City of Seattle

2019 Surveillance Impact Report

ACYCLICA

Seattle Department of Transportation

DRAFT

Table of Contents

Surveillance Impact Report ("SIR") overview 3
Privacy Impact Assessment 4
Financial Information 16
Expertise and References 18
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 20
Privacy and Civil Liberties Assessment 31
Submitting Department Memo 32
Appendix A: Glossary 33
Appendix B: Public Comment Analysis 35
Appendix C: Public Comment Demographics 35
Appendix D: Comment Analysis Methodology 35
Appendix E: Questions and Department Responses 35
Appendix F: Public Outreach Overview 35
Appendix G: Meeting Notice(s) 35
Appendix H: Meeting Sign-in Sheet(s) 35
Appendix I: All Comments Received from Members of the Public 35
Appendix J: Letters from Organizations or Commissions 35
Appendix K: Supporting Policy Documentation 35
Appendix L: CTO Notification of Surveillance Technology 36

DRAFT

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. 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

This document is completed by the requesting department staff, support and coordinated by the Seattle information technology department ("Seattle it"). As Seattle it and department staff complete the document, they should keep the following in mind.

1. 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.
2. 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.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

DRAFT

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.

Acyclica is a provider of high resolution, real-time traffic congestion information. Acyclica's suite of traffic analytics software and sensor devices is currently being used by over 50 agencies both domestic and international to help to monitor and improve traffic congestion. Acyclica works with cities, municipalities, and transportation departments to aggregate and analyze data to bridge gaps in traditional traffic data services.

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

Acyclica meets inclusion criteria 3.2.1.3 from the PR-02 Surveillance Policy which states, "The technology collects data that is personally identifiable even if the data is obscured, de-identified, or anonymized after collection."

DRAFT

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.

SDOT has 301 Acyclica units installed throughout the City. Based on the data captured, SDOT has information that can be provided to travelers and traffic engineers. This information includes calculated average speeds for different monitored roadway segments, and average progress time along different monitored roadway segments, representative of travel time and delays. This data allows traffic engineers to correct traffic signal timing and provide information to travelers about expected delays.

Seattle Acyclica Locations.xlsx

In addition, the data generated by the use of Acyclica allows SDOT to meet records and reporting requirements 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.

2.2 Provide any data or research demonstrating anticipated benefits.

SDOT's preliminary deployment of Acyclica technology was along the Mercer Street. This corridor provides access to I-5, Seattle Center, and our growing technology business hub in South Lake Union. As one of the primary options for moving east and west across our City, Mercer Street was typically highly congested during the morning and evening commute. By using travel time data provided by Acyclica, we were able to accurately gauge how long it was taking people to make their way through the congestion. In 2017, we launched a new adaptive traffic signal system to help ease the backups. Prior to deployment, wait times during the height of work-week rush hour backups (between 6 and 7 PM) were approximately 34 minutes. Today, during that exact same time frame, the wait is down to 17 minutes. The information provided by Acyclica was incredibly valuable during this process, and we plan for it to continue informing our future data-driven decisions.

DRAFT

2.3 Describe the technology involved.

Acyclica technology collects encrypted media access control (MAC) address information and sends the data to the cloud using their RoadTrend Sensor. This sensor is a proprietary Linux-based device that is discreetly installed inside of traffic control cabinets for SDOT. The devices are Ethernet connected and have a Wi-Fi adapter capturing the MAC addresses of all devices within its range. Using the detection of MAC addresses, Acyclica identifies and differentiates vehicle movement as it approaches, stops and leaves an intersection. When Wi-Fi enabled device comes within range, the sensor generates a one-way hash code from the detected device's MAC address (using a SHA-256 algorithm). Only the hash codes are transmitted to their cloud server, and there is no way to reverse this process and access addresses of the original devices. From the aggregated data, Acyclica can extract and provide actionable traffic related information to SDOT.

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

This technology is part of the Mayor's Smart Cities initiative and creates new opportunities to use data to help reduce traffic congestion. SDOT's mission is to deliver a high-quality transportation system for Seattle. In our quickly growing city, moving people safely and reliably is an ever-increasing challenge. Technology can help us make more efficient use of our streets. Through Intelligent Transportation Systems (ITS), we can use communications technologies on the street and via automated traffic systems, to improve safety and mobility for all travelers. Travel time measurement gives SDOT the most important traffic information for indicating a road's mobility performance, and these measurements are the basis for decisions which improve the traffic operations of Seattle's road networks.

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

Deployment and maintenance of Acyclica devices is provided by Western Systems, a transportation solutions vendor with which the City has had a long relationship. SDOT Signal Electricians are also on site for every deployment to ensure the work is completed properly per standard practice. The data is primarily used by both our Traffic Signal Timing Engineers and Transportation Operations Center (TOC) staff. Timing Engineers work with modeling software to optimize traffic movements, and the travel time data provided by Acyclica informs the effectiveness of their actions. The TOC provides the data to commuters in real-time on both large roadside reader boards, and on the Traveler Information Map web application.

DRAFT

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City 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.

The City of Seattle is purchasing data as a service (terms are attached below). Past procurements have been funded by individual projects based on their performance metrics needs. Additionally, all new traffic signal cabinets will include Acyclica units as part of their standard build.

Western Systems owns, operates, and is responsible for maintenance and replacement of the hardware used to gather the data. The devices are then monitored for malfunction, and issues are resolved through cooperation between the two entities. Acyclica's aggregated data is available from their cloud server through a secure web portal. Only specified personnel have access to that site. The data is also available for consumption using a web application programming interface (API), which is what the TOC leverages to provide the information to the public.

Western Systems Terms

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

There are no legal standards dictating the deployment and use of Acyclica technology.

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.

Western Systems received on-site training from Acyclica on how to properly install and monitor the devices. Acyclica also works closely with the appropriate SDOT staff to ensure that they remain fully informed about all available system features. Acyclica also provides a manual for system administrators detailing how to configure sensors and routes, run analytics, create alerts, and integrate with the API:

AcyclicaUserGuide

Additonally, all SDOT employees are required to take annual Privacy and Information Security Awareness training as provided by Seattle IT.

DRAFT

4.0 Data Collection and Use

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.

Acyclica does not collect data from sources other than encrypted MAC addresses from Wi-Fi enabled devices.

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

A MAC address uniquely identifies a device connected to a network. MAC addresses are usually assigned by a manufacturer, and the information is hard-coded to the device and stored in its hardware. If device ownership changes, the device MAC address remains unchanged. Within the product and services provided by Acyclica, the applicable device is a mobile device. The intended design of the sensor devices limits the collection of MAC address data based upon the signal strength that is broadcasted to the Wi-Fi antenna within the designated traffic cabinets range (500-700 feet). This means that there is a focused effort to only capture data within the predetermined range which will provide the most relevant data.

When Wi-Fi enabled device comes within range, the sensor generates a one-way hash code from the detected device's MAC address (using a SHA-256 algorithm). Only the hash codes are transmitted to their cloud server, and there is no way to reverse this process and access addresses of the original devices. From the aggregated data, Acyclica can extract and provide actionable traffic related information to SDOT.

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?

SDOT has deployed Acyclica units on many of Seattle's primary road arterials since 2014, with the goal of having complete coverage on those identified streets. The attachment below identifies locations of all currently deployed Acyclica units in Seattle. The TOC/ITS Program Manager has final decision on where they are installed.

Past procurements have been funded by individual projects based on their performance metrics needs. Additionally, all new traffic signal cabinets will include Acyclica units as part of their standard build.

Seattle Acyclica Locations.xlsx

DRAFT

4.4 How often will the technology be in operation?

The technology collects data 24 hours a day, seven days a week, 365 days a year.

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

Acyclica devices are installed in traffic cabinets only accessible by qualified personnel. The City of Seattle is purchasing data as a service through Western Systems. Western Systems owns, operates, and is responsible for maintenance and replacement of the hardware used to gather the data. The devices can be moved from one location to another based on SDOT's needs.

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?

Although the RoadTrend sensor is installed inside of a traffic cabinet, communication is facilitated by affixing a low-profile antenna to its roof. The antenna is weather proof and adhered to the cabinet with sealant. The antenna is connected to the RoadTrend sensor by a wire that goes through a small hole that was drilled through the roof when the device was installed. No other indications are present distinguishing it from any other of our 1000+ roadside cabinets.

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

All aggregated traffic data will be accessed by SDOT personnel through Acyclica's web portal, or by applications leveraging the API. Users include:

1. Intelligent Transportation System Engineers
2. Transportation Operations Center Staff
3. Traffic Signal Timing Engineers
4. Traffic Operations Division Leadership

DRAFT

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

Deployment and maintenance of Acyclica devices is provided by Western Systems, a transportation solutions vendor with which the City has had a long relationship. Western Systems owns, operates, and is responsible for maintenance and replacement of the hardware used to gather the data. The devices are then monitored for malfunction, and issues are resolved through cooperation between the two entities.

Western Systems Terms

No user (including the vendor administrator) can access personally identifiable information from the web portal as it only provides the corresponding results of data aggregation. SDOT may provide access to the hashed data to consultants who are performing work on our behalf. This is accomplished by an SDOT administrator creating a user on Acyclica's front-end web application and providing those credentials to the consultant. Once the contract has concluded that user access will be eliminated. Types of accessible information include:

- Route Travel Times by Segment
- Speed
- Congestion Index
- Route Delay
- Progression Diagram
- Route Speed by Segment
- Timing Plan Analysis
- Day of Week Analysis
- Weekly Analysis
- Timing Run
- Delay by Phase
- Delay by Approach
- Idle Emissions
- Purdue Coordination Diagram

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

Acceptable reasons for access to the equipment include device installation or issue troubleshooting. Access to the data is permitted to perform traffic analysis, conduct research, create reports, or connecting to the API with software applications.

DRAFT

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.)?

Acyclica has created proprietary code that incorporates encryption technology using industry standard algorithm and cipher strengths, as well as inclusion of the use of a cryptographic hash function with a generated salt value.

A cryptographic hash function is a way to easily validate that a string of data corresponds to a specific hash value. If the original data string is unknown, but the stored hash value is known, by design, the cryptographic hash function makes it challenging to recreate the original data string. Utilization of hash function is intended to assure the integrity of data in transmission. In cryptography, a salt is a random piece of data that is used, in addition to a string of data, and in the creation of a hash value through use of a hash function. The primary function of salts is to prevent retro calculation of the hashed value if the hash function is known. Use of a salt precludes the effectiveness of using a list of possible pre-computed values since the salt is randomly generated.

With Acyclica's proprietary technology solutions, the salt rotates every 24 hours on the actual sensor device. The salt value is determined by timestamp which enables the hash to be dynamic. This encryption methodology is per industry standard protocols. Additionally, there is proprietary code that is running on the sensor device that performs the encryption function. The methodology of transmission to the cloud is a direct post to the back-end systems, versus an HTTPS transmission or broadcast over open, public networks which is considered less secure.

DRAFT

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Acyclica uses of a pared down proprietary Linux installation with a specific embedded Computer Processing Unit (CPU) chosen for processing optimization. Minimal storage is available on this device to enable only intended functionality and to also limit data retained. Additionally, there are specific access controls set to ensure restricted logical access to the device. Acyclica also employs logical access controls to ensure minimally assigned access and privileges, on a need-to-know basis. Vulnerability of systems is managed with patch procedures and change management processes, and logs are captured and monitored for maximum security awareness of the state of the devices and systems.

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

Acyclica has built specific security language into their contracts to clearly delineate the responsibilities between Acyclica and the customer/client for security of data and associated requirements. The aggregated traffic data is owned by SDOT, and there is a 10 year internal deletion requirement per item#42 of the SDOT Public Retention Schedule & Destruction Authorization Schedule:

SDOT Records Retention Schedule.

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

Acyclica hosts the aggregated traffic data on their servers, and the gathered data is encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall SDOT or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

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

The SDOT Transportation Operations Center (TOC) departmental unit is responsible for ensuring compliance with data requirements.

DRAFT

6.0 Data Sharing and Accuracy

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

SDOT receives and shares summarized traffic information with a variety of internal stakeholders, as well as the motoring public. However, the underlying anonymized data used to create that information is unavailable to SDOT or any other partner.

6.2 Why is data sharing necessary?

SDOT and data sharing partners have no access to the anonymized data used by Acyclica to create travel times and other information, but strictly the aggregated data related to traffic flow. The summarized traffic information that comes to SDOT and is shared with the public, is necessary to make traffic and route-planning decisions.

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.

The data provided by Acyclica is used for the purposes defined in the previous sections and for no other purposes.

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?

This question is not applicable to this technology.

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

If SDOT, in their sole discretion, determines that the analytics software is producing unacceptable travel time and delay metrics to such an extent that SDOT will not use the data for public information or their own analysis purposes, SDOT will notify Western Systems of the issue. Within 3 days, Western Systems must test the software and respond with a remediation plan and schedule to resolve the issue. If the issue is not resolved within the Contractor-stated time period, or if the issue lasts longer than 3 calendar months, SDOT will no longer pay for any portion of the system, and will notify Western Systems to remove the system, and the field devices, and the contract will be terminated.

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

The information provided through the Acyclica web portal and API is read-only, and we work directly with Acyclica if we have any questions about accuracy.

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?

The City of Seattle is purchasing Acyclica data as a service. Western Systems owns, operates, and is responsible for maintenance and replacement of the hardware used to gather the data.

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.

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

Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles. No user can access personally identifiable information from the web portal as it only provides aggregated data. Users are trained on how to use the web portal to pull reports relevant to their program or project. Applications of Acyclica technology include: signal timing & coordination, traffic network optimization, street parking congestion analysis, congestion mapping, route planning, work zone congestion enforcement, variable message signs, incident detection, emergency responder routing and route utilization.

Additionally, all SDOT employees are required to take annual Privacy and Information Security Awareness training as provided by Seattle IT.

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.

Risk: A specific individual's movements are tracked due to the implementation of this technology.

Mitigation: The only way to connect a MAC address to the mobile device owner or user is to work with a mobile carrier to associate the MAC address to an active mobile phone number listed on mobile customer's account. Acyclica protects the data using encryption technology embedded within proprietary code that secures MAC address at the device prior to transmission to the backend infrastructure for analysis. Other methods of securing the data include specific design and configuration of the backend infrastructure components, as well as industry standard security practices for access controls and logging, monitoring and alerting.

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?

The aspect of the technology that might cause public concern is by implying that the City is tracking the movements of individuals.

DRAFT

8.0 Monitoring and Enforcement

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

Public information requests are funneled to the appropriate staff member and tracked by SDOT administrative staff.

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.

On April 20th 2015, SDOT informed Acyclica about Seattle's privacy legislation. We asked that Acyclica obtain third party assurance from a licensed audit or security firm that the company's controls implemented to protect the privacy of individuals' data captured by their devices is maintained. This assessment was required to be performed in accordance with the AICPA AT-101 Attest engagement standard. Acyclica was instructed to consult with an audit firm of their choice to see if an existing audit standard is sufficient (e.g. SOC2 Privacy), or if a custom agreed-upon procedures assessment was necessary. We then requested a copy of the auditor's opinion and report, with the intention to make it public as part of our privacy assessment of the traffic management program.

Attest Engagement Standard 101.pdf

In response, Acyclica hired Coalfire Systems, Inc. to perform a privacy audit per our recommendations. They submitted the finalized report titled, "Acyclica White Paper: RoadTrend does not Capture PII" on Decmber 18th, 2015. SDOT will submit that paper as part of the Acyclica Surveillance Impact Report.

Acyclica White Paper_RoadTrend d

DRAFT

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
8/2014	8/2014	$355,885	$0	$0	Next Generation ITS

Notes:

Initial investment included 58 units.

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
$482,800	$0	$0	$0	Next Generation ITS

Notes:

Service fee is $1,775/unit per year.

DRAFT

1.3 Cost savings potential through use of the technology

According to King 5 News, “Seattle drivers spent an average of 55 peak hours in 2017 stuck in congestion, finishing ninth in the United States… Seattle drivers paid $1,853 each in 2017 for that privilege of being stuck in the city's traffic congestion.” Leveraging Acyclica’s data allows SDOT to improve traffic conditions for all Seattle travelers, which provides a quantifiable cost impact for those who experience delay.

If SDOT wanted to emulate the data collection provided by Acyclica using traditional means, we would have to employ a team of personnel to drive Seattle’s corridors 24x7x365 and report back on their travel time experiences. That data would then have to be entered into a database and managed by additional IT staff.

Pittman, Travis. “Seattle, Tacoma among worst traffic congestion in U.S., INRIX reports.” KING, 6 Feb. 2018, www.king5.com/article/news/local/seattle-tacoma-among-worst-traffic-congestion-in-us-inrix-reports/281-515147593.

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

This question is not applicable.

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
Boulder, CO	Mike Sweeney	Real-time and historical congestion monitoring
Henderson, NV	Alyssa Rodriguez	Signal timing analysis, connected vehicle

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
Transpo Group	Bruce Haldors	Signal Timing and adaptive performance integration
University of Washington	Mark Hallenbeck	Transportation Data Collaborative

DRAFT

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
Florence Boulevard Traffic Analysis	Acyclica Report	Florence Boulevard Traffic Analysis
Traffic Success: Greeley Colorado	Acyclica Report	Traffic Success: Greeley Colorado

DRAFT

Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR 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.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation 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

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET 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.

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.

DRAFT

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Despite Acyclica's anonymization of raw data prior to aggregation, the perception may exist that The City is tracking its citizen's movements by leveraging the technology.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

Acyclica makes it feasible to provide drivers with real time information about how long it will take to reach a given destination. Travel time is also a key piece of information for transportation agencies. Real-time travel time information allows SDOT to monitor roadway performance, identify problems, develop forecasts, plan future projects, and evaluate the effects of new projects.

The current deployment of the technology is primarily concentrated in and around the central business district and along several other major arterials. Through 2020 there are a series of technology projects installing Acyclica sensors along additional corridors including those that traverse historically diverse Seattle neighborhoods (e.g. Rainier Ave S and Martin Luther King Ways S).

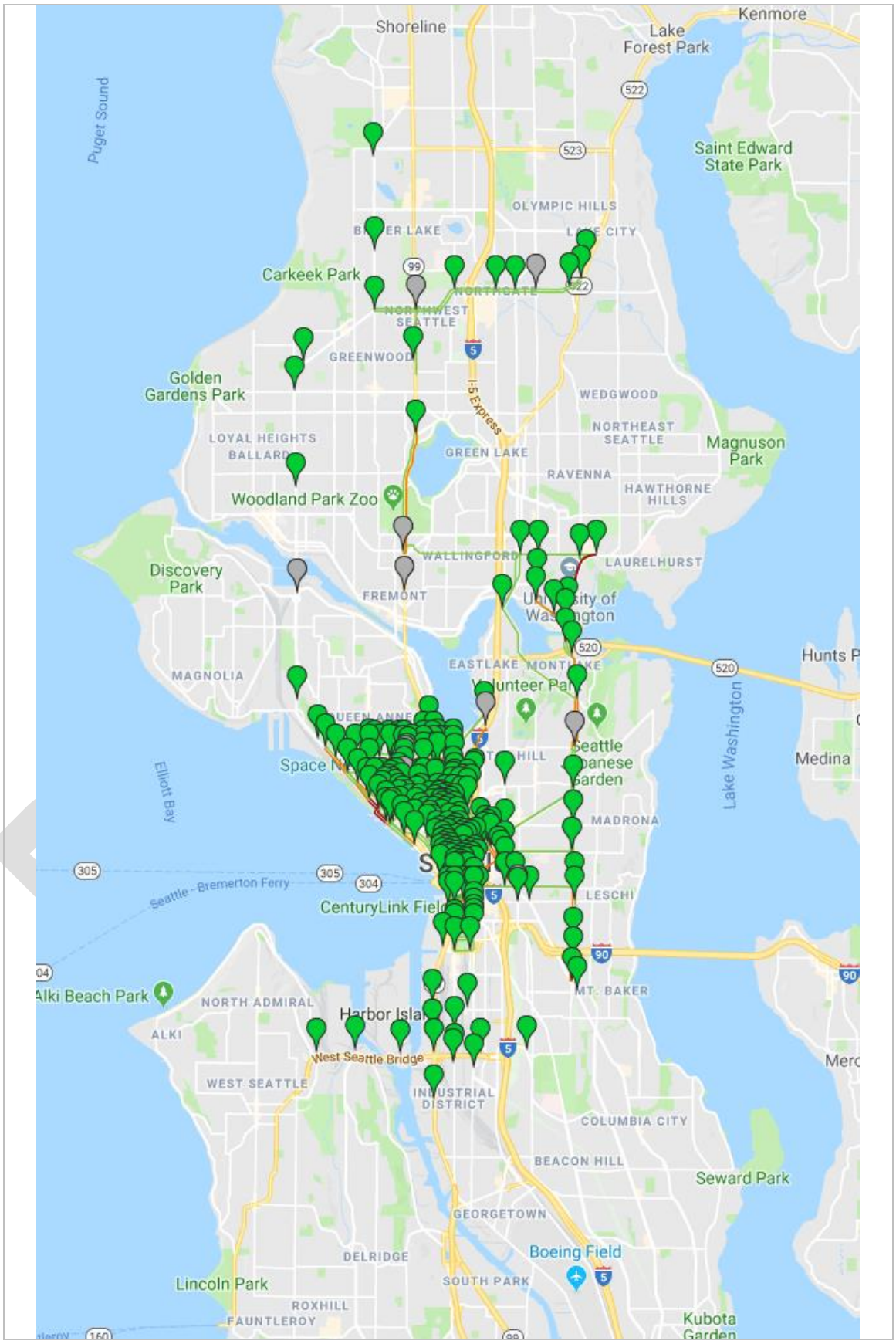
1.4 Where in the City is the technology used or deployed?

☐ all Seattle neighborhoods

- ☒ Ballard
- ☒ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☒ International District
- ☒ Interbay
- ☒ North
- ☒ Northeast
- ☒ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☒ South Lake Union / Eastlake
- ☒ Southeast
- ☒ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☒ West Seattle
- ☐ King county (outside Seattle)
- ☐ Outside King County.

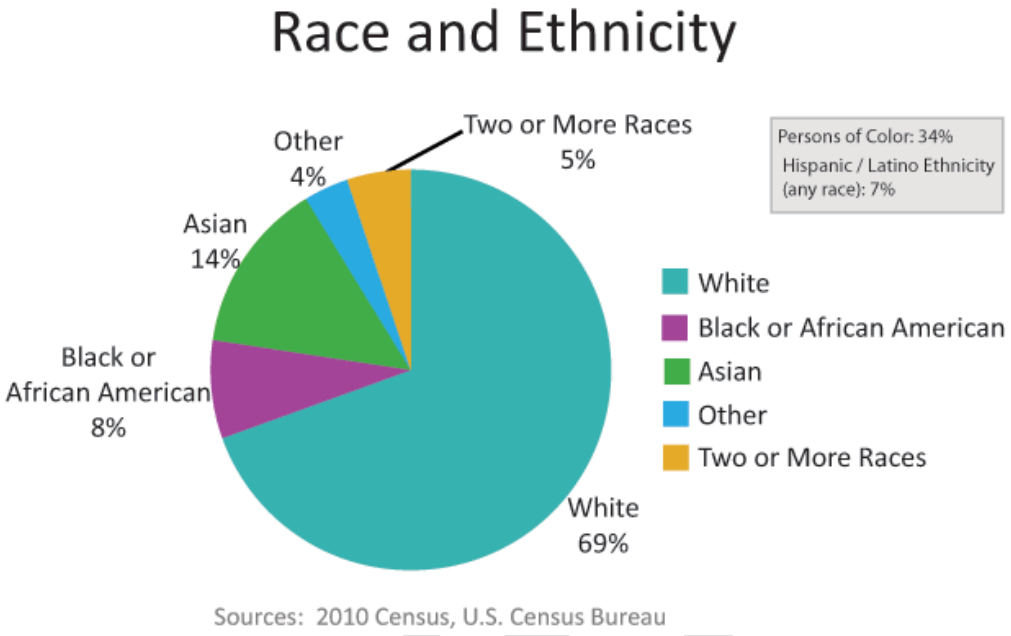
If possible, please include any maps or visualizations of historical deployments / use.

DRAFT


Shoreline
Kenmore
Lake Forest Park
Puget Sound
Saint Edward State Park
OLYMPIC HILLS
Carkeek Park
NORTHGATE
NORTHWEST SEATTLE
GREENWOOD
Golden Gardens Park
I-5 Express
WEDGWOOD
NORTHEAST SEATTLE
Magnuson Park
LOYAL HEIGHTS
BALLARD
GREEN LAKE
RAVENNA
HAWTHORNE HILLS
Woodland Park Zoo
WALLINGFORD
LAURELHURST
Discovery Park
FREMONT
MAGNOLIA
EASTLAKE
Hunts P
Lake Washington
Medina
Elliott Bay
MADRONA
Seattle - Bremerton Ferry
LESCHI
CenturyLink Field
Alki Beach Park
NORTH ADMIRAL
MT. BAKER
ALKI
West Seattle Bridge
WEST SEATTLE
INDUSTRIAL DISTRICT
COLUMBIA CITY
BEACON HILL
Seward Park
GEORGETOWN
Boeing Field
DELRIDGE
SOUTH PARK
Lincoln Park
ROXHILL
FAUNTLEROY
Kubota Garden

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

From Seattle's Office of Planning & Community Development, Race & Ethnicity Quick Statistics:



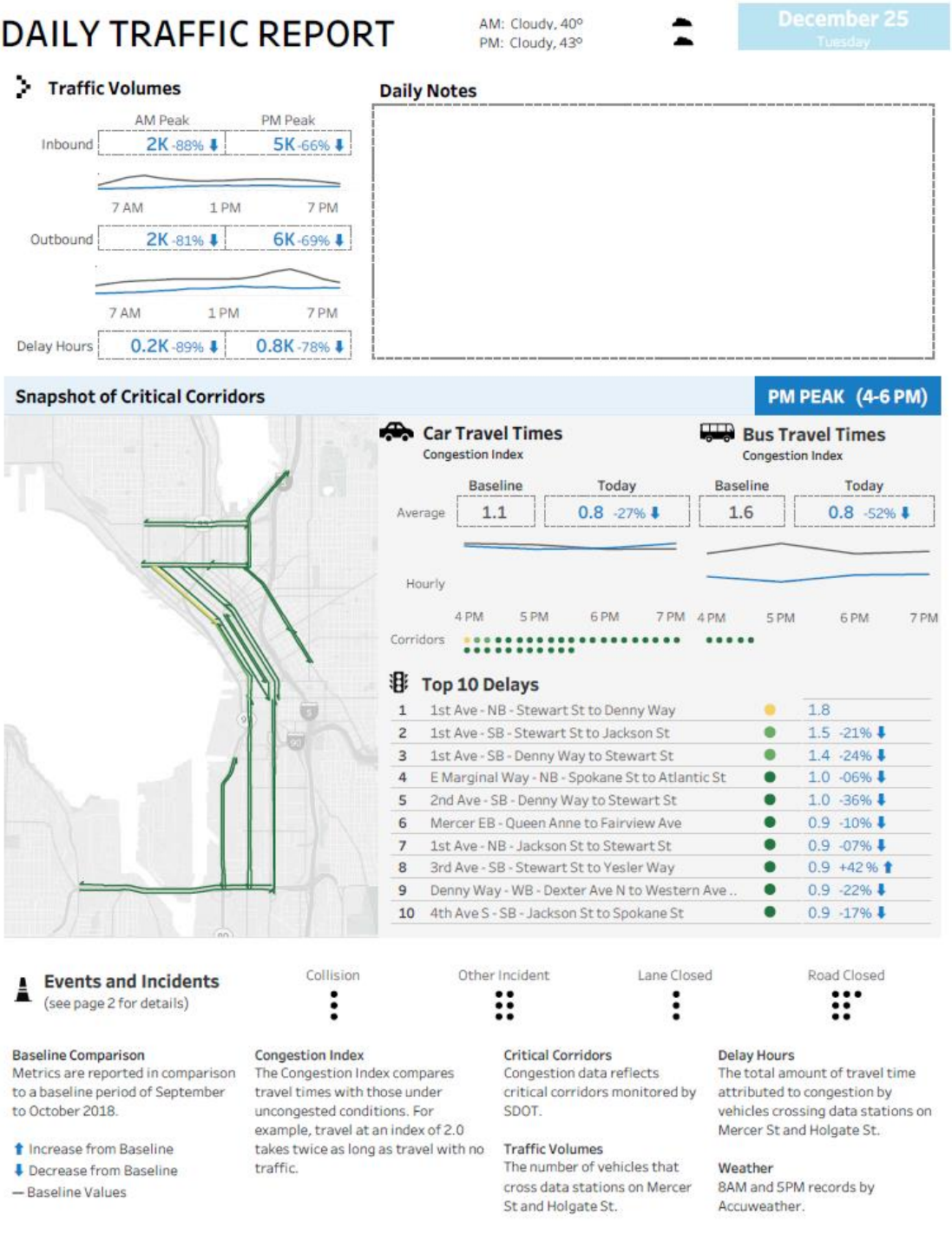
1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

Acyclica has created proprietary code that incorporates encryption technology using industry standard algorithm and cipher strengths, as well as inclusion of the use of a cryptographic hash function with a generated salt value. This anonymization ensures that the Department does not specifically target diverse neighborhoods, communities, or individuals through the use or deployment of this technology.

DRAFT

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The department is mitigating the risk for creating disparate impacts on historically targeted communities around data sharing by creating reports that combine information around traffic volumes and travel times which are sourced anonymously:



1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

All traffic data storage and retention policies are equal regardless of where the information is sourced from.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

To the extent that people are not able to access SDOT Travelers Information or are not aware of the SDOT information, they may find more difficulties with their commutes or they may avoid the downtown area if they are worried about the cameras. To the extent that travel time data lead to transportation infrastructure and investment in certain areas or for certain modes (autos) have the sense of perpetuating inequities or privilege for white communities.

DRAFT

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Please include a list of all organizations specifically invited to provide feedback on this technology.

1. ACLU of Washington	2. Ethiopian Community Center	3. Planned Parenthood Votes Northwest and Hawaii
4. ACRS (Asian Counselling and Referral Service)	5. Faith Action Network	6. PROVAIL
7. API Chaya	8. Filipino Advisory Council (SPD)	9. Real Change
10. API Coalition of King County	11. Friends of Little Saigon	12. SCIPDA
13. API Coalition of Pierce County	14. Full Life Care	15. Seattle Japanese American Citizens League (JACL)
16. CAIR	17. Garinagu HounGua	18. Seattle Neighborhood Group
19. CARE	20. Helping Link	21. Senior Center of West Seattle
22. Central International District Business Improvement District	23. Horn of Africa	24. Seniors in Action
25. Church Council of Greater Seattle	26. International ImCDA	27. Somali Family Safety Task Force
28. City of Seattle Community Police Commission (CPC)	29. John T. Williams Organizing Committee	30. South East Effective Development
31. City of Seattle Community Technology Advisory Board	32. Kin On Community Health Care	33. South Park Information and Resource Center SPIARC
34. City of Seattle Human Rights Commission	35. Korean Advisory Council (SPD)	36. STEMPaths Innovation Network
37. Coalition for Refugees from Burma	38. Latina/o Bar Association of Washington	39. University of Washington Women's Center
40. Community Passageways	41. Latino Civic Alliance	42. United Indians of All Tribes Foundation
43. Council of American Islamic Relations - Washington	44. LELO (Legacy of Equality, Leadership, and Organizing)	45. Urban League
46. East African Advisory Council (SPD)	47. Literacy Source	48. Wallingford Boys & Girls Club
49. East African Community Services	50. Millionair Club Charity	51. Washington Association of Criminal Defense Lawyers
52. Education for All	53. Native American Advisory Council (SPD)	54. Washington Hall
55. El Centro de la Raza	56. Northwest Immigrant Rights Project	57. West African Community Council
58. Entre Hermanos	59. OneAmerica	60. YouthCare
61. US Transportation expertise	62. Local 27	63. Local 2898
64. (SPD) Demographic Advisory Council	65. South Seattle Crime Prevention Coalition (SSCPC)	66. CWAC
67. NAAC		

DRAFT

2.1 Scheduled public meeting(s).

Meeting notes, sign-in sheets, all comments received, and questions from the public will be included in Appendix B, C, D, E, F, G, H and I. Comment analysis will be summarized in section 3.0 Public Comment Analysis.

Location	El Centro de la Raza: 1660 S Roberto Maestas Festival St. Seattle, WA 98144
Time	February 23, 2019; 11 a.m – 3 p.m.
Capacity	100+
Link to URL Invite	

2.2 Scheduled Focus Group Meeting(s)

Meeting 1

Community Engaged	
Date	

Meeting 2

Community Engaged	
Date	

DRAFT

3.0 Public Comment Analysis

This section will be completed after the public comment period has been completed on [DATE] by Privacy Office staff.

3.1 Summary of Response Volume

Dashboard of respondent demographics.

3.2 Question One: What concerns, if any, do you have about the use of this technology?

Dashboard of respondent demographics.

3.3 Question Two: What value, if any, do you see in the use of this technology?

Dashboard of respondent demographics.

3.4 Question Three: What would you want City leadership to consider when making a decision about the use of this technology?

Dashboard of respondent demographics.

3.5 Question Four: General response to the technology.

Dashboard of respondent demographics.

3.5 General Surveillance Comments

These are comments received that are not particular to any technology currently under review.

Dashboard of respondent demographics.

DRAFT

4.0 Response to Public Comments

This section will be completed after the public comment period has been completed on [DATE].

4.1 How will you address the concerns that have been identified by the public?

What program, policy and partnership strategies will you implement? What strategies address immediate impacts? Long-term impacts? What strategies address root causes of inequity listed above? How will you partner with stakeholders for long-term positive change?

DRAFT

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Respond here.

DRAFT

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:

"Provide 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

Respond here.

DRAFT

Submitting Department Memo

Description

Provide the high-level description of the technology, including whether software or hardware, who uses it and where/when.

Purpose

State the reasons for the use cases for this technology; how it helps meet the departmental mission; benefits to personnel and the public; under what ordinance or law it is used/mandated or required; risks to mission or public if this technology were not available.

Benefits to the Public

Provide technology benefit information, including those that affect departmental personnel, members of the public and the City in general.

Privacy and Civil Liberties Considerations

Provide an overview of the privacy and civil liberties concerns that have been raised over the use or potential mis-use of the technology; include real and perceived concerns.

Summary

Provide summary of reasons for technology use; benefits; and privacy considerations and how we are incorporating those concerns into our operational plans.

DRAFT

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.

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."

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.

OCR: "Office of Civil Rights."

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.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

DRAFT

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

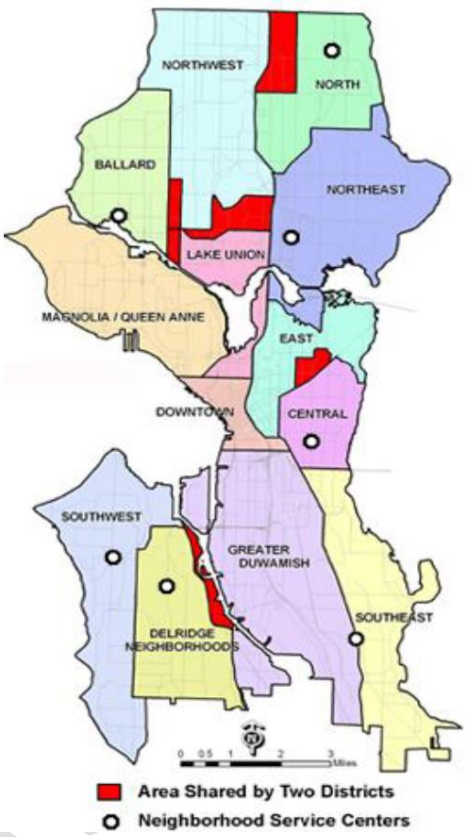
RET: "racial equity toolkit"

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 Analysis

Appendix C: Public Comment Demographics

Appendix D: Comment Analysis Methodology

Appendix E: Questions and Department Responses

Appendix F: Public Outreach Overview

Appendix G: Meeting Notice(s)

Appendix H: Meeting Sign-in Sheet(s)

Appendix I: All Comments Received from Members of the Public

Appendix J: Letters from Organizations or Commissions

Appendix K: Supporting Policy Documentation

DRAFT

Appendix L: CTO Notification of Surveillance Technology

Thank you for your department's efforts to comply with the new Surveillance Ordinance, including a review of your existing technologies to determine which may be subject to the Ordinance. I recognize this was a significant investment of time by your staff; their efforts are helping to build Council and public trust in how the City collects and uses data.

As required by the Ordinance (SMC 14.18.020.D), this is formal notice that the technologies listed below will require review and approval by City Council to remain in use. This list was determined through a process outlined in the Ordinance and was submitted at the end of last year for review to the Mayor's Office and City Council.

The first technology on the list below must be submitted for review by March 31, 2018, with one additional technology submitted for review at the end of each month after that. The City's Privacy Team has been tasked with assisting you and your staff with the completion of this process and has already begun working with your designated department team members to provide direction about the Surveillance Impact Report completion process.

Please let me know if you have any questions.

Thank you,

Michael Mattmiller
Chief Technology Officer

DRAFT

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