates to the active investigation.

Any activity by a user to access this information is logged and auditable. Washington State's Public Records Act requires release of collected ALPR data, however, making it possible for members of the public to make those identification connections on their own if they have access to the information necessary to do so, such as an independent knowledge of an individual's license plate number.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

Data collected by ALPR may cause the most concern, as it relates to Parking Enforcement. As mentioned in 7.3, the data could be used to personally identify individuals; however, SPD policy prohibits the use of data collected by ALPR to be used in any capacity by SPD personnel beyond its relation to a specific criminal investigation or parking enforcement action. Additionally, all collected Parking Enforcement from ALPR-equipped sedans is deleted when the Parking Enforcement Officer logs off the system at the end of shift, and all other collected ALPR data that is not relevant to an active investigation is deleted 90 days after collection.

8.0 MONITORING AND ENFORCEMENT

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Data collected by Parking Enforcement Systems is only disclosed pursuant to the public under the PRA. The only data available for disclosure is that data which remains in the system within the 90-day retention window.

Discrete pieces of data collected by ALPR may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by [SPD Policy 12.050](#) and [SPD Policy 12.110](#). All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the [Mayor's Directive](#), dated February 6, 2018. SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by [SPD Policy 12.055](#). This sharing may include discrete pieces of data related to specific investigative files collected by the devices.

Per [SPD Policy 12.080](#), the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any requests for disclosure are logged by SPD's Crime Records Unit or Legal Unit, as appropriate. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained in SPD's GovQA system for two years after the request is completed.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

Parking Enforcement Systems, including ALPR, do not self-audit. Instead, third party audits exist, as follows: 1) The Parking Enforcement Supervisor has the responsibility of managing the user list and ensuring proper access to the system; 2) The Office of the Inspector General (OIG) can also conduct an audit at any time. Violations of policy may result in referral to Office of Professional Accountability (OPA).

FINANCIAL INFORMATION

PURPOSE

This section provides a description of the fiscal impact of the surveillance technology, as required by the Surveillance Ordinance.

1.0 FISCAL IMPACT

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs

Current Potential

Date of Initial Acquisition	Date of Go Live	Direct Initial Acquisition Cost	Professional Services for Acquisition	Other Acquisition Costs	Initial Acquisition Funding Source
2012/2013 (Genetec)	2012/2013	\$18,085.050			SPD Budget
2014 (Gtechna)	2014	\$529,769.99			SPD Budget
2016 (PCS Mobile)	2016	\$263,123.68			SPD Budget

Notes:

These fiscal totals reflect the invoiced totals for the year of system/technology acquisition.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current Potential

Annual Maintenance and Licensing	Legal/compliance, audit, data retention and other security costs	Department Overhead	IT Overhead	Annual Funding Source
\$162,628.00				SPD Budget

Notes:

N/A

1.3 Cost savings potential through use of the technology

These are not quantified; however, potential cost savings may result from enhanced Parking Enforcement Officer efficiency. It may reduce distractions for Parking Enforcement Officers while driving because they do not have to visually scan chalk marks or license plates while driving.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

N/A

DRAFT

EXPERTISE AND REFERENCES

PURPOSE

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed Surveillance Impact Report (“SIR”). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 OTHER GOVERNMENT REFERENCES

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, Municipality, etc.	Primary Contact	Description of Current Use
Multiple Municipalities utilize different configurations of systems for parking enforcement		

2.0 ACADEMICS, CONSULTANTS, AND OTHER EXPERTS

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, Municipality, etc.	Primary Contact	Description of Current Use
Bryce Newell, PhD	Brycnewell@uky.edu	“Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy” – A Dissertation

3.0 WHITE PAPERS OR OTHER DOCUMENTS

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement	US Department of Justice (federally-funded grant report)	https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf
License Plate Readers for Law Enforcement: Opportunities and Obstacles	Rand Corporation	https://www.ncjrs.gov/pdffiles1/nij/grants/247283.pdf
Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information	66 Maine Law Review 398, 2014 Bryce Clayton Newell	https://cpb-us-w2.wpmucdn.com/wpsites.maine.edu/dist/d/46/files/2014/06/03-Newell.pdf

RACIAL EQUITY TOOLKIT AND ENGAGEMENT FOR PUBLIC COMMENT WORKSHEET

PURPOSE

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit (“RET”).

1. To provide a framework for the mindful completion of the Surveillance Impact Reports in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts Departments will complete as part of the Surveillance Impact Report.
2. To highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
3. To highlight and mitigate any disparate impacts on individuals or vulnerable communities.
4. To fulfill the public engagement requirements of the Surveillance Impact Report.

ADAPTION OF THE RET FOR SURVEILLANCE IMPACT REPORTS

The RET was adapted for the specific use by the Seattle Information Technology Departments’ (“Seattle IT”) Privacy Team, the Office of Civil Rights (“OCR”), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

RACIAL EQUITY TOOLKIT OVERVIEW

RACIAL EQUITY TOOLKIT: TO ASSESS POLICIES, INITIATIVES, PROGRAMS, AND BUDGET ISSUES

The vision of the Seattle Race and Social Justice Initiative is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The Racial Equity Toolkit lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

WHEN DO I USE THIS TOOLKIT?

Early. Apply the toolkit early for alignment with departmental racial equity goals and desired outcomes.

HOW DO I USE THIS TOOLKIT?

With inclusion. The analysis should be completed by people with different racial perspectives.

Step by step. The Racial Equity Analysis is made up of six steps from beginning to completion:

Please refer to the following resources available on the Office of Civil Rights’ website [here](#): Creating effective community outcomes; Identifying stakeholders & listening to communities of color; Data resources

1.0 SET OUTCOMES

1.1. Seattle City council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

- 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.

1.2 What are the potential impacts on civil liberties through the implementation of this technology?

Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. [SPD Policy 16.170](#) mitigates this concern by limiting operation to solely routine patrol or criminal investigation.

An additional potential civil liberties concern is that the SPD would over-surveil vulnerable or historically targeted communities, deploying ALPR to diverse neighborhoods more often than to other areas of the City.

1.3 What does your department define as the most important racially equitable community outcomes related to the implementation of this technology?

Trust in SPD is affected by its treatment of all individuals. Equity in treatment, regardless of actual or perceived race, gender, sex, sexual orientation, country of origin, religion, ethnicity, age, and ability is critical to establishing and maintaining trust.

Per the [2016 Race and Social Justice Initiative Community Survey](#), measuring “the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities,” 56.1% of African American/Black respondents, 47.3% of Multiracial respondents, and 47% of Indian/Alaska Native respondents have little to no confidence in the police to do a good job enforcing the law, as compared with 31.5% of White respondents. Further, while 54.9% of people of color have a great deal or fair amount of confidence in the police to treat people of color and White people equally, 45.1% of people of color have little to no confidence in the police to treat people equitably. This is contrasted with White respondents, of which 67.5% have a great deal or fair amount of confidence in the police to treat people of color and White people equally. This may be rooted in feelings of disparate types of contact with the police, across racial groups. While 14.3% of White respondents, 14.7% of Asian/Pacific Islander respondents, and 16.7% of Latino/Hispanic respondents reported being questioned by the police, charged, or arrested when they had not committed a crime, some communities of color reported much higher rates (American Indian/Alaska Native -52.7%; Black/African American - 46.8%; and Multiracial - 36.8%) of this type of contact with the criminal justice system.

As it relates to ALPR, it is important that SPD continue to follow its policy of limiting use of the technology to strictly routine patrol or criminal investigation, as well as limiting access to ALPR data to only instances in which it relates to a specific criminal investigation. Further, continuing to audit the system on a regular basis, provides a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity.

The desired outcome is to ensure that Parking Enforcement occurs throughout the City equitably in areas where parking restrictions exist, without over-surveilling areas where historically targeted communities reside or congregate.

1.4 What racial equity opportunity area(s) will be affected by the application of the technology?

- | | |
|--|--|
| <input type="checkbox"/> Education | <input checked="" type="checkbox"/> Criminal Justice |
| <input type="checkbox"/> Community Development | <input type="checkbox"/> Jobs |
| <input type="checkbox"/> Health | <input type="checkbox"/> Housing |
| <input type="checkbox"/> Environment | <input type="checkbox"/> Other |

1.5 Are there impacts on:

- Contracting Equity
- Workforce Equity
- Immigrant and Refugee Access to Services
- Inclusive Outreach and Public Engagement
- Other

- Contracting Equity
- Workforce Equity
- Immigrant and Refugee Access to Services
- Inclusive Outreach and Public Engagement

2.0 INVOLVE STAKEHOLDERS, ANALYZE DATA

2.1 Departmental conclusions about potential neighborhood impacts of the technology. Are the impacts on geographic areas? Yes No

Check all neighborhoods that apply (*see map of neighborhood boundaries in Appendix A: Glossary, under "Seattle Neighborhoods"*):

- All Seattle neighborhoods
 - Ballard
 - North
 - Northeast
 - Central
 - Lake Union
 - Southwest
 - Southeast
 - Delridge
 - Greater Duwamish
 - East District
 - King County (outside Seattle)

Outside King County. Please describe:

[Respond here, if applicable.]

2.2 What are the racial demographics of those living in the area or impacted by the issue? (*see Stakeholder and Data Resources [here](#).*)

The demographics for the City of Seattle: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Other Pac. Islander - 0.4%; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

STOP: Department should complete RET questions 2.3 – 6 and Appendices B-I AFTER completing their public comment and engagement requirements.

2.3 Have you completed the following steps to engage the public? If you have not completed these steps, pause here until public outreach and engagement has been completed. (*See OCR's RET worksheet [here](#) for more information about engaging the public at this point in the process to ensure their concerns and expertise are part of analysis.*)

Create a public outreach plan. Residents, community leaders, and the public were informed of the public meeting and feedback options via:

- Email
- Mailings
- Fliers
- Phone calls
- Social media
- Other

The following community leaders were identified and invited to the public meeting(s):

- American Civil Liberties Union (ACLU)
- CARE
- Northwest Immigrant Rights
- OneAmerica
- JACL
- For Seattle Police Department only, Community Police Commissions
- Other:

[Please describe]

Engagement for Public Comment #1

Date of meeting: [Respond here.]

Location of meeting: [Respond here.]

Summary of discussion:
[Respond here, if applicable.]

Full meeting transcript, including City attendees, community leaders in attendance, and attendee demographic data, is attached as an appendix to the SIR

Engagement for Public Comment #2

Date of meeting: [Respond here.]

Location of meeting: [Respond here.]

Summary of discussion:
[Respond here, if applicable.]

Full meeting transcript, including City attendees, community leaders in attendance, and attendee demographic data, is attached as an appendix to the SIR

Engagement for Public Comment #3 (if applicable)

Date of meeting: [Respond here.]

Location of meeting: [Respond here.]

Summary of discussion:

[Respond here, if applicable.]

Full meeting transcript, including City attendees, community leaders in attendance, and attendee demographic data, is attached as an appendix to the SIR

Collect public feedback via mail and email

Number of feedback submissions received: [Respond here.]

Summary of feedback: [Respond here.]

Open comment period: [Respond here.]

Complete compilation of feedback is attached as an appendix to the SIR

Community Technology Advisory Board (CTAB) Presentation

Date of presentation: [Respond here,]

Summary of comments:

[Respond here.]

Complete meeting minutes and comments are attached as an appendix to the SIR

Any letters of feedback by CTAB members are attached as an appendix to the SIR

2.4 What does data and conversations with stakeholders tell you about existing racial inequities that influence people's lives and should be taken into consideration when applying/implementing/using the technology? (See OCR's RET worksheet [here](#) for more information; King County Opportunity Maps are a good resource for information based on geography, race, and income.)

[Respond to question 2.4 here.]

2.5 What are the root causes or factors creating these racial inequities? Mitigation strategies will be addressed in 4.1 and 5.3. *Examples: bias in process; lack of access or barriers; lack of racially inclusive engagement.*

[Respond to question 2.5 here.]

3.0 DETERMINE BENEFIT AND/OR BURDEN

Provide a description of any potential disparate impact of surveillance on civil rights and liberties on communities of color and other marginalized communities. Given what you have learned from data and from stakeholder involvement...

3.1 How will the technology, or use of the technology increase or decrease racial equity? What are potential unintended consequences? What benefits may result? Are the impacts aligned with your department's community outcomes that were defined in 1.0?

[Respond to question 3.1 here.]

3.2 What benefits to the impacted community/demographic may result?

[Respond to question 3.1 here.]

3.3 What are potential unintended consequences (both negative and positive potential impact)?

[Respond to question 3.1 here.]

3.4 Are the impacts aligned with your department's community outcomes that were defined in Step 1.0?

[Respond to question 3.1 here.]

4.0 ADVANCE OPPORTUNITY OR MINIMIZE HARM

Provide a mitigation plan for the impacts described in step 3.

4.1 How will you address the impacts (including unintended consequences) on racial equity? What strategies address immediate impacts? What strategies address root causes of inequity listed in 2.5? How will you partner with stakeholders for long-term positive change? If impacts are not aligned with desired community outcomes for surveillance technology (see 1a), how will you re-align your work?

Program Strategies:

[Respond here.]

Policy Strategies:

[Respond here.]

Partnership Strategies:

[Respond here.]

5.0 EVALUATE, RAISE RACIAL AWARENESS, BE ACCOUNTABLE

The following information must be provided to the CTO, via the Privacy Office, on an annual basis for the purposes of an annual report to the City Council on the equitable use of surveillance technology. For Seattle Police Department, the equity impact assessments may be prepared by the Inspector General for Public Safety.

The following information does not need to be completed in the SIR submitted to Council, unless this is a retroactive review.

5.1 Which neighborhoods were impacted/targeted by the technology over the past year and how many people in each neighborhood were impacted?

- All Seattle neighborhoods
- Ballard
- North
- NE
- Central
- Lake Union
- Southwest
- Southeast
- Greater Duwamish
- East District
- King County (outside Seattle)
- Outside King County. Please describe:

[Respond here, if applicable.]

5.2 Demographic information of people impacted/targeted by the technology over the past year...

To the best of the department's ability, provide demographic information of the persons surveilled by this technology. If any of the neighborhoods above were included, compare the surveilled demographics to the neighborhood averages and City averages.

[Respond to question 5.2 here.]

5.3 Which of the mitigation strategies that you identified in Step 4 were implemented in the past year? Specifically, what adjustments to laws and policies should be made to remedy any disproportionate impacts so as to achieve a more equitable outcome in the future.

Type of Strategy (program, policy, partnership)	Description of Strategy	Percent complete of implementation	Describe successes and challenges with strategy implementation

5.4 How have you involved stakeholders since the implementation/application of the technology began?

- Public Meeting(s)
- CTAB Presentation
- Postings to Privacy webpage seattle.gov/privacy
- Other external communications
- Stakeholders have not been involved since the implementation/application

5.5 What is unresolved? What resources/partnerships do you still need to make changes?

[Respond to question 5.5 here.]

6.0 REPORT BACK

Responses to Step 5 will be compiled and analyzed as part of the CTO’s Annual Report on Equitable Use of Surveillance Technology.

Departments will be responsible for sharing their own evaluations with department leadership, Change Team Leads, and community leaders identified in the public outreach plan (Step 2c).

PRIVACY AND CIVIL LIBERTIES ASSESSMENT

PURPOSE

This section shall be completed after public engagement has concluded and the department has completed the Racial Equity Toolkit section above. The Privacy and Civil Liberties Assessment is completed by the Community Surveillance Working Group (“Working Group”), per the Surveillance Ordinance which states that the Working Group shall:

“[p]rovide to the Executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the Working Group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the Working Group at least six weeks prior to submittal of the SIR to Council for approval. The Working Group shall provide its impact assessment in writing to the Executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the Working Group does not provide the impact assessment before such time, the Working Group must ask for a two-week extension of time to City Council in writing. If the Working Group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement.”

WORKING GROUP PRIVACY AND CIVIL LIBERTIES ASSESSMENT

[Assessment to be placed here.]

APPENDIX A: GLOSSARY

Accountable: (Taken from the Racial Equity Toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

ALPR: “Automated License Plate Readers”

Community Outcomes: (Taken from the Racial Equity Toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting Equity: (Taken from the Racial Equity Toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: “Department of Neighborhoods.”

Genetec’s Patroller software: a non-surveillance technology that is required for ALPR to be used for Parking Enforcement purposes, the interface and backend server through which retention periods are set (and auditable), user permissions are managed, user activity is tracked and logged, and camera “read” and “hit” data is accessible.

Gtechna software: a non-surveillance technology that is required for ALPR to be used for Parking Enforcement purposes, prints citations for vehicles found in violation of scofflaw, overtime zone parking, and metered parking.

Immigrant and Refugee Access to Services: (Taken from the Racial Equity Toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle’s civic, economic and cultural life.

Inclusive Outreach and Public Engagement: (Taken from the Racial Equity Toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual Racism: (Taken from the Racial Equity Toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional Racism: (Taken from the Racial Equity Toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

Neology Back Office System Software (BOSS): System through which ALPR camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera “read” and “hit” data, and manage user permissions.

Neology PIPS: Mobile license plate recognitions system installed in eleven Patrol vehicles.

OCR: “Office of Arts and Culture.”

Opportunity Areas: (Taken from the Racial Equity Toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: Education, Health, Community Development, Criminal Justice, Jobs, Housing, and the Environment.

Paylock’s Bootview software: a non-surveillance, Municipal Court technology that is required for APLR to be used for Parking Enforcement purposes, which tracks the status of vehicles in violation of Scofflaw through its Bootview software program.

Racial Equity: (Taken from the Racial Equity Toolkit.) When social, economic and political opportunities are not predicted based upon a person’s race.

Racial Inequity: (Taken from the Racial Equity Toolkit.) When a person’s race can predict their social, economic, and political opportunities and outcomes.

RET: “Racial Equity Toolkit”

Samsung devices: a non-surveillance technology that is required for APLR to be used for Parking Enforcement purposes, which allows Officers to access the software required to write tickets and enter ticket information.

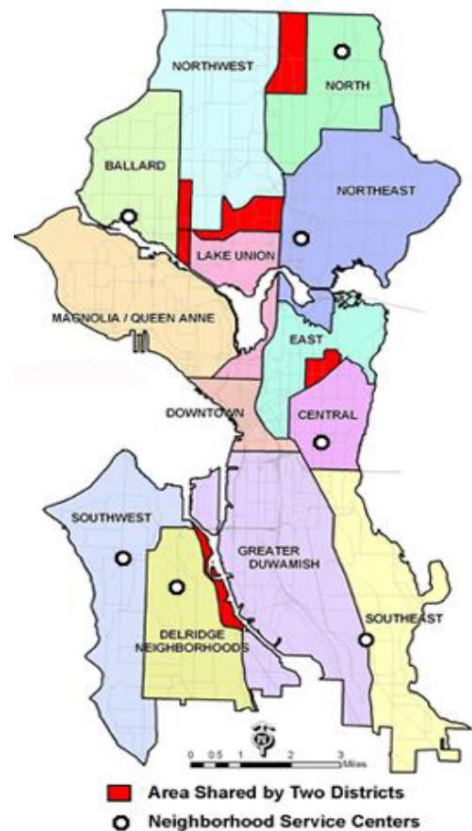
Seattle Neighborhoods: (Taken from the Racial Equity Toolkit Neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.


Stakeholders: (Taken from the Racial Equity Toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle Housing Authority, schools, community-based organizations, Change Teams, City employees, unions, etc.

Structural Racism: (Taken from the Racial Equity Toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance Ordinance: Seattle City Council passed Ordinance [125376](#), also referred to as the “Surveillance Ordinance.”

SIR: “Surveillance Impact Report”, a document which captures the fulfillment of the Council-defined Surveillance technology review process, as required by Ordinance [125376](#).





Workforce Equity: (Taken from the Racial Equity Toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

DRAFT

APPENDIX B: PUBLIC COMMENT DEMOGRAPHICS AND OVERVIEW

APPENDIX C: PUBLIC MEETING NOTICE(S)

APPENDIX D: MEETING SIGN-IN SHEET(S)

APPENDIX E: MEETING TRANSCRIPT(S)

APPENDIX F: LETTERS FROM ORGANIZATIONS

APPENDIX H: EMAILS FROM THE PUBLIC

APPENDIX I: LETTERS FROM THE PUBLIC

DRAFT