2019 Surveillance Impact Report

Acyclica

Seattle Department of Transportation

Table of Contents

City of Seattle

Submitting Department Memo

Seattle
Department of
Transportation

To: Seattle City Council

From: Adiam Emery, Interim Transportation Operations Division Director, SDOT

Subject: Cover Memo – Surveillance Impact Report for the Acyclica system

The Seattle Department of Transportation (SDOT) is transmitting the Surveillance Impact Report (SIR) about the Acyclica system for review and consideration within the Surveillance Ordinance process. The Acyclica system, along with the Traffic Cameras and License Plate Reader technology also under surveillance review, are highly critical transportation technologies for managing movement of people and goods during the Seattle Squeeze – the next five years when significant private and public construction projects will make it more difficult for people and goods to travel to and through Downtown Seattle. At no time with the Acyclica system does SDOT or our vendor have personally identifiably information about drivers or vehicle registration.

Purpose

SDOT began using the Acyclica system in 2014 to measure real-time vehicle travel times on city streets, primarily along Mercer St, in the downtown, and other congested arterial corridors. The small sensors (typically installed on SDOT street furniture) recognize Wi-Fi-enabled devices in vehicles (like smartphones) traveling between multiple sites. The sensors measure travel time from point A to point B without knowing any specific phone owners or their vehicle information–all data are securely encrypted, salted and hashed.

Benefits to the Public

The ability to gather traffic volumes across the city in real-time is a primary component of SDOT’s transportation operations approach. The data is used in three ways:

- Incident detection and management: SDOT staff assigned to the Transportation Operations Center (TOC) monitor network travel times. The TOC consists of a planned and coordinated multi-disciplinary program and technology to detect, respond to, and clear traffic incidents so that traffic flow may be restored as safely and quickly as possible. If an anomaly in travel time is detected by TOC staff, they investigate further. Often, the source is an incident, and the TOC is the first to detect it. The data is used through the course of the incident response and recovery to advise motorists of alternative routes and travel times to reduce overall delays. Acyclica allows the TOC to work to reduce duration and impacts of traffic incidents and improve safety of motorists, crash victims, and emergency responders.

- Performance monitoring and operations improvements: As an example of Acyclica usage, the TOC used Acyclica and other traffic technology during the Viaduct Closure. SDOT uses travel time as the key indicator of our street system's performance allowing mitigation efforts to be focused on the appropriate intersections and corridors. Traffic signal timing improvements are also reliant on this data.

- Public information: The data gathered from the Acyclica sensors is used to provide real-time en route travel times to motorists by posting travel times on electronic message boards located across the city. The real-time travel times are also posted to SDOT's public travelers.gov website which is used by many to plan their daily travel. The information is an important tool to support delay reduction for travelers.

The Acyclica and other travel time measurement technologies, are the traffic information backbone of SDOT's response to the "Seattle Squeeze."

If SDOT was directed to remove these technologies, the data SDOT receives would be incredibly difficult to replicate. No other real-time data sources for arterial travel times are as accurate as those gathered via these technologies. SDOT would not be able to provide real-time travel times to the public, as they would not be sufficiently reliable. TOC incident detection and management operations would suffer without this data, and performance monitoring would not reflect actual operations. In terms of performance monitoring and signal operations improvements, this data enables SDOT to understand operations throughout the day. In the past, that data was collected by agencies by conducting "floating-car studies", which are conducted only during short time periods – not continuously. Using this technique, a team of City personnel would use fleet vehicles to regularly drive those same routes while recording their travel times, and subsequently manually enter that data into a spreadsheet or database. This would be a significant additional need for resources, in addition to a substantial downgrade of data time-of-day coverage, accuracy and timeliness.

Privacy and Civil Liberties Considerations

In 2015 after testing Acyclica, SDOT hired Coalfire System to independently audit Acyclica's security practices. The report stated:

> Coalfire was able to confirm the operation effectiveness of Acyclica's device and systems design such that there is no PII retained in any data repository, nor is the non PII MAC address ever presented to customer/clients in an unencrypted, unhashed format."

Furthermore, SDOT has strong, effective personnel rules for Transportation Operations Center staff and they were reviewed to ensure alignment with the City's Privacy/Surveillance Program.

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.

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."

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.

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.

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.

PDF

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:

PDF

AcyclicaUserGuide

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

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

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

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.

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.

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.

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.

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.

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.

PDF

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.

PDF

Acyclica White
Paper_RoadTrend d

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.

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.

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

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

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.

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.

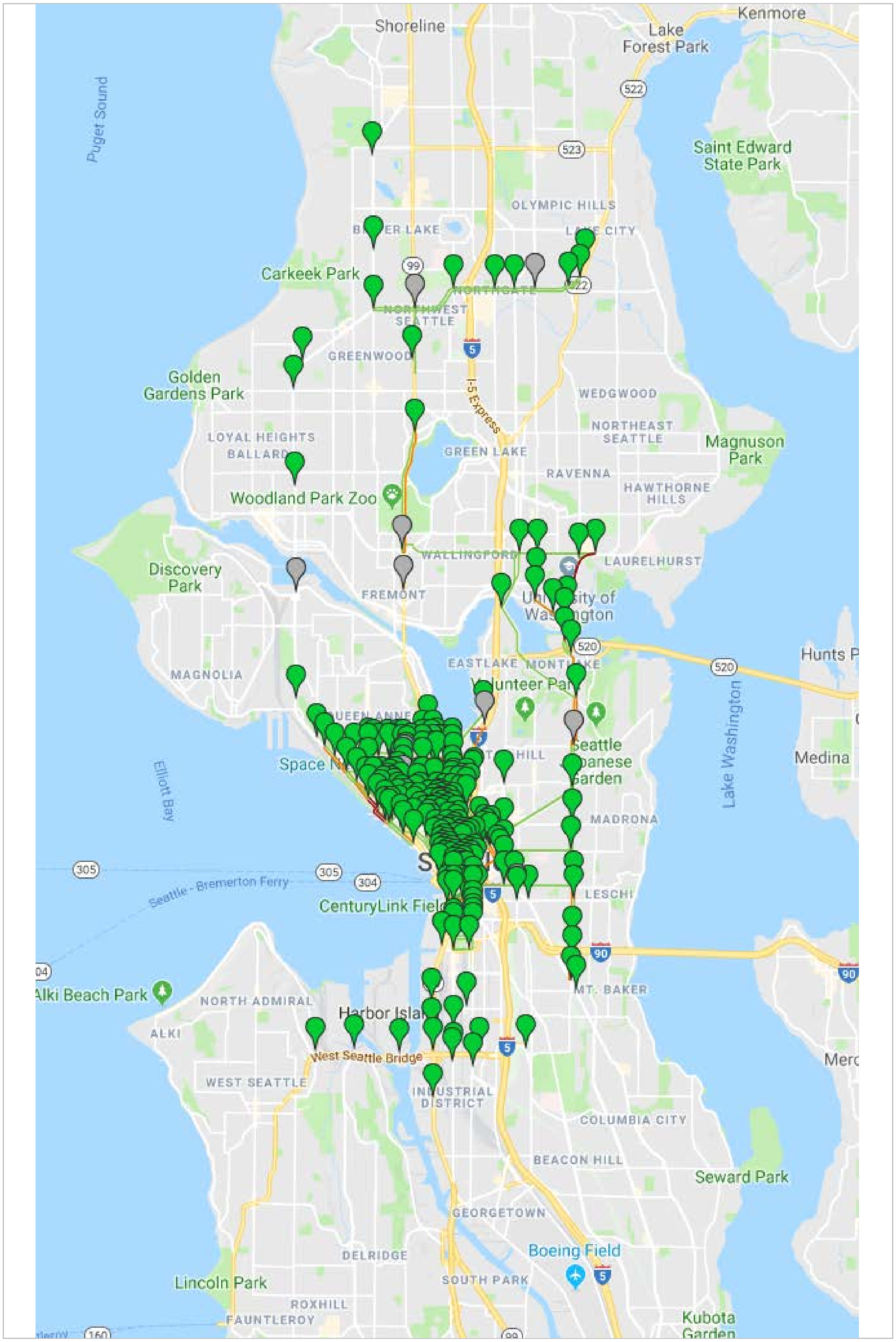
The current deployment of the technology is primarily concentrated in and around the central business district and along several other major arterials. Through 2020 there are a series of technology projects installing Acyclica sensors along additional corridors including those that traverse historically 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

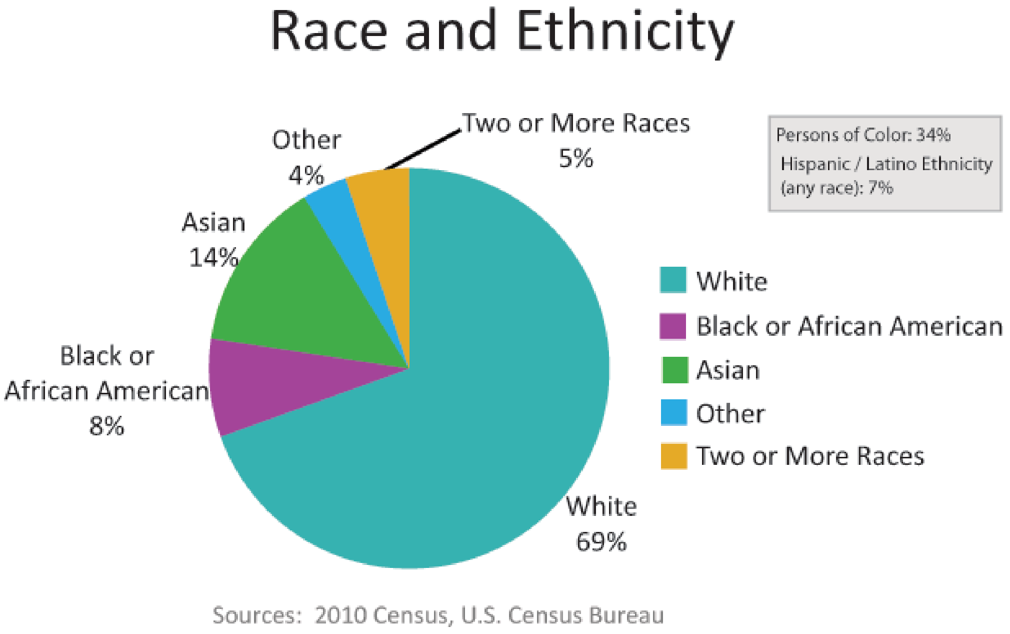
- ☒ Ballard
- ☒ Belltown
- ☐ Beacon Hill
- ☒ Capitol Hill
- ☒ Central District
- ☐ Columbia City
- ☐ Delridge
- ☒ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☒ International District
- ☒ Interbay
- ☒ North
- ☒ Northeast
- ☒ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier 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.


Shoreline
Kenmore
Lake Forest Park
Puget Sound
522
523
Saint Edward State Park
OLYMPIC HILLS
LAKE CITY
BITTER LAKE
Carkeek Park
99
NORTHGATE
NORTHWEST SEATTLE
5
GREENWOOD
Golden Gardens Park
WEDGWOOD
I-5 Express
NORTHEAST SEATTLE
LOYAL HEIGHTS
BALLARD
GREEN LAKE
Magnuson Park
RAVENNA
HAWTHORNE HILLS
Woodland Park Zoo
WALLINGFORD
LAURELHURST
Discovery Park
FREMONT
University of Washington
520
Hunts P
EASTLAKE
MONTLAKE
MAGNOLIA
Volunteer Park
QUEEN ANNE
CAPITOL HILL
Seattle Japanese Garden
Medina
Lake Washington
Space Needle
Elliott Bay
MADRONA
305
304
Seattle - Bremerton Ferry
CenturyLink Field
LESCHI
90
Alki Beach Park
NORTH ADMIRAL
MT. BAKER
Harbor Island
ALKI
West Seattle Bridge
Merc
WEST SEATTLE
INDUSTRIAL DISTRICT
COLUMBIA CITY
BEACON HILL
Seward Park
GEORGETOWN
DELRIDGE
Boeing Field
SOUTH PARK
Lincoln Park
ROXHILL
FAUNTLEROY
Kubota Garden
160

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:

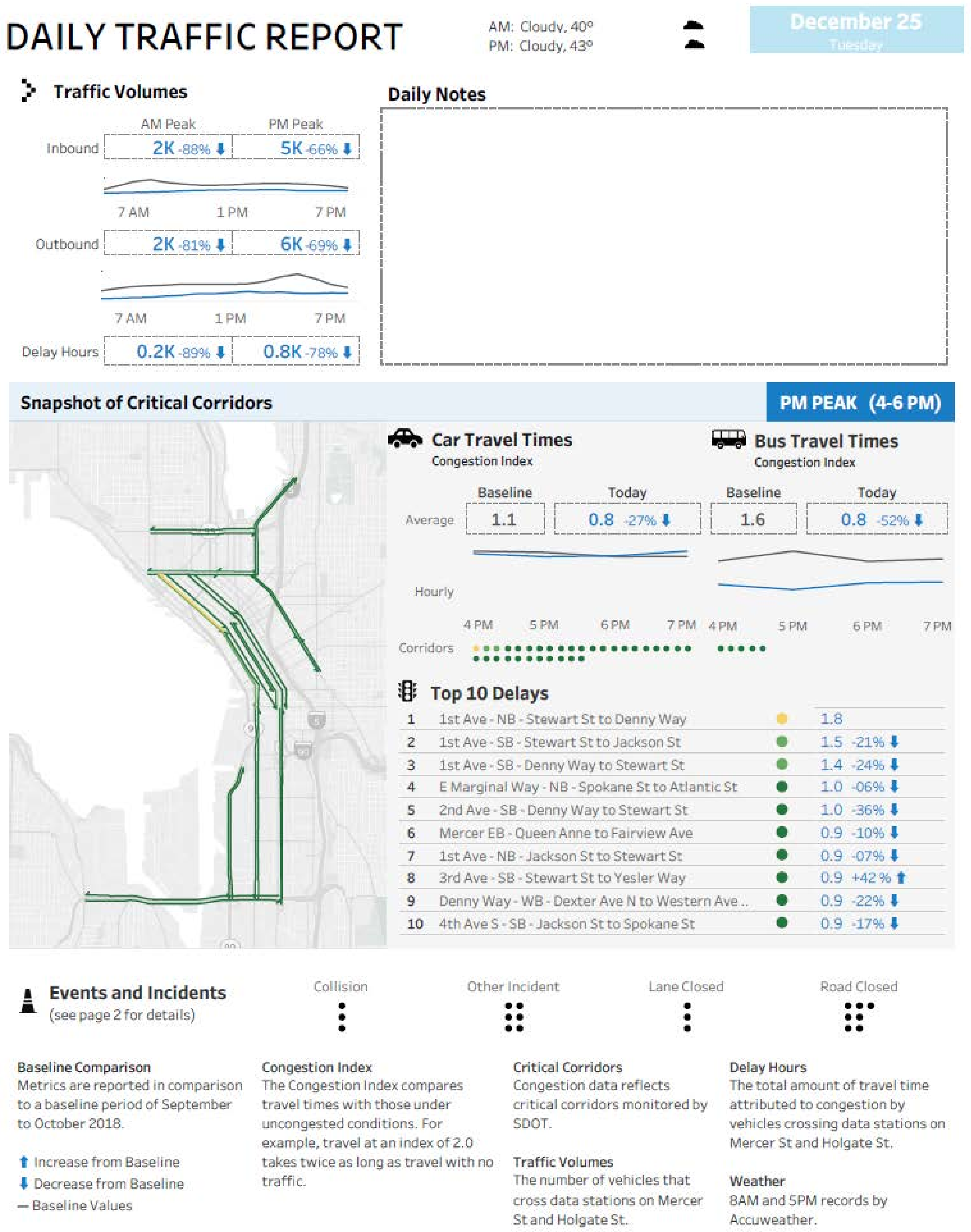


1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

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.

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:



DAILY TRAFFIC REPORT

AM: Cloudy, 40°
PM: Cloudy, 43°

December 25
Tuesday

Traffic Volumes

	AM Peak	PM Peak
Inbound	2K -88% ⬇	5K -66% ⬇
Outbound	2K -81% ⬇	6K -69% ⬇
Delay Hours	0.2K -89% ⬇	0.8K -78% ⬇

Daily Notes

Snapshot of Critical Corridors

PM PEAK (4-6 PM)

Car Travel Times
Congestion Index

Bus Travel Times
Congestion Index

	Car Baseline	Car Today	Bus Baseline	Bus Today
Average	1.1	0.8 -27% ⬇	1.6	0.8 -52% ⬇

Top 10 Delays

1	1st Ave - NB - Stewart St to Denny Way	●	1.8
2	1st Ave - SB - Stewart St to Jackson St	●	1.5 -21% ⬇
3	1st Ave - SB - Denny Way to Stewart St	●	1.4 -24% ⬇
4	E Marginal Way - NB - Spokane St to Atlantic St	●	1.0 -06% ⬇
5	2nd Ave - SB - Denny Way to Stewart St	●	1.0 -36% ⬇
6	Mercer EB - Queen Anne to Fairview Ave	●	0.9 -10% ⬇
7	1st Ave - NB - Jackson St to Stewart St	●	0.9 -07% ⬇
8	3rd Ave - SB - Stewart St to Yesler Way	●	0.9 +42 % ⬆
9	Denny Way - WB - Dexter Ave N to Western Ave ..	●	0.9 -22% ⬇
10	4th Ave S - SB - Jackson St to Spokane St	●	0.9 -17% ⬇

Events and Incidents
(see page 2 for details)

Baseline Comparison
Metrics are reported in comparison to a baseline period of September to October 2018.

⬆ Increase from Baseline
⬇ Decrease from Baseline
— Baseline Values

Congestion Index
The Congestion Index compares travel times with those under uncongested conditions. For example, travel at an index of 2.0 takes twice as long as travel with no traffic.

Critical Corridors
Congestion data reflects critical corridors monitored by SDOT.

Traffic Volumes
The number of vehicles that cross data stations on Mercer St and Holgate St.

Delay Hours
The total amount of travel time attributed to congestion by vehicles crossing data stations on Mercer St and Holgate St.

Weather
8AM and 5PM records by Accuweather.

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.

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		

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.
ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy. And used at a number of Department of Neighborhoods-led focus groups.

2.3 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	Bertha Knight Landes Room, 1st Floor City Hall 600 4th Avenue, Seattle, WA 98104
Time	February 27, 2018; 6 p.m. – 8 p.m.
Capacity	100+
Link to URL Invite	BKL Event Invitation

2.4 Scheduled Focus Group Meeting(s)

The following Focus Groups were organized by the Department of Neighborhoods and may or may not have discussed this specific technology. The content of the focus group discussion was determined by the community engaged and/or the focus group attendees. A summary of the discussion notes may be found in Appendix D.

Meeting 1

Community Engaged	Council on American-Islamic Relations - Washington (CAIR-WA)
Date	Thursday, February 21, 2019

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

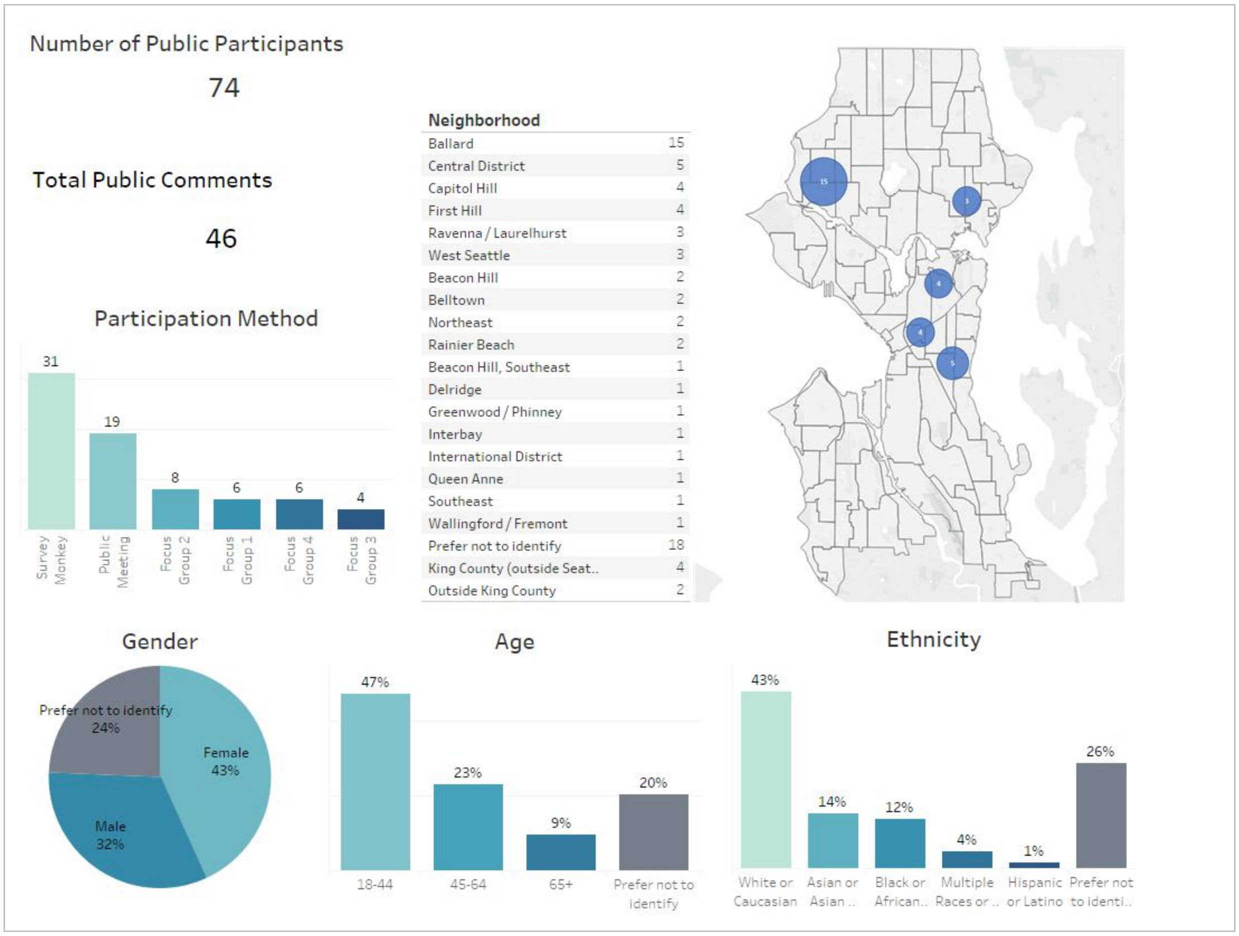
Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

Meeting 4

Community Engaged	Friends of Little Saigon
Date	Wednesday, February 27, 2019

3.0 Public Comment Analysis

3.1 Summary of Response Volume and Demographic Information



Number of Public Participants

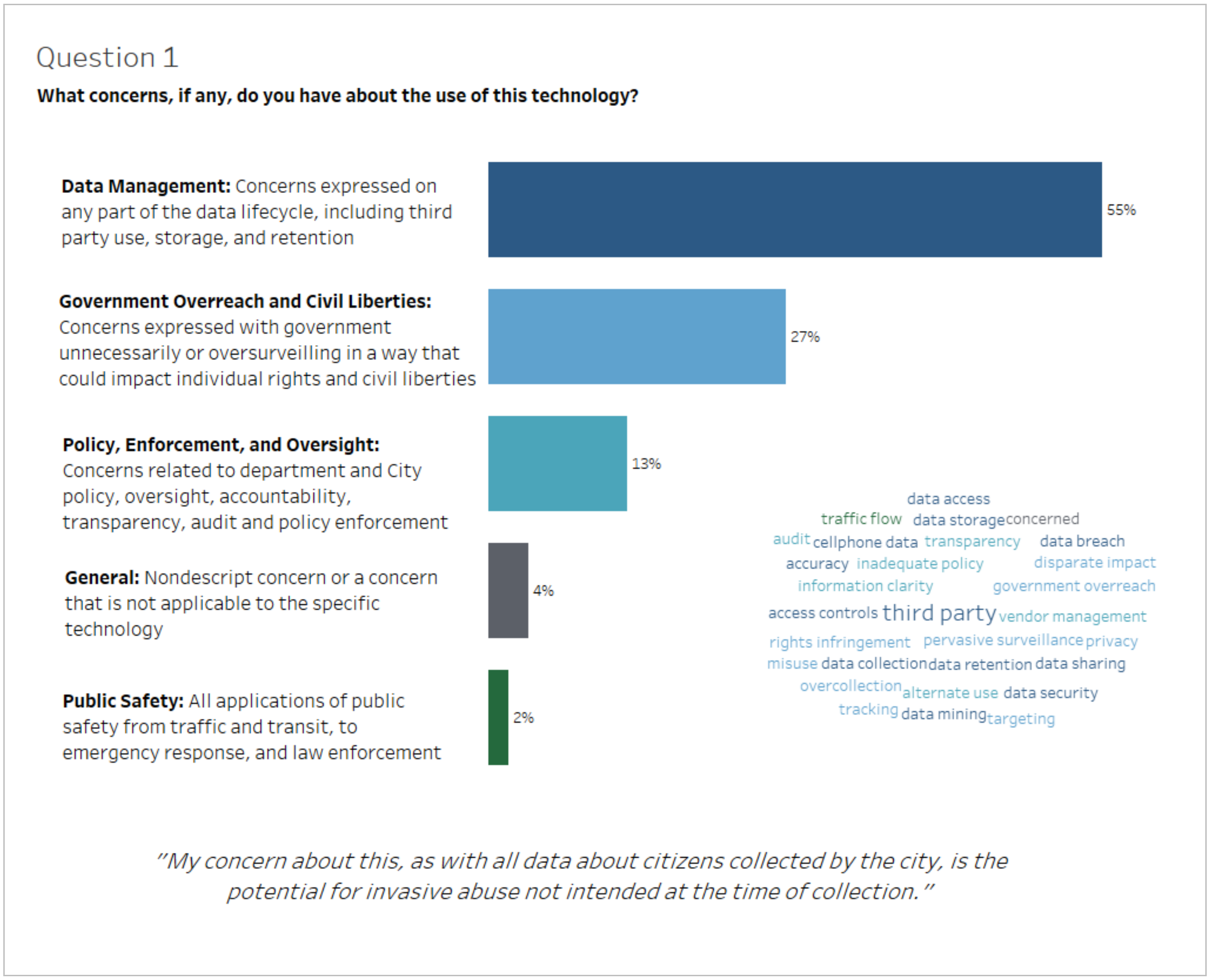
74

Total Public Comments

46

Neighborhood	
Ballard	15
Central District	5
Capitol Hill	4
First Hill	4
Ravenna / Laurelhurst	3
West Seattle	3
Beacon Hill	2
Belltown	2
Northeast	2
Rainier Beach	2
Beacon Hill, Southeast	1
Delridge	1
Greenwood / Phinney	1
Interbay	1
International District	1
Queen Anne	1
Southeast	1
Wallingford / Fremont	1
Prefer not to identify	18
King County (outside Seat..	4
Outside King County	2

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



Question 1

What concerns, if any, do you have about the use of this technology?

Data Management: Concerns expressed on any part of the data lifecycle, including third party use, storage, and retention

Government Overreach and Civil Liberties: Concerns expressed with government unnecessarily or oversurveilling in a way that could impact individual rights and civil liberties

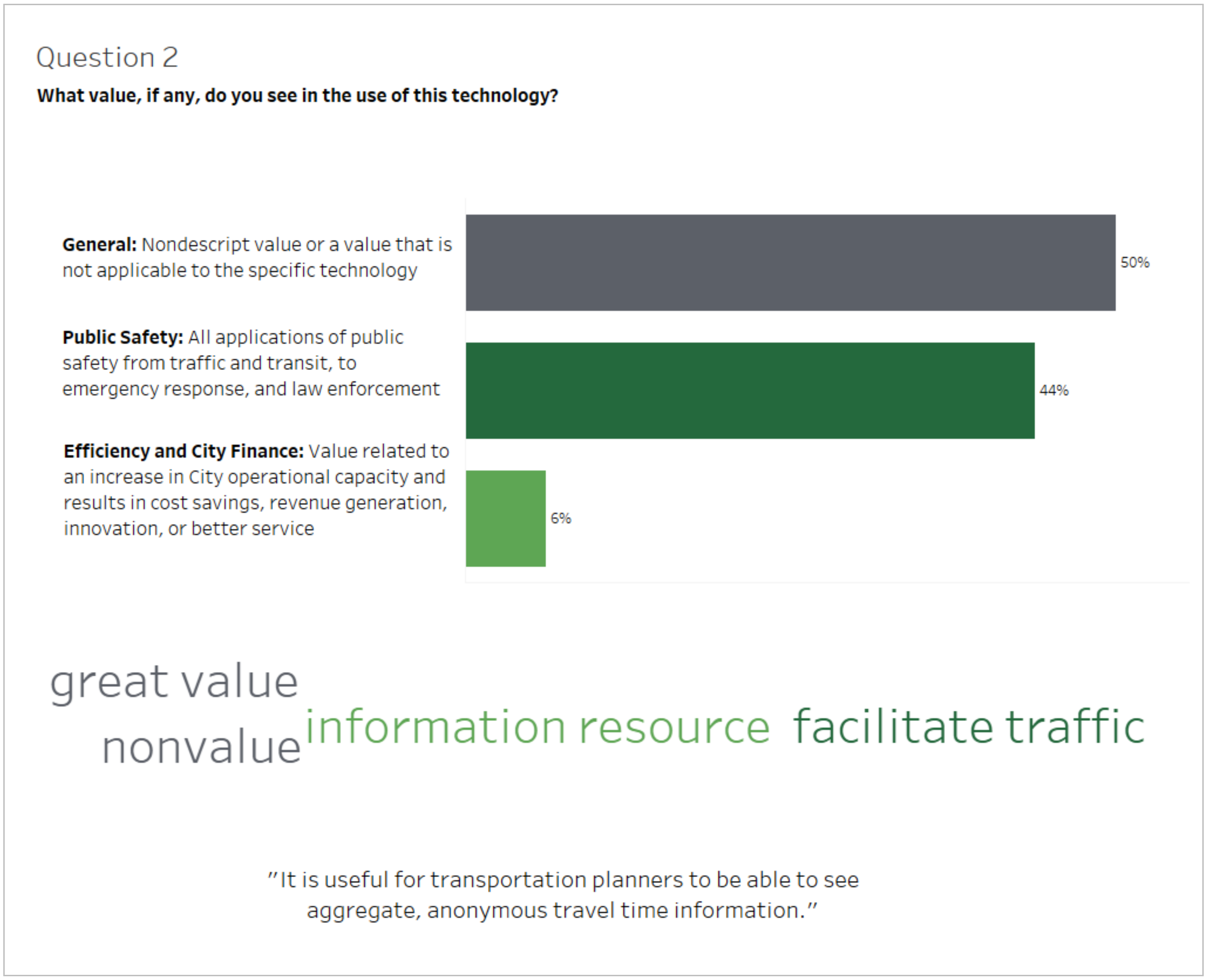
Policy, Enforcement, and Oversight: Concerns related to department and City policy, oversight, accountability, transparency, audit and policy enforcement

General: Nondescript concern or a concern that is not applicable to the specific technology

Public Safety: All applications of public safety from traffic and transit, to emergency response, and law enforcement

"My concern about this, as with all data about citizens collected by the city, is the potential for invasive abuse not intended at the time of collection."

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



Question 2

What value, if any, do you see in the use of this technology?

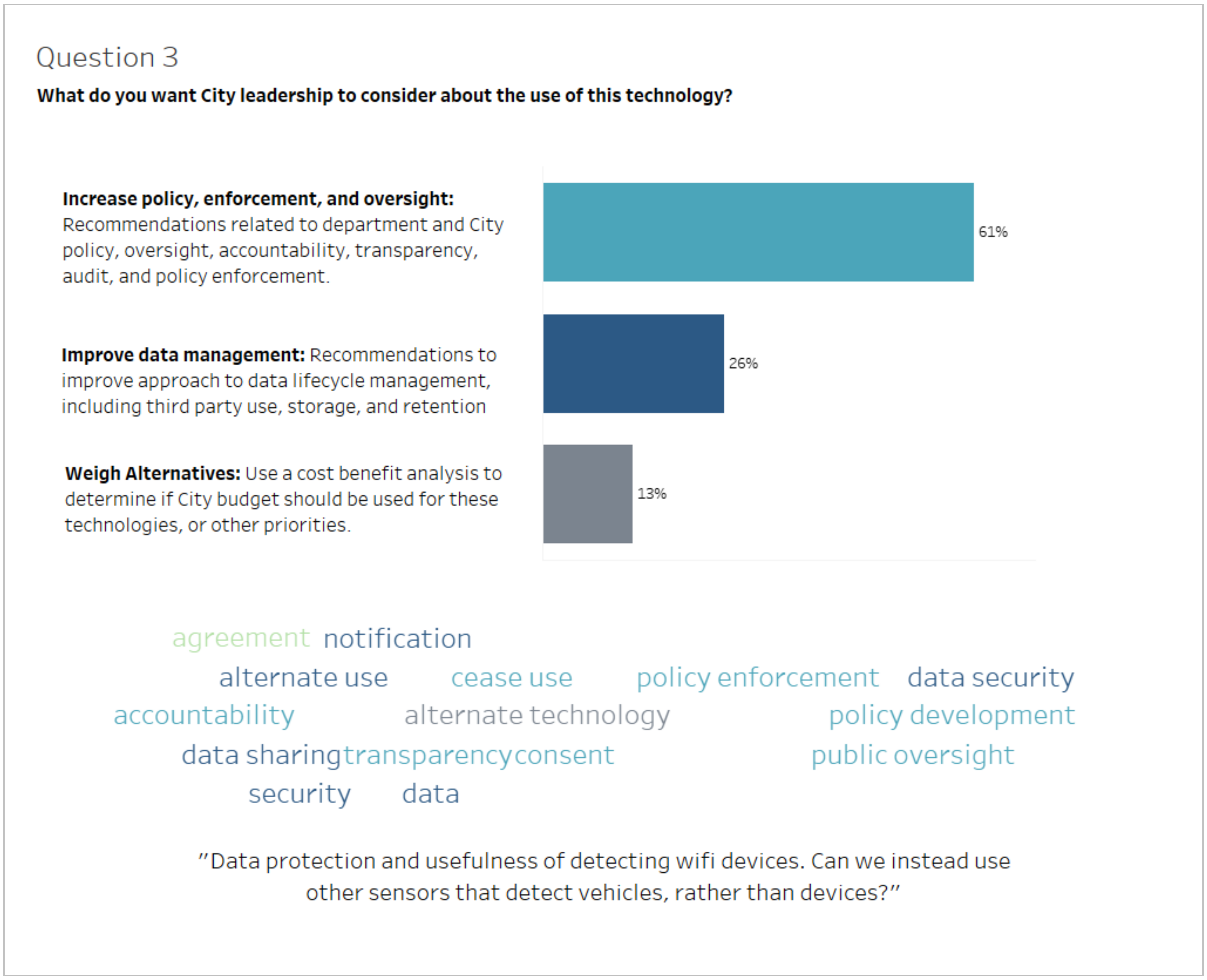
General: Nondescript value or a value that is not applicable to the specific technology

Public Safety: All applications of public safety from traffic and transit, to emergency response, and law enforcement

Efficiency and City Finance: Value related to an increase in City operational capacity and results in cost savings, revenue generation, innovation, or better service

"It is useful for transportation planners to be able to see aggregate, anonymous travel time information."

3.4 Question Three: What do you want City leadership to consider about the use of this technology?



Question 3

What do you want City leadership to consider about the use of this technology?

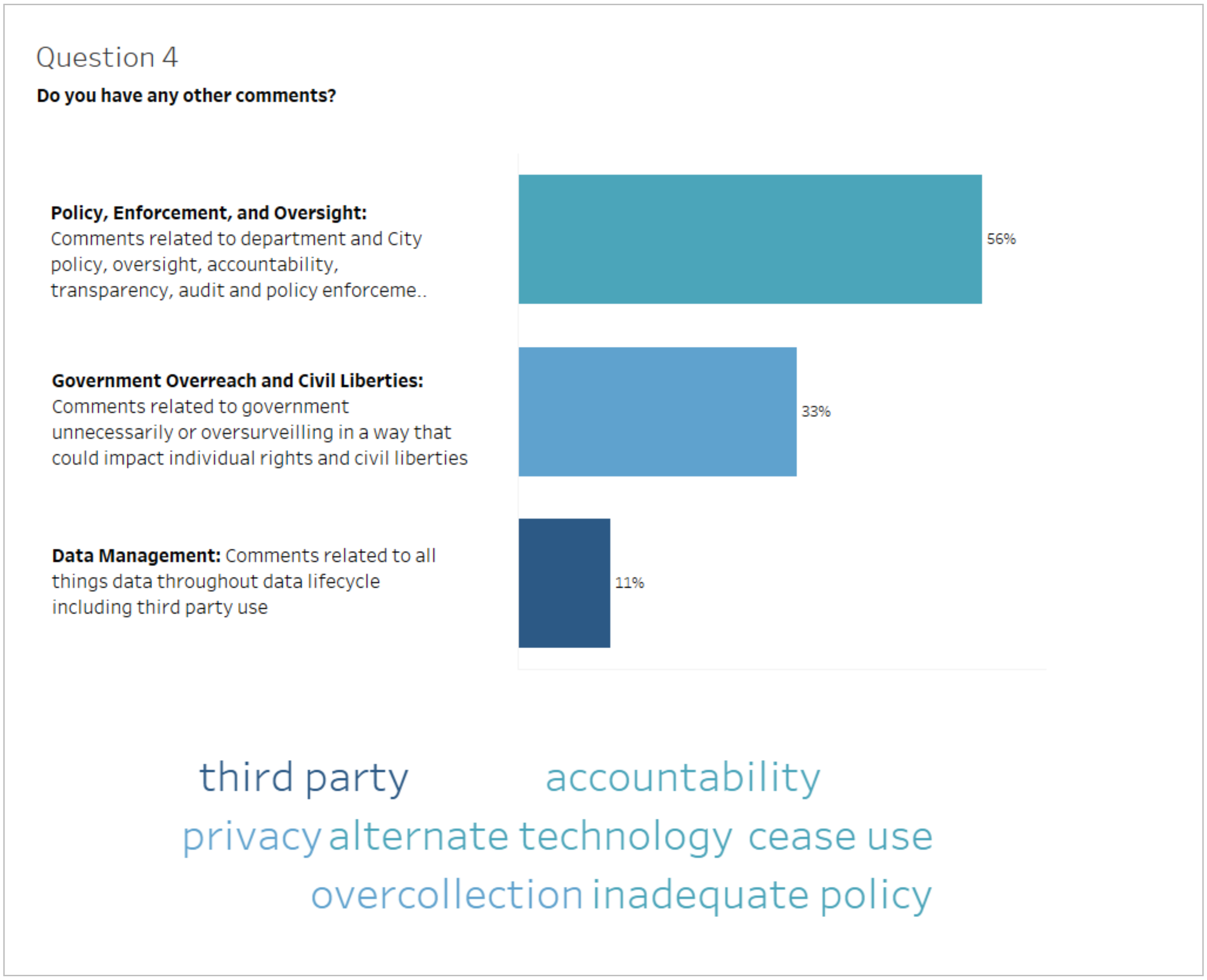
Increase policy, enforcement, and oversight: Recommendations related to department and City policy, oversight, accountability, transparency, audit, and policy enforcement.

Improve data management: Recommendations to improve approach to data lifecycle management, including third party use, storage, and retention

Weigh Alternatives: Use a cost benefit analysis to determine if City budget should be used for these technologies, or other priorities.

"Data protection and usefulness of detecting wifi devices. Can we instead use other sensors that detect vehicles, rather than devices?"

3.5 Question Four: Do you have any other comments?



Question 4

Do you have any other comments?

Policy, Enforcement, and Oversight: Comments related to department and City policy, oversight, accountability, transparency, audit and policy enforceme..

Government Overreach and Civil Liberties: Comments related to government unnecessarily or oversurveilling in a way that could impact individual rights and civil liberties

Data Management: Comments related to all things data throughout data lifecycle including third party use

4.0 Equity Annual Reporting

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

The Seattle Department of Transportation is currently working to finalize the metrics.

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

The Working Group's Privacy and Civil Liberties Impact Assessment for this technology is below, and is also included in the Ordinance submission package, available as an attachment.

From: Seattle Community Surveillance Working Group
(CSWG) To: Seattle City Council

Date: June 4, 2019

Re: Privacy and Civil Liberties Impact Assessment for Acyclica (SDOT)

Executive Summary

On April 25, 2019, the CSWG received the Surveillance Impact Report (SIR) on Acyclica, a surveillance technology included in Group 2 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for this technology as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIR submitted to the City Council.

This document first provides our recommendations to the Council, then provides background information, key concerns, and outstanding questions on Acyclica technology.

Our assessment of Acyclica focuses on three major issues rendering protections around this technology inadequate:

1. SDOT has no explicit policies governing its use of Acyclica technology.
2. There is no contract between SDOT and Acyclica, which contributes to the following concerns:
   a. There is no policy or other agreement that ensures SDOT owns the non-aggregated data collected by Acyclica devices;
   b. Acyclica's stated data security practices are misleading and unclear;
   c. There are no limits on Acyclica's retention of non-aggregated data; and
   d. There is no limit on or designation of which third parties will access Acyclica's data, for what purpose, and under what conditions.
3. There is no evaluation of the technical abilities of the EDI DA-300 (the new sensor that we have learned will replace the RoadTrend sensor evaluated in the SIR), and it is not stated whether the EDI DA-300 will be used in conjunction with or replace all RoadTrend sensors.

Recommendations

The Council should adopt, via ordinance, clear and enforceable rules that ensure, at the minimum, the following:

1. The purpose of Acyclica technology must be clearly defined, and operation of the technology and data collected by it must be explicitly restricted to those purposes only. For example: Acyclica may only be used for traffic management purposes, explicitly defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.
2. There must be a written, binding contract directly between SDOT and Acyclica (as well as Western Systems, if applicable) that includes the following minimum provisions:
   a. SDOT owns all data, not Acyclica (or FLIR, the company that acquired Acyclica).
   b. SDOT receives only aggregated data.
   c. The data retention period for any data Acyclica collects shall be 12 hours or less, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both the non-aggregated and aggregated data.
   d. Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.
3. SDOT must produce an annual report detailing its use of Acyclica, including details of what data is collected, how much data is collected, how SDOT used the data collected, for how long it was retained, and in what form.

Background: Privacy and Civil Liberties Concerns with Acyclica Technology

Acyclica technology is a transportation management tool used by SDOT that raises privacy and civil liberties concerns because of its ability to uniquely track, identify, and create a detailed map of individuals' movements. Acyclica manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that collect encrypted media access control (MAC) addresses—unique identifiers attached to devices—from any WiFi-enabled device (e.g., cell phones, computers, and vehicles) within range of the sensors in Seattle.

Because these sensors are placed on at least 301 intersections in Seattle and collect and record MAC addresses 24 hours a day, 7 days a week, and 365 days a year, Acyclica can generate extremely precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of drivers and riders in vehicles, but they can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close buildings (e.g. apartments and offices). This powerful location-tracking technology raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These privacy concerns are exacerbated by the absence of specific policies governing use of Acyclica technology and the absence of a contract between SDOT and Acyclica. Without contractual restrictions on data use, ownership, and sharing, Acyclica data can be shared with third parties (e.g., companies and law enforcement), may be combined with additional data such as facial recognition data, and repurposed for non-traffic management purposes.

Of additional concern is that the RoadTrend sensors evaluated in the current SIR were discontinued in March 2019 after Acyclica was acquired by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense. While SDOT states that it is in the process of procuring a new sensor, the EDI DA-300, the SIR does not include an evaluation of this new sensor's capabilities.

Finally, while SDOT cites cost savings and Acyclica's ability to accurately measure traffic times as the two key reasons it decided to procure Acyclica technology, the results of the study attached to the SIR[1] are inconclusive on Acyclica's accuracy. The study states: "In terms of accuracy, Acyclica did not perform as well as desired."[2] Given this assessment, it is unclear how privacy and civil liberties concerns were considered when SDOT made the decision to acquire Acyclica—while Acyclica may generate cost savings relative to some other (but potentially not all) comparable technologies, it also creates new privacy challenges without presenting clear gains on accuracy.

[1] *Acyclica Travel Time Accuracy & Reliability Analysis*

[2] The study states, "Acyclica did not pass the t-test because the results showed that the means were not the same." This means that Acyclica was unable to produce similar values to License Plate Reader Cameras, which were assumed to represent the ground truth. Though it is possible that the LPR data itself could have been inaccurate, the study's results are inconclusive on Acyclica's accuracy in measuring traffic times.

Key Concerns

(1) **There are no specific policies defining purpose of use.** In the updated SIR, SDOT states, "We have no specific policies guiding our use of Acyclica, but SDOT's intent is to use this data service to deliver travel time, delay, analytics and other traffic data."[3] This stated intent and other uses cited in the SIR are vague and impose no meaningful restrictions on the purposes for which Acyclica devices may be used. For example:

- Section 1.1 of the abstract states that Acyclica is used by over 50 agencies "to help to monitor and improve traffic congestion."
- Section 2.1 provides some examples of types of information Acyclica uses (e.g., calculated average speeds) to produce certain outcomes (e.g., correcting traffic signal timing), but it is unclear if the examples cited constitute a complete list.

The above statements do not describe the purpose of use, all the types of information Acyclica collects, and all the types of work that Acyclica technology facilitates.

(2) **There is no contract between SDOT and Acyclica.** In the updated SIR, SDOT states, "SDOT does not have a contract with Acyclica."[4] Without a contract or statutory protections, data ownership and restrictions on the scope of data sharing and repurposing cannot be enforced. For example, without contractual restrictions or statutory protections, Acyclica would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate readers or facial recognition data. Because SDOT does not have a contract with Acyclica, even if SDOT did have specific policies defining and restricting purpose of use, SDOT cannot enforce those policies restricting the use of Acyclica technology to the intended purpose.

(3) **There is a lack of clarity on data ownership.** In the updated SIR, SDOT states, "SDOT owns the raw and aggregated data. See the attached letter *SDOT Acyclica Data Ownership* which clarifies that."[5] However the attached letter[6] does not actually provide any documentation showing that SDOT owns the raw (i.e., non-aggregated) data. This letter simply states that FLIR will not grant unauthorized users access to Acyclica software.[7]

[3] 2019 Surveillance Impact Report Acyclica SDOT, Appendix F, page 120.

[4] Ibid.

[5] Ibid.

[6] See Appendix A – Letter on SDOT Acyclica Data Ownership

[7] Moreover, in a 2018 conversation between the American Civil Liberties of Washington (ACLU-WA) and Daniel Benhammou (President of Acyclica), Benhammou stated that Acyclica owns all of the non-aggregated data. These contradictory statements make it unclear who actually owns the non-aggregated data.

(4) **There are no limits on Acyclica data retention.** In the updated SIR, SDOT states, "Acyclica/FLIR does not have a limit on data retention. The reason for this policy is that as they develop new methods of analyzing traffic, the analyses are effective as of the date the sensors were first deployed rather than when the feature was first available in the software."[8] If SDOT owns all of the data, including the non- aggregated data, it is unclear why Acyclica/FLIR would be setting their own limits on data retention. The upshot appears to be no enforceable limits on data retention.

(5) **There is a lack of clarity on the capabilities and usage of the new Acyclica/FLIR sensor (EDI DA- 300).**[9] Acyclica has recently been acquired by FLIR Systems, and the RoadTrend sensors evaluated in the SIR have been discontinued. SDOT states: "Since the RoadTrend product line was discontinued, we've begun procuring the EDI DA-300 (please see attached data sheet) in its place. The EDI DA-300 will be the model we consistently deploy in the foreseeable future, and there are no plans to consider an alternative at this point. This unit has additional features differentiating it from the RoadTrend such as generating alarms when a traffic cabinet door is opened, and the ability to provide remote access to traffic signals using cellular communication." It is unclear whether the EDI DA-300 will be used in conjunction with or to replace all RoadTrend Sensors. Because a full description of the capabilities of the EDI DA-300 has not been included in the SIR, neither the public nor the CSWG was been able to conduct a full evaluation of the technology. The involvement of Western Systems[10], a third-party vendor which is the only entity with whom SDOT currently appears to have a written agreement, further complicates matters—it is unclear if terms in the MoU with Western Systems are still applicable. The relationship between SDOT, Western Systems, and Acyclica/FLIR must be explicitly clarified, and explicit contractual terms ensuring purpose, operation, data use, data dissemination, and data deletion should be put in place if they do not already exist.

[8] 2019 Surveillance Impact Report Acyclica SDOT, Appendix F, page 121.

[9] The initial SIR failed to mention that Acyclica had been acquired by FLIR and that the RoadTrend sensor had been discontinued. Only in response to the ACLU-WA's pointed questions did SDOT include in the updated SIR that it was aware of the FLIR acquisition and has been making clear plans to procure a new sensor.

[10] Western Systems is the vendor that owns, operates, and is responsible for the maintenance and replacement of the hardware used to gather the data.

(6) **There are inaccurate and contradictory descriptions of data security practices.**[11] The SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor.[12] However, according to a letter from Daniel Benhammou (President of Acyclica) provided by SDOT representatives at the first public comment meeting on the Group 2 technologies,[13] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. The response from SDOT in the updated SIR does not clarify whether the data is or is not hashed on the sensor. It simply states: "Prior to being transmitted from the sensor in the field to the cloud, the data is encrypted end-to-end using TLS and a 2048-bit encryption certificate." These contradictory descriptions make it difficult to understand Acyclica's data security practices.

(7) **It is unclear which third parties have access to the non-aggregated data, for what purpose, and under what conditions.** In the updated SIR, SDOT states: "Acyclica has given the ability for cities to manage their own users and additionally taken steps to eliminate data sharing unless the owning city has given explicit authorization. Existing users of SDOT's aggregated travel time data include: (1) SDOT staff conducting engineering studies, (2) WSDOT and KC Metro staff conducting engineering studies in partnership with SDOT, (3) Consulting partners who build traffic products on SDOT's behalf."[14] It is unclear if these users listed are *all* the users that have access to SDOT's aggregated travel time data. Of greater importance, it remains unclear who has access to the non-aggregated data, if any, for what purposes, and under what conditions.

Outstanding Questions

The following information should be included in an update to the Acyclica SIR:

(1) Who owns the non-aggregated data collected by Acyclica devices, and what policies or other documentation state this?
(2) What are Acyclica's data security practices, and what policies or other documentation state this?
(3) Which third parties that will access Acyclica's data (both aggregated and non-aggregated), for what purpose, and under what conditions?
(4) What is the relationship between SDOT, Acyclica/FLIR, and Western Systems? Are the Western Systems terms still applicable given the FLIR acquisition?
(5) What are the capabilities of the new EDI DA-300 sensors?

The answers to these questions can further inform the content of any binding policy the Council chooses to include in an ordinance on this technology, as recommended above.

[11] Section 7.2 of the SIR states: "Contractually, Acyclica guarantees that the data is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key or access to the data can identify individuals.

[12] 2019 Surveillance Impact Report Acyclica SDOT, Section 4.2, page 11.

[13] See Appendix B – Benhammou Letter

[14] 2019 Surveillance Impact Report Acyclica SDOT, Appendix F, page 121.

Appendix A – Letter on SDOT Acyclica Data Ownership

FLIR | The World's Sixth Sense™

March 14, 2019

Jason Cambridge

Seattle Department of
Transportation 700 5th Avenue
Seattle, WA

Dear Mr. Cambridge,

Thank you for taking the time to meet with me on the 14th of March to discuss data privacy and ownership. When we started working with Seattle DOT in2014, we committed that the only parties who would have access to the data generated by Seattle DOT would employees and those individuals which authorized users had granted access to the Acyclica software. FLIR's contractual obligations for data and support have been governed by the terms of use and the contract which our intermediary, Western Systems, executed with Seattle DOT. Some of these users, as designated by Seattle DOT have also been granted APIs for programmatically accessing aggregated data.

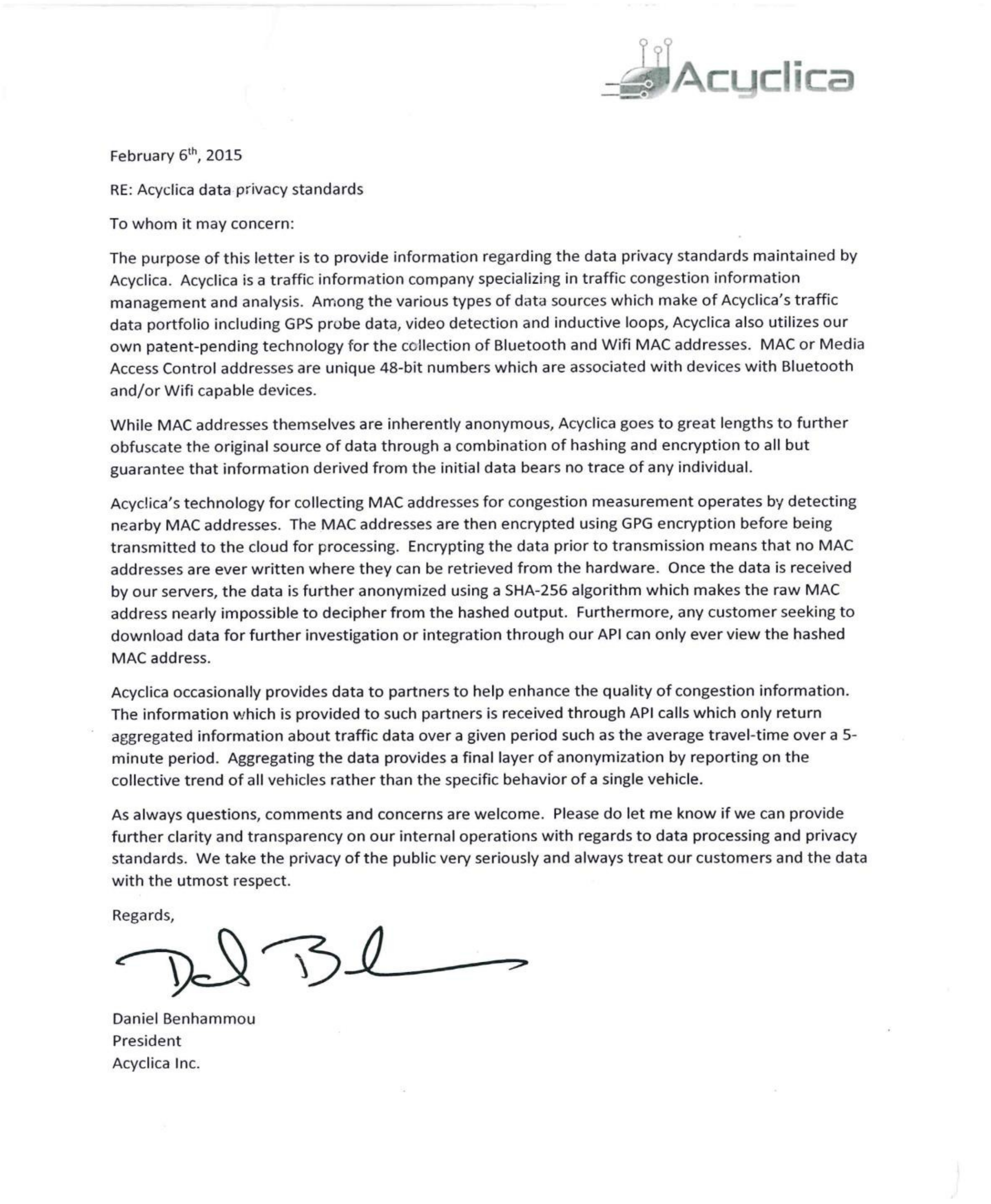
Moving forward, we renew our commitment to data privacy and security. FLIR will not grant access to Seattle DOT data to anyone without the express, written consent to do so. As the needs of Seattle DOT evolve, we are open to implementing additional measures to protect privacy of individuals while providing the best insights through the Acyclica platform.

Best Regards,

Daniel Benhammou

Senior Director, Software and
Solutions FLIR Systems, Inc.

Appendix B - Benhammou Letter



Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

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.

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

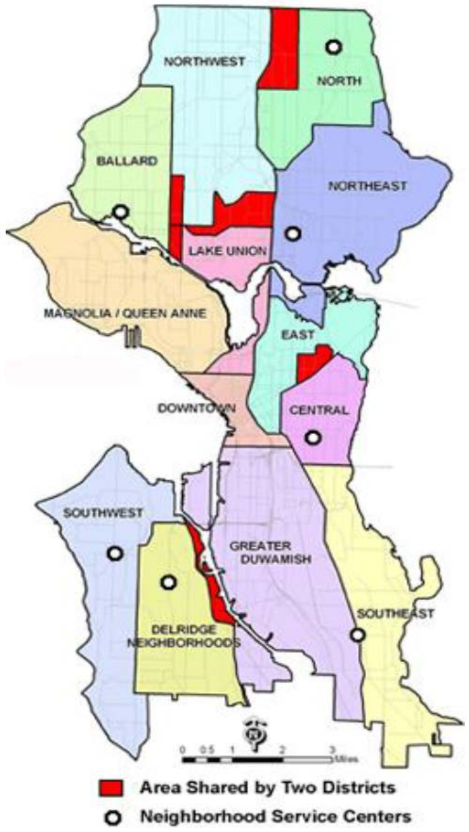
RET: "racial equity toolkit"

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.

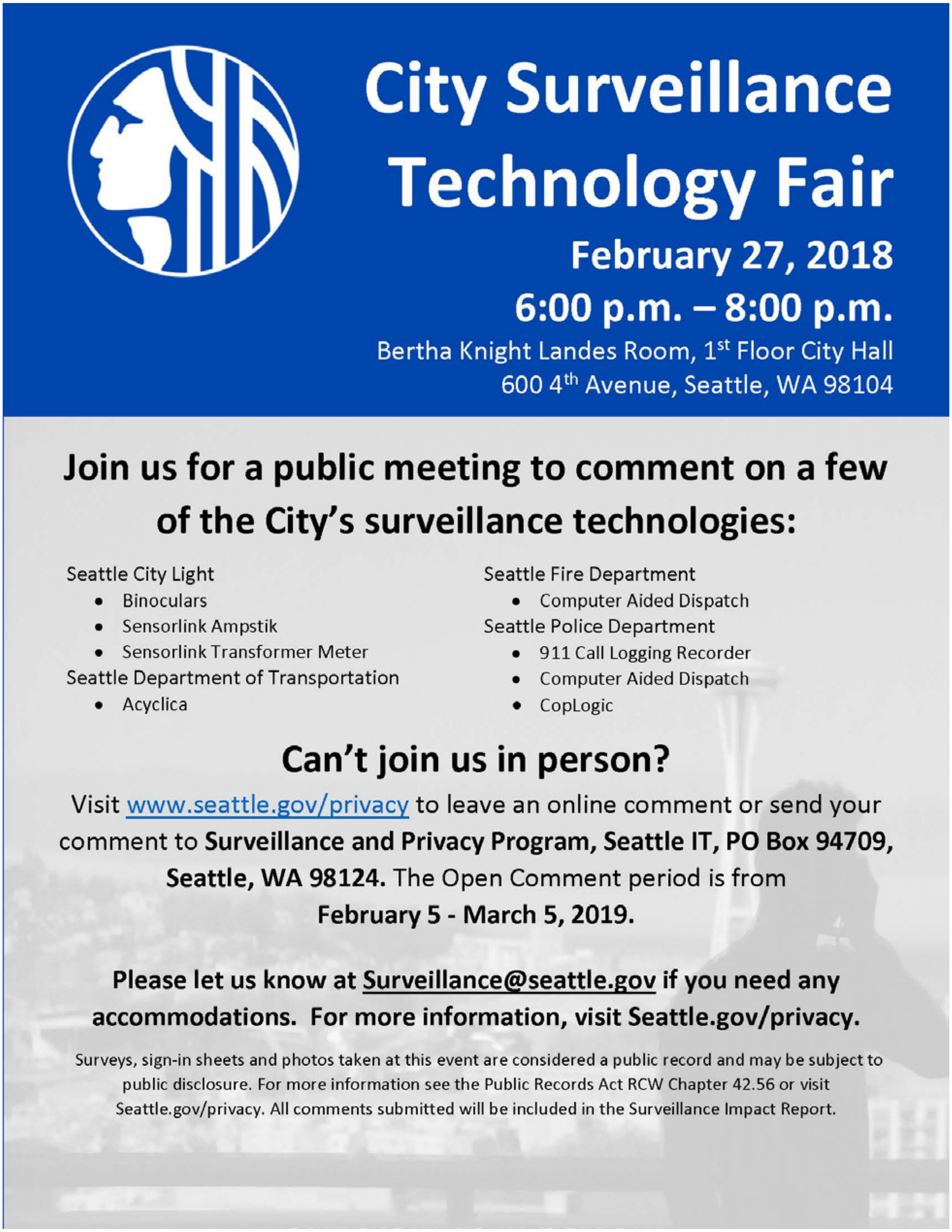
Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



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.

Appendix B: Meeting Notice(s)



City Surveillance Technology Fair

February 27, 2018

6:00 p.m. – 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Join us for a public meeting to comment on a few of the City's surveillance technologies:

Seattle City Light

- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation

- Acyclica

Seattle Fire Department

- Computer Aided Dispatch

Seattle Police Department

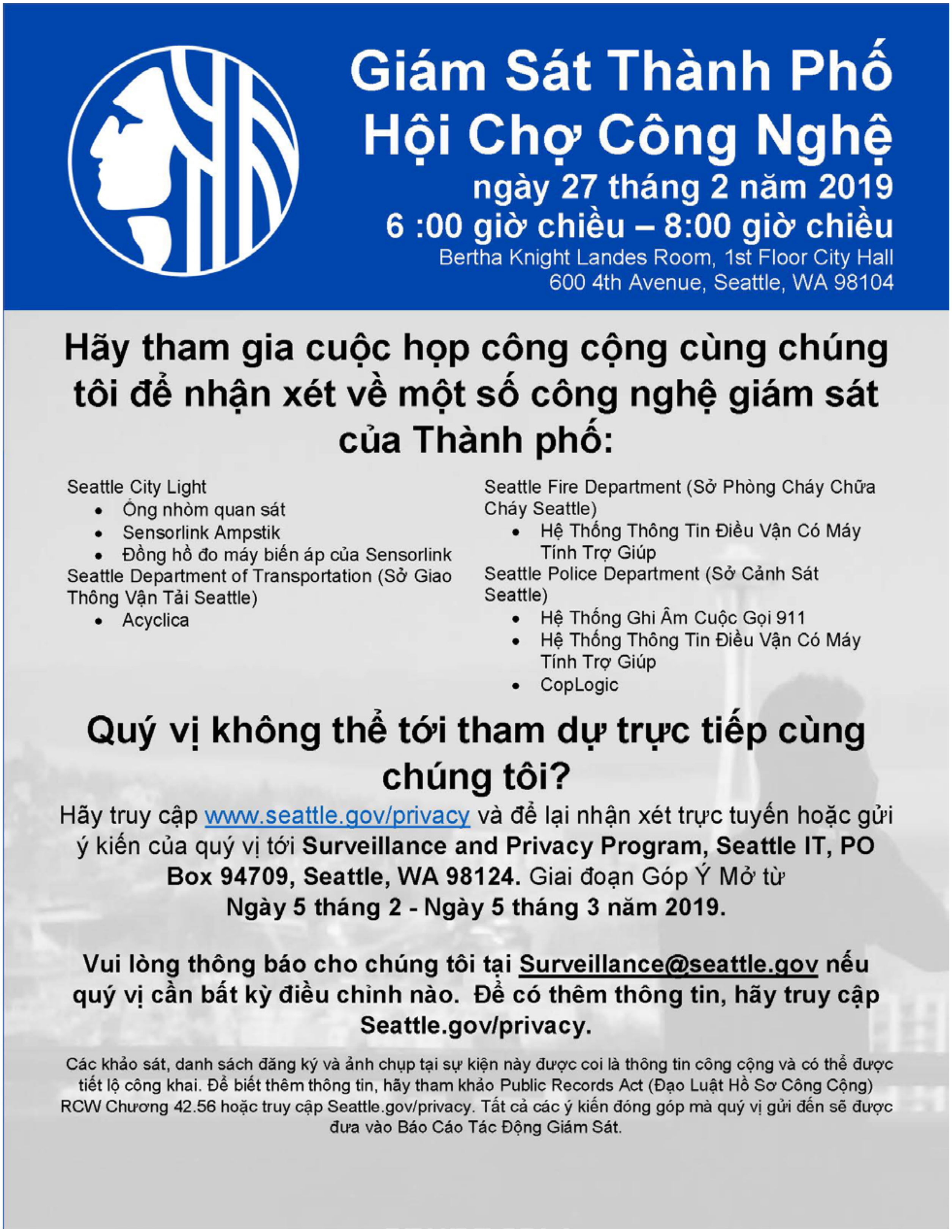
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

Can't join us in person?

Visit www.seattle.gov/privacy to leave an online comment or send your comment to **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** The Open Comment period is from **February 5 - March 5, 2019.**

Please let us know at Surveillance@seattle.gov if you need any accommodations. For more information, visit Seattle.gov/privacy.

Surveys, sign-in sheets and photos taken at this event are considered a public record and may be subject to public disclosure. For more information see the Public Records Act RCW Chapter 42.56 or visit Seattle.gov/privacy. All comments submitted will be included in the Surveillance Impact Report.



Giám Sát Thành Phố Hội Chợ Công Nghệ

ngày 27 tháng 2 năm 2019

6 :00 giờ chiều – 8:00 giờ chiều

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Hãy tham gia cuộc họp công cộng cùng chúng tôi để nhận xét về một số công nghệ giám sát của Thành phố:

Seattle City Light

- Ống nhòm quan sát
- Sensorlink Ampstik
- Đồng hồ đo máy biến áp của Sensorlink

Seattle Department of Transportation (Sở Giao Thông Vận Tải Seattle)

- Acyclica

Seattle Fire Department (Sở Phòng Cháy Chữa Cháy Seattle)

- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp

Seattle Police Department (Sở Cảnh Sát Seattle)

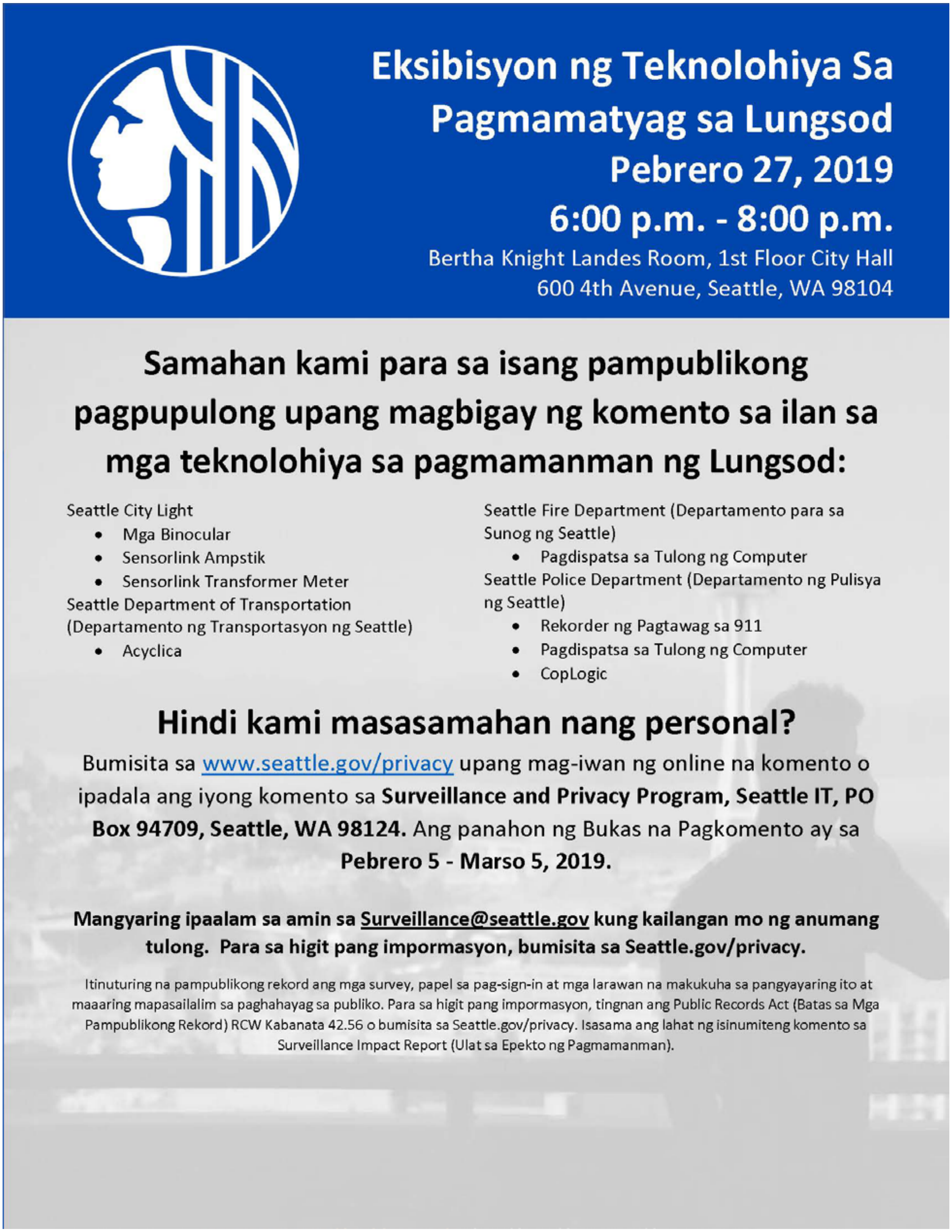
- Hệ Thống Ghi Âm Cuộc Gọi 911
- Hệ Thống Thông Tin Điều Vận Có Máy Tính Trợ Giúp
- CopLogic

Quý vị không thể tới tham dự trực tiếp cùng chúng tôi?

Hãy truy cập www.seattle.gov/privacy và để lại nhận xét trực tuyến hoặc gửi ý kiến của quý vị tới **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Giai đoạn Góp Ý Mở từ **Ngày 5 tháng 2 - Ngày 5 tháng 3 năm 2019.**

Vui lòng thông báo cho chúng tôi tại Surveillance@seattle.gov nếu quý vị cần bất kỳ điều chỉnh nào. Để có thêm thông tin, hãy truy cập Seattle.gov/privacy.

Các khảo sát, danh sách đăng ký và ảnh chụp tại sự kiện này được coi là thông tin công cộng và có thể được tiết lộ công khai. Để biết thêm thông tin, hãy tham khảo Public Records Act (Đạo Luật Hồ Sơ Công Cộng) RCW Chương 42.56 hoặc truy cập Seattle.gov/privacy. Tất cả các ý kiến đóng góp mà quý vị gửi đến sẽ được đưa vào Báo Cáo Tác Động Giám Sát.



Eksibisyon ng Teknolohiya Sa Pagmamatyag sa Lungsod

Pebrero 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Samahan kami para sa isang pampublikong pagpupulong upang magbigay ng komento sa ilan sa mga teknolohiya sa pagmamanman ng Lungsod:

Seattle City Light

- Mga Binocular
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento ng Transportasyon ng Seattle)

- Acyclica

Seattle Fire Department (Departamento para sa Sunog ng Seattle)

- Pagdispatsa sa Tulong ng Computer

Seattle Police Department (Departamento ng Pulisya ng Seattle)

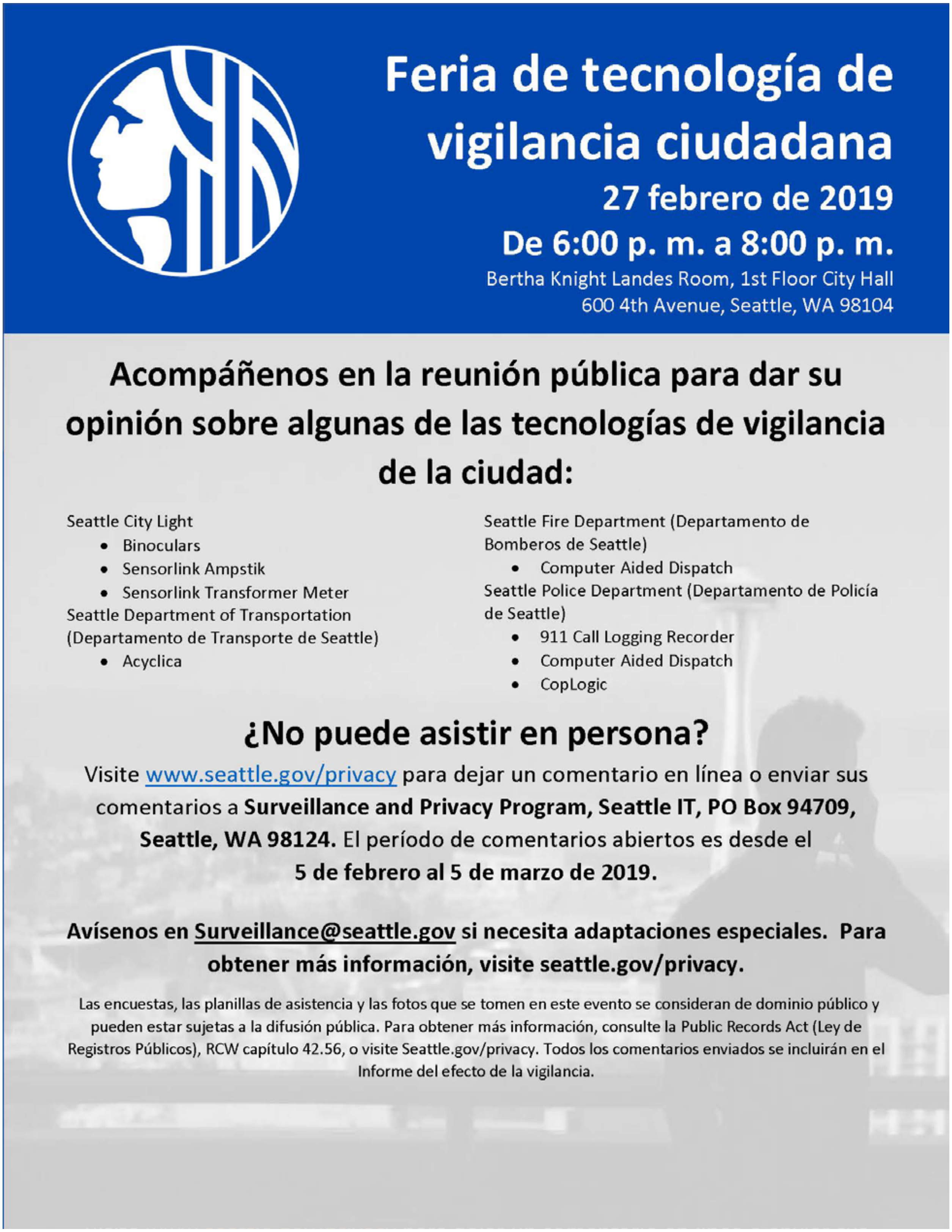
- Rekorder ng Pagtawag sa 911
- Pagdispatsa sa Tulong ng Computer
- CopLogic

Hindi kami masasamahan nang personal?

Bumisita sa www.seattle.gov/privacy upang mag-iwan ng online na komento o ipadala ang iyong komento sa **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** Ang panahon ng Bukas na Pagkomento ay sa **Pebrero 5 - Marso 5, 2019.**

Mangyaring ipaalam sa amin sa Surveillance@seattle.gov kung kailangan mo ng anumang tulong. Para sa higit pang impormasyon, bumisita sa Seattle.gov/privacy.

Itinuturing na pampublikong rekord ang mga survey, papel sa pag-sign-in at mga larawan na makukuha sa pangyayaring ito at maaaring mapasailalim sa paghahayag sa publiko. Para sa higit pang impormasyon, tingnan ang Public Records Act (Batas sa Mga Pampublikong Rekord) RCW Kabanata 42.56 o bumisita sa Seattle.gov/privacy. Isasama ang lahat ng isinumiteng komento sa Surveillance Impact Report (Ulat sa Epekto ng Pagmamanman).



Feria de tecnología de vigilancia ciudadana

27 febrero de 2019

De 6:00 p. m. a 8:00 p. m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Acompáñenos en la reunión pública para dar su opinión sobre algunas de las tecnologías de vigilancia de la ciudad:

Seattle City Light

- Binoculars
- Sensorlink Ampstik
- Sensorlink Transformer Meter

Seattle Department of Transportation (Departamento de Transporte de Seattle)

- Acyclica

Seattle Fire Department (Departamento de Bomberos de Seattle)

- Computer Aided Dispatch

Seattle Police Department (Departamento de Policía de Seattle)

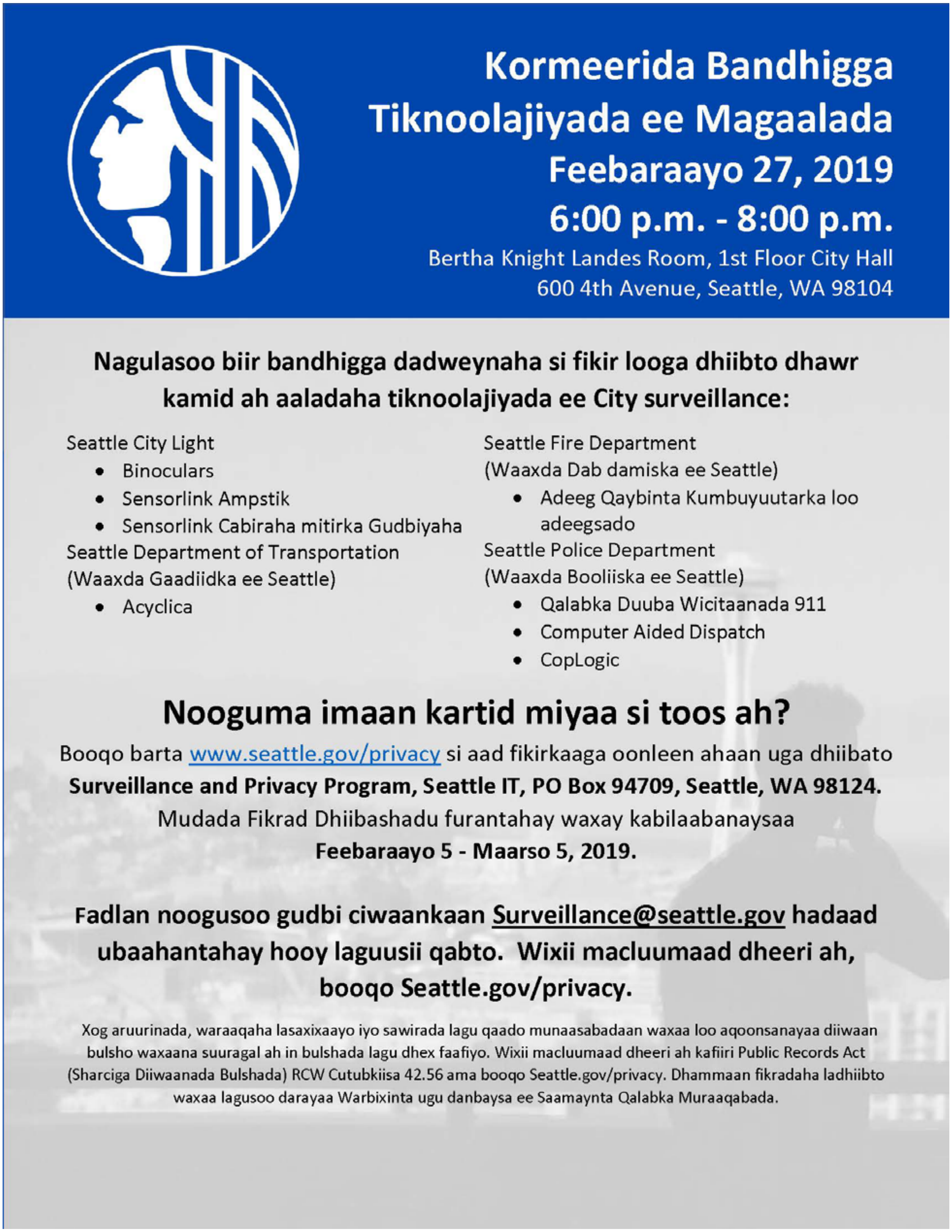
- 911 Call Logging Recorder
- Computer Aided Dispatch
- CopLogic

¿No puede asistir en persona?

Visite www.seattle.gov/privacy para dejar un comentario en línea o enviar sus comentarios a **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.** El período de comentarios abiertos es desde el **5 de febrero al 5 de marzo de 2019.**

Avísenos en Surveillance@seattle.gov si necesita adaptaciones especiales. Para obtener más información, visite seattle.gov/privacy.

Las encuestas, las planillas de asistencia y las fotos que se tomen en este evento se consideran de dominio público y pueden estar sujetas a la difusión pública. Para obtener más información, consulte la Public Records Act (Ley de Registros Públicos), RCW capítulo 42.56, o visite Seattle.gov/privacy. Todos los comentarios enviados se incluirán en el Informe del efecto de la vigilancia.



Kormeerida Bandhigga Tiknoolajiyada ee Magaalada

Feebaraayo 27, 2019

6:00 p.m. - 8:00 p.m.

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

Nagulasoo biir bandhigga dadweynaha si fikir looga dhiibto dhawr kamid ah aaladaha tiknoolajiyada ee City surveillance:

Seattle City Light

- Binoculars
- Sensorlink Ampstik
- Sensorlink Cabiraha mitirka Gudbiyaha

Seattle Department of Transportation
(Waaxda Gaadiidka ee Seattle)

- Acyclica

Seattle Fire Department
(Waaxda Dab damiska ee Seattle)

- Adeeg Qaybinta Kumbuyuutarka loo adeegsado

Seattle Police Department
(Waaxda Booliiska ee Seattle)

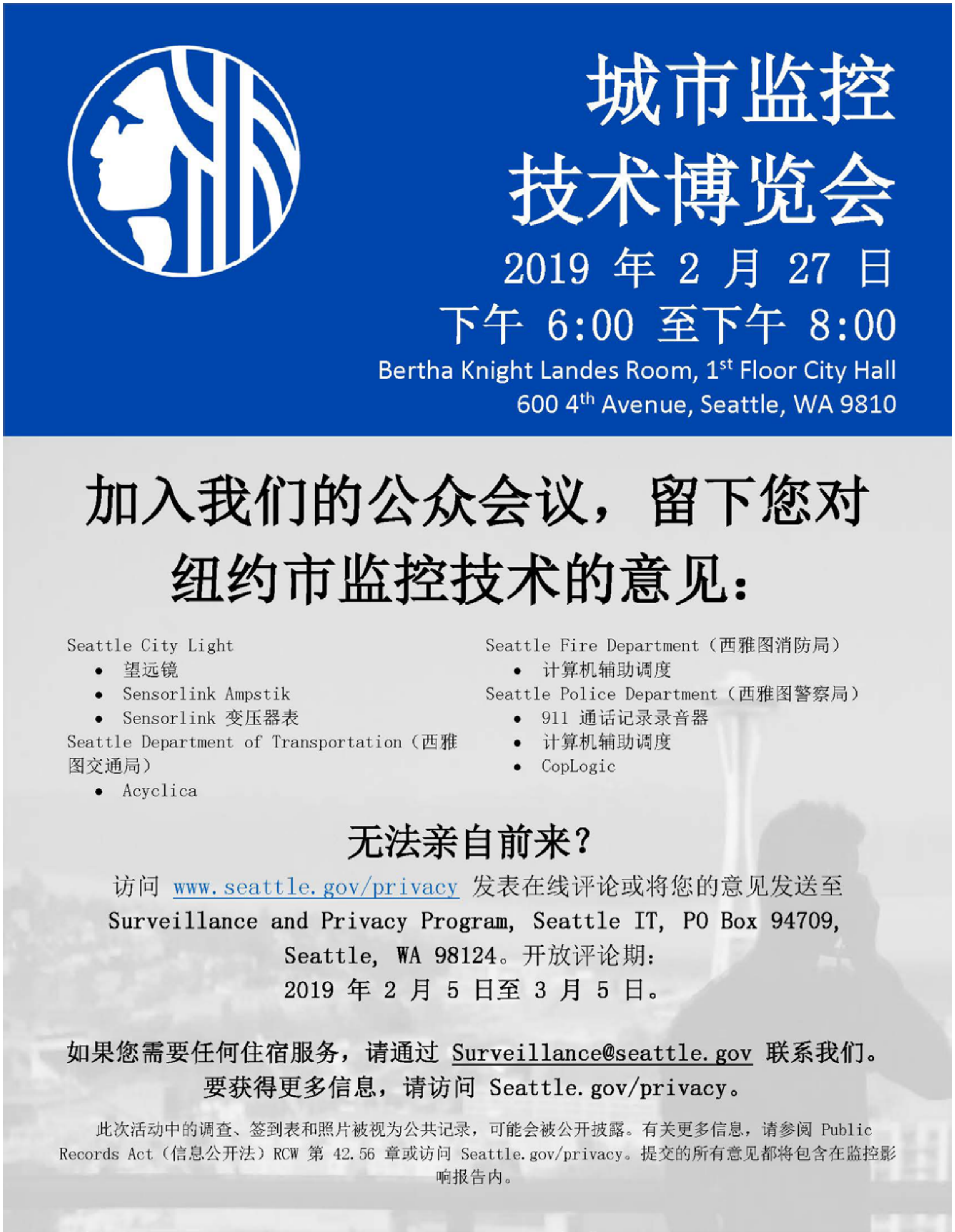
- Qalabka Duuba Wicitaanada 911
- Computer Aided Dispatch
- CopLogic

Nooguma imaan kartid miyaa si toos ah?

Booqo barta www.seattle.gov/privacy si aad fikirkaaga oonleen ahaan uga dhiibato **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124.**
Mudada Fikrad Dhiibashadu furantahay waxay kabilaabanaysaa
Feebaraayo 5 - Maarso 5, 2019.

Fadlan noogusoo gudbi ciwaankaan Surveillance@seattle.gov hadaad ubaahantahay hooy laguusii qabto. Wixii macluumaad dheeri ah, booqo Seattle.gov/privacy.

Xog aruurinada, waraaqaha lasaxixaayo iyo sawirada lagu qaado munaasabadaan waxaa loo aqoonsanayaa diiwaan bulsho waxaana suuragal ah in bulshada lagu dhex faafiyo. Wixii macluumaad dheeri ah kafiiri Public Records Act (Sharciga Diiwaanada Bulshada) RCW Cutubkiisa 42.56 ama booqo Seattle.gov/privacy. Dhammaan fikradaha ladhiibto waxaa lagusoo darayaa Warbixinta ugu danbaysa ee Saamaynta Qalabka Muraaqabada.



城市监控技术博览会

2019 年 2 月 27 日

下午 6:00 至下午 8:00

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 9810

加入我们的公众会议，留下您对纽约市监控技术的意见：

Seattle City Light

- 望远镜
- Sensorlink Ampstik
- Sensorlink 变压器表

Seattle Department of Transportation（西雅图交通局）

- Acyclica

Seattle Fire Department（西雅图消防局）

- 计算机辅助调度

Seattle Police Department（西雅图警察局）

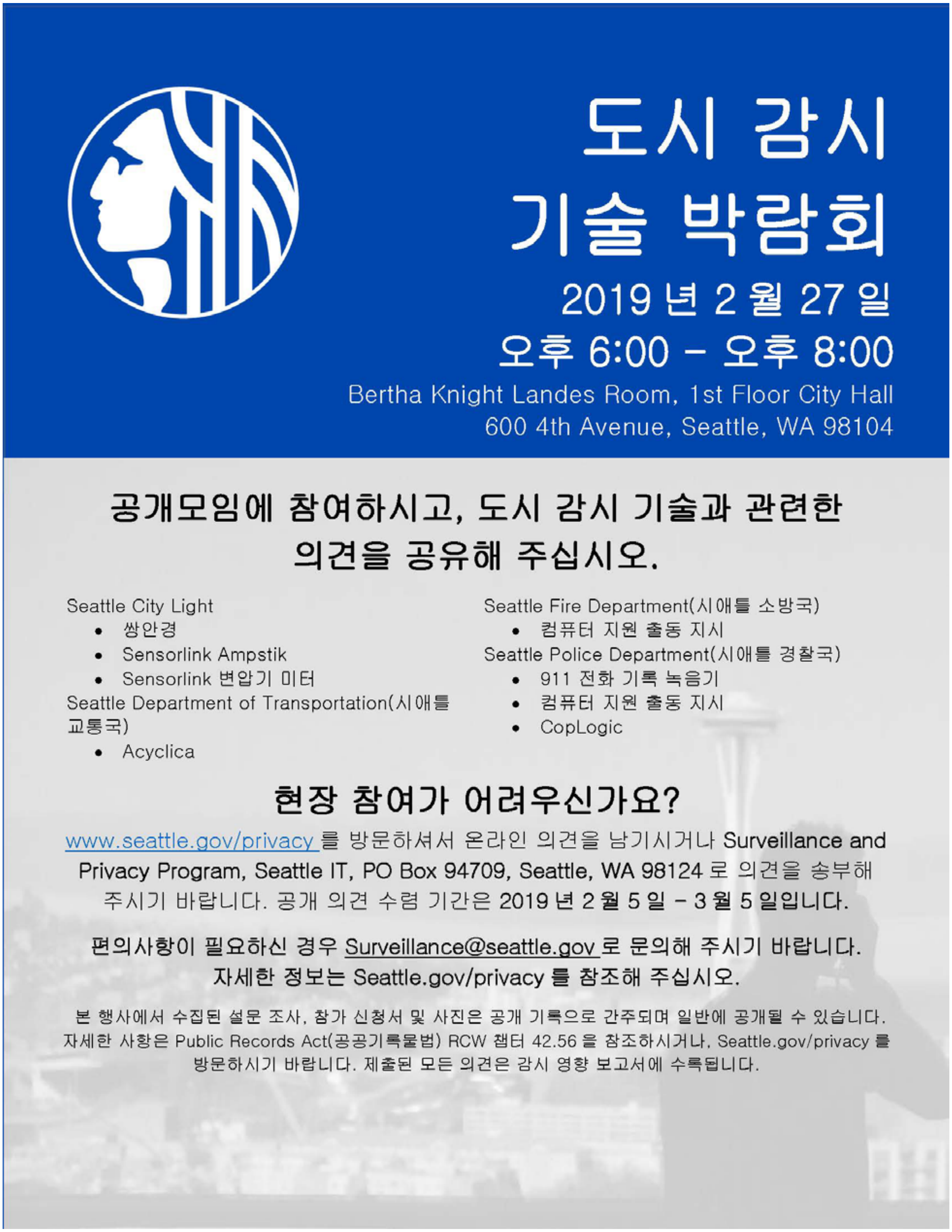
- 911 通话记录录音器
- 计算机辅助调度
- CopLogic

无法亲自前来?

访问 www.seattle.gov/privacy 发表在线评论或将您的意见发送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。开放评论期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何住宿服务，请通过 Surveillance@seattle.gov 联系我们。要获得更多信息，请访问 Seattle.gov/privacy。

此次活动中的调查、签到表和照片被视为公共记录，可能会被公开披露。有关更多信息，请参阅 Public Records Act（信息公开法）RCW 第 42.56 章或访问 Seattle.gov/privacy。提交的所有意见都将包含在监控影响报告内。



도시 감시 기술 박람회

2019 년 2 월 27 일
오후 6:00 – 오후 8:00

Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

공개모임에 참여하시고, 도시 감시 기술과 관련한 의견을 공유해 주십시오.

Seattle City Light

- 쌍안경
- Sensorlink Ampstik
- Sensorlink 변압기 미터

Seattle Department of Transportation(시애틀 교통국)

- Acyclica

Seattle Fire Department(시애틀 소방국)

- 컴퓨터 지원 출동 지시

Seattle Police Department(시애틀 경찰국)

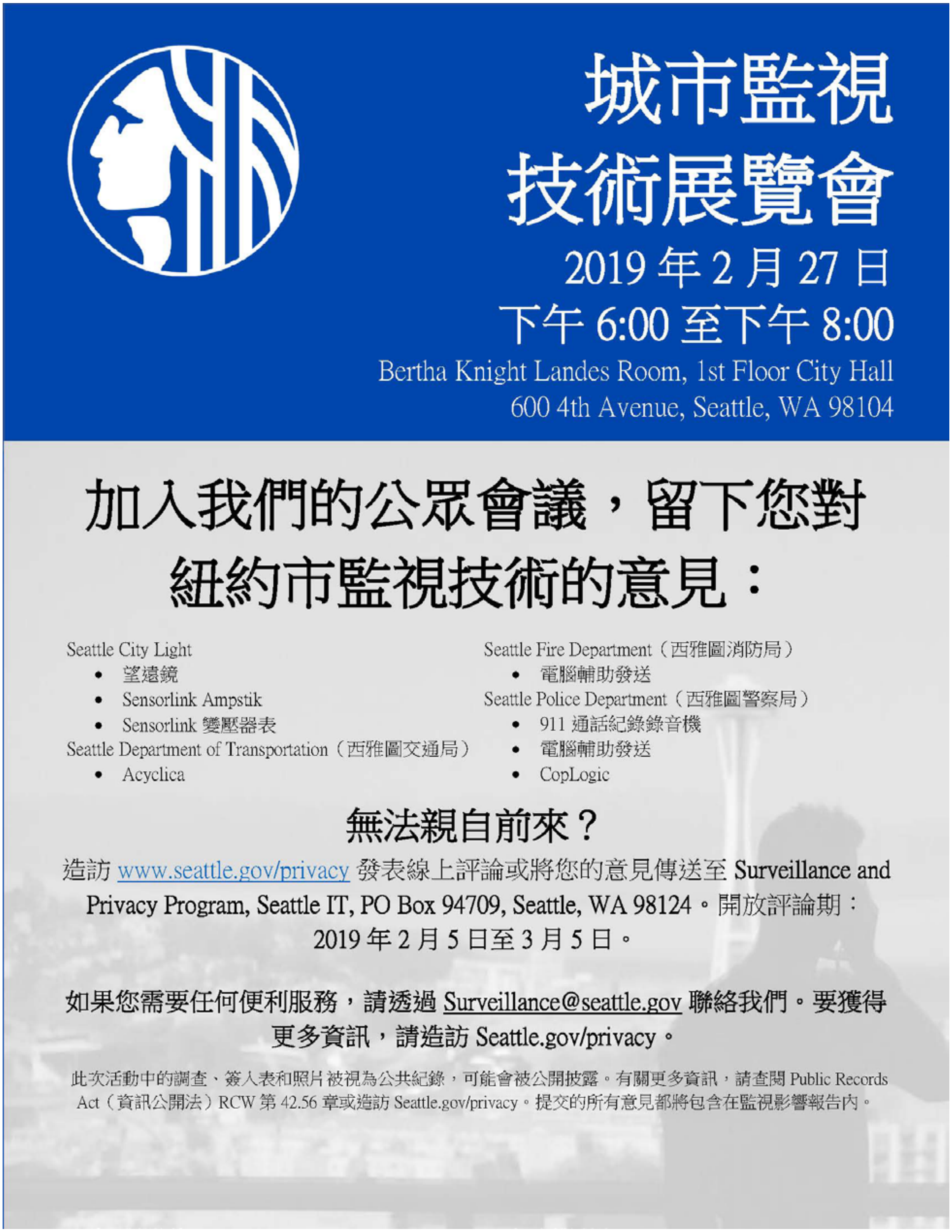
- 911 전화 기록 녹음기
- 컴퓨터 지원 출동 지시
- CopLogic

현장 참여가 어려우신가요?

www.seattle.gov/privacy 를 방문하셔서 온라인 의견을 남기시거나 **Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124** 로 의견을 송부해 주시기 바랍니다. 공개 의견 수렴 기간은 **2019 년 2 월 5 일 – 3 월 5 일입니다.**

편의사항이 필요하신 경우 Surveillance@seattle.gov 로 문의해 주시기 바랍니다.
자세한 정보는 Seattle.gov/privacy 를 참조해 주십시오.

본 행사에서 수집된 설문 조사, 참가 신청서 및 사진은 공개 기록으로 간주되며 일반에 공개될 수 있습니다. 자세한 사항은 Public Records Act(공공기록물법) RCW 챕터 42.56 을 참조하시거나, Seattle.gov/privacy 를 방문하시기 바랍니다. 제출된 모든 의견은 감시 영향 보고서에 수록됩니다.



城市監視技術展覽會

2019 年 2 月 27 日
下午 6:00 至下午 8:00
Bertha Knight Landes Room, 1st Floor City Hall
600 4th Avenue, Seattle, WA 98104

加入我們的公眾會議，留下您對紐約市監視技術的意見：

Seattle City Light
- 望遠鏡
- Sensorlink Ampstik
- Sensorlink 變壓器表

Seattle Department of Transportation（西雅圖交通局）
- Acyclica

Seattle Fire Department（西雅圖消防局）
- 電腦輔助發送

Seattle Police Department（西雅圖警察局）
- 911 通話紀錄錄音機
- 電腦輔助發送
- CopLogic

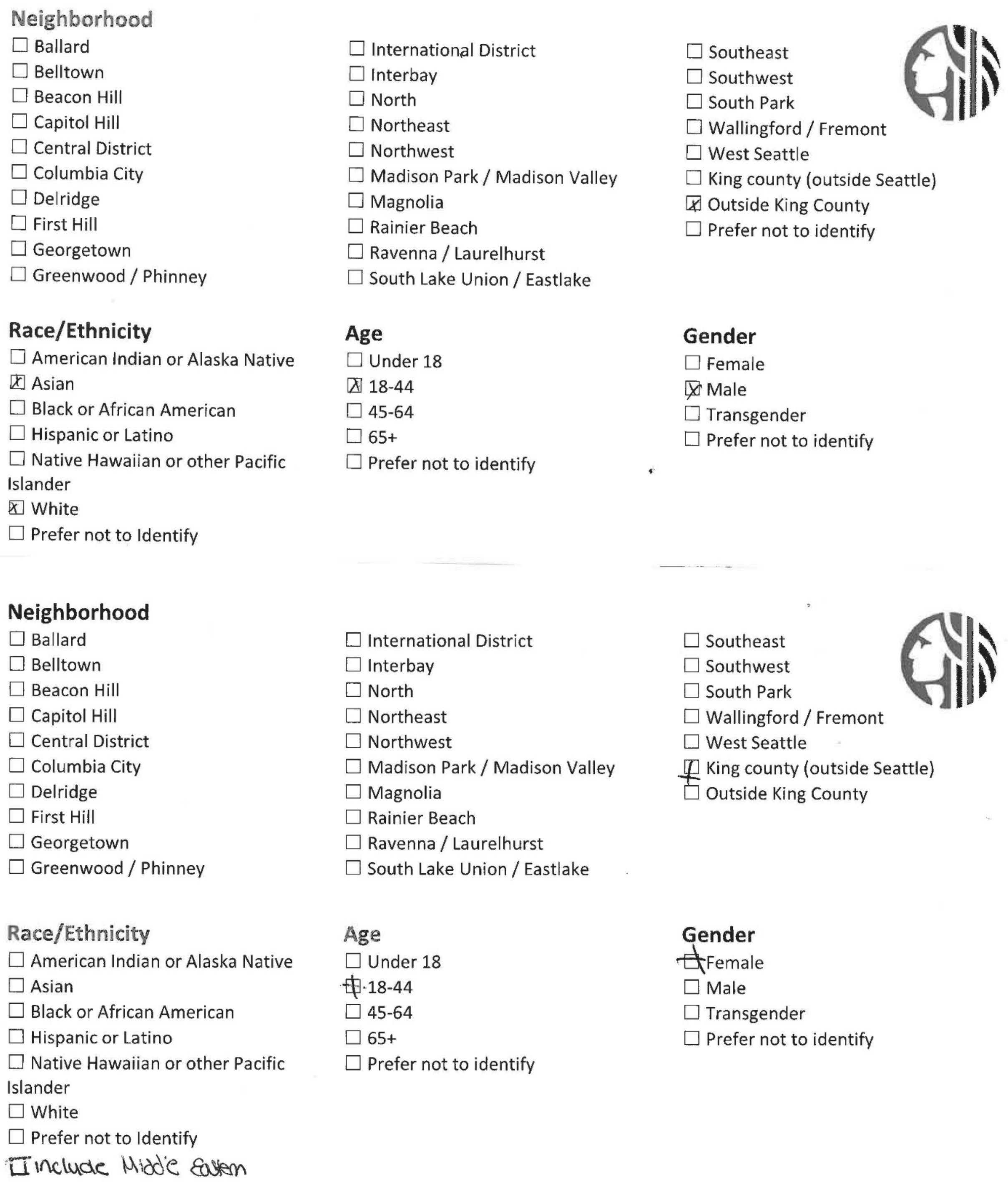
無法親自前來？

造訪 www.seattle.gov/privacy 發表線上評論或將您的意見傳送至 Surveillance and Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124。開放評論期：2019 年 2 月 5 日至 3 月 5 日。

如果您需要任何便利服務，請透過 Surveillance@seattle.gov 聯絡我們。要獲得更多資訊，請造訪 Seattle.gov/privacy。

此次活動中的調查、簽入表和照片被視為公共紀錄，可能會被公開披露。有關更多資訊，請查閱 Public Records Act（資訊公開法）RCW 第 42.56 章或造訪 Seattle.gov/privacy。提交的所有意見都將包含在監視影響報告內。

Appendix C: Meeting Sign-in Sheet(s)



Neighborhood

☐ 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
☐ Prefer not to identify

Race/Ethnicity

☐ American Indian or Alaska Native
☒ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☒ White
☐ Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☒ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

☐ 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

Race/Ethnicity

☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify
☐ include Middle Eastern

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

□ 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
□ Prefer not to identify

Race/Ethnicity

□ American Indian or Alaska Native
□ Asian
☒ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
□ White
□ Prefer not to Identify

Age

□ Under 18
☒ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

☒ Female
□ Male
□ Transgender
□ Prefer not to identify

Neighborhood

□ 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
□ Prefer not to identify

Race/Ethnicity

□ American Indian or Alaska Native
□ Asian
☒ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
□ White
□ Prefer not to Identify

Age

□ Under 18
☒ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☒ Male
□ Transgender
□ Prefer not to identify

Neighborhood

☐ 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
☐ Prefer not to identify

Race/Ethnicity

☐ American Indian or Alaska Native
☐ Asian
☒ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

☐ 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

Race/Ethnicity

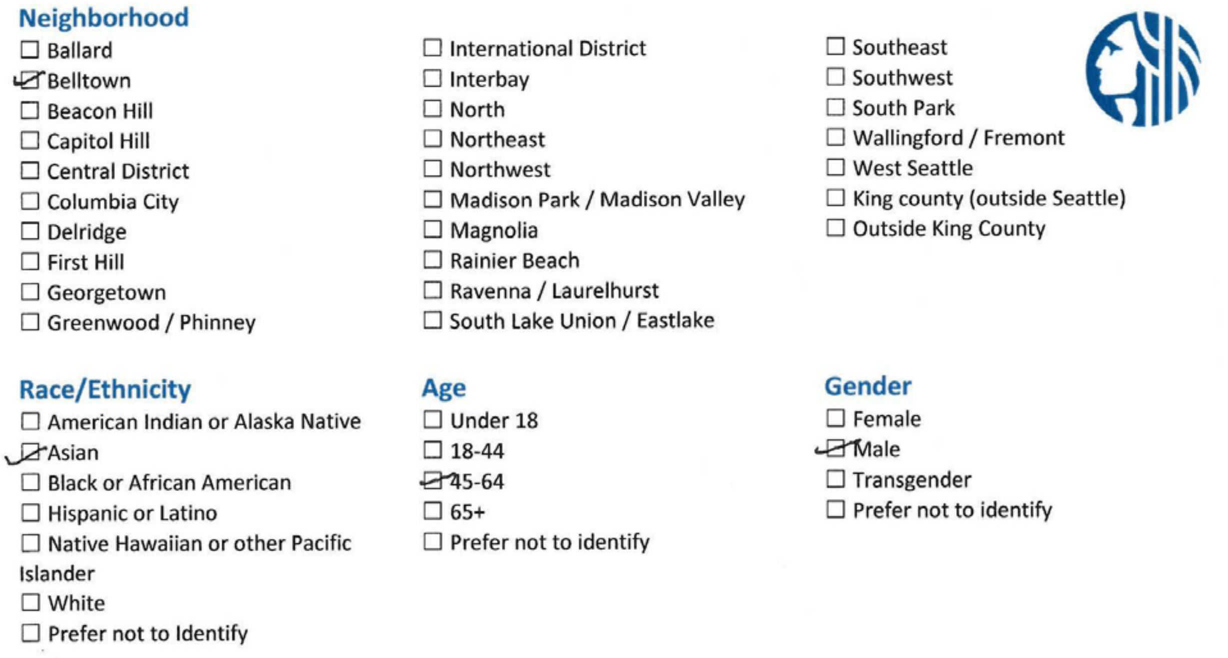
☐ American Indian or Alaska Native
☑ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify

Age

☐ Under 18
☑ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

□ 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

Race/Ethnicity

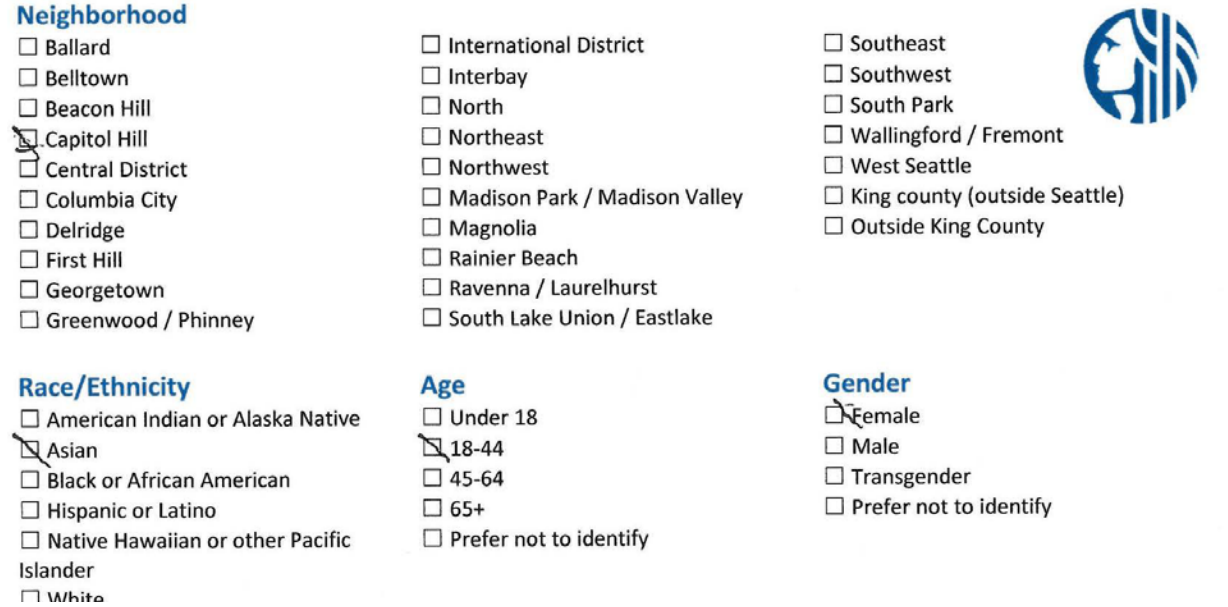
□ American Indian or Alaska Native
☑ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
□ White
□ Prefer not to Identify

Age

□ Under 18
□ 18-44
☑ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☑ Male
□ Transgender
□ Prefer not to identify



Neighborhood

□ 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

Race/Ethnicity

□ American Indian or Alaska Native
☒ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
□ White

Age

□ Under 18
☒ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

☒ Female
□ Male
□ Transgender
□ Prefer not to identify

Neighborhood

□ 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

Race/Ethnicity

□ American Indian or Alaska Native
☑ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
□ White
□ Prefer not to Identify

Age

□ Under 18
☑ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☑ Male
□ Transgender
□ Prefer not to identify

Neighborhood

☒ 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

Race/Ethnicity

□ American Indian or Alaska Native
□ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
☒ White
□ Prefer not to Identify

Age

□ Under 18
☒ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☒ Male
□ Transgender
□ Prefer not to identify

Neighborhood

☐ 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

Race/Ethnicity

☐ American Indian or Alaska Native
☑ Asian
☐ Black or African American
☑ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify

Age

☐ Under 18
☑ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

Queen Anne

Neighborhood

☐ 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

Race/Ethnicity

☐ American Indian or Alaska Native
☒ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

☐ 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

Race/Ethnicity

☐ American Indian or Alaska Native
☐ Asian
☑ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify

Age

☐ Under 18
☑ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

☐ 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

Race/Ethnicity

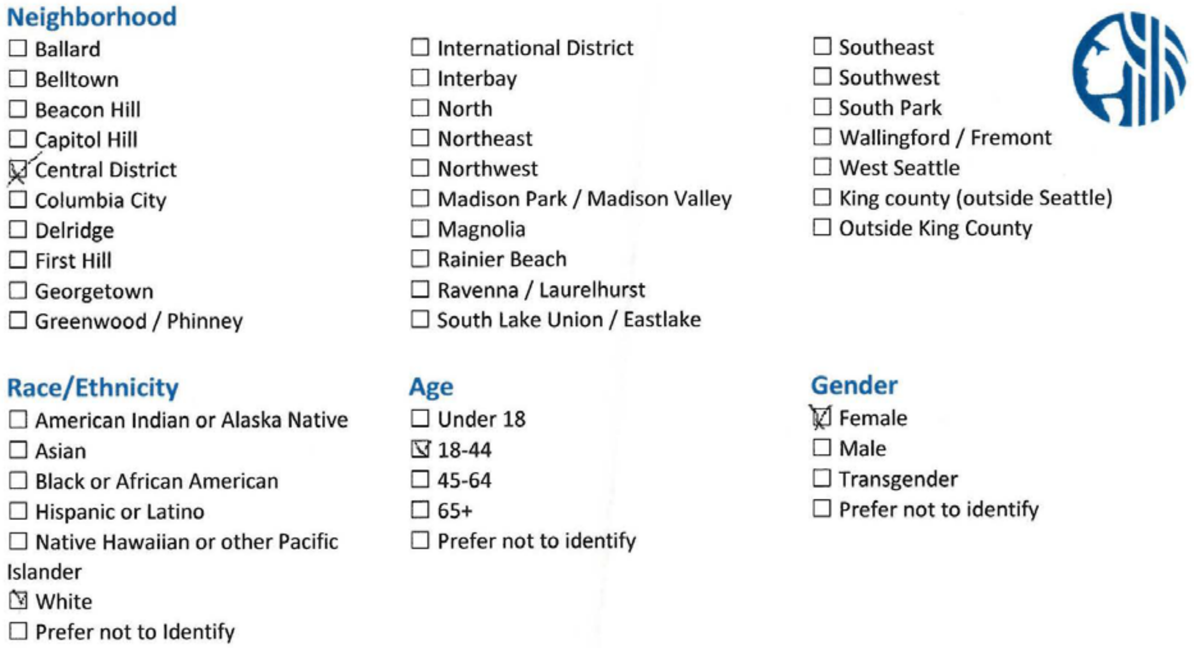
☐ American Indian or Alaska Native
☐ Asian
☑ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☒ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

☐ 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

Race/Ethnicity

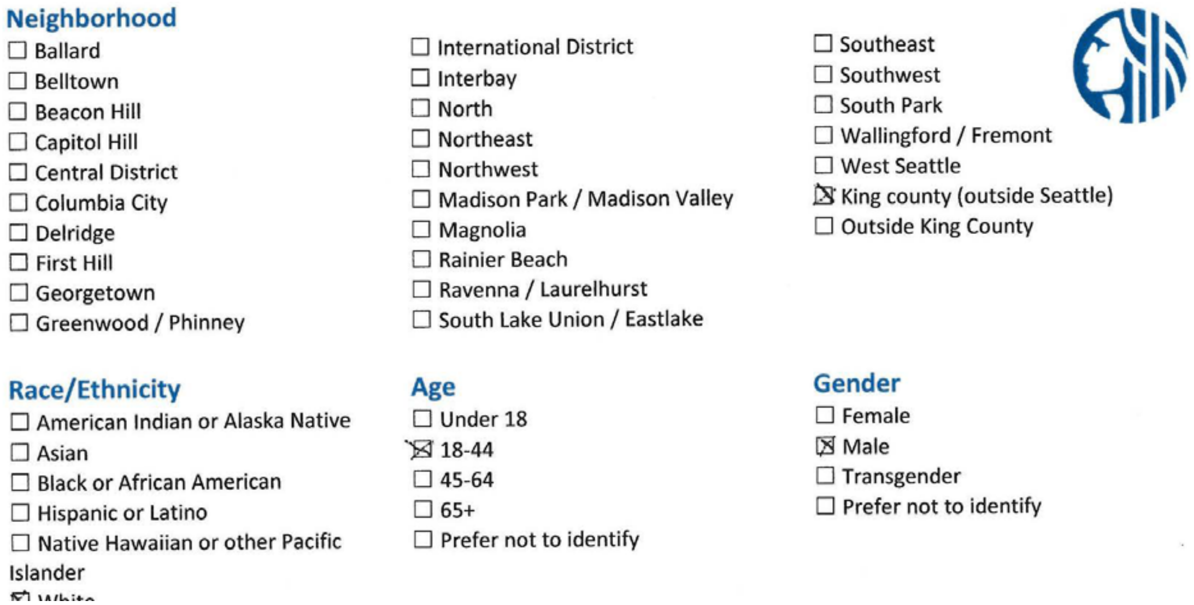
☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☒ White
☐ Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

☐ 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

Race/Ethnicity

☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☒ White

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☒ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

☒ 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

Race/Ethnicity

☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☒ White
☐ Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

Neighborhood

☐ 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

Race/Ethnicity

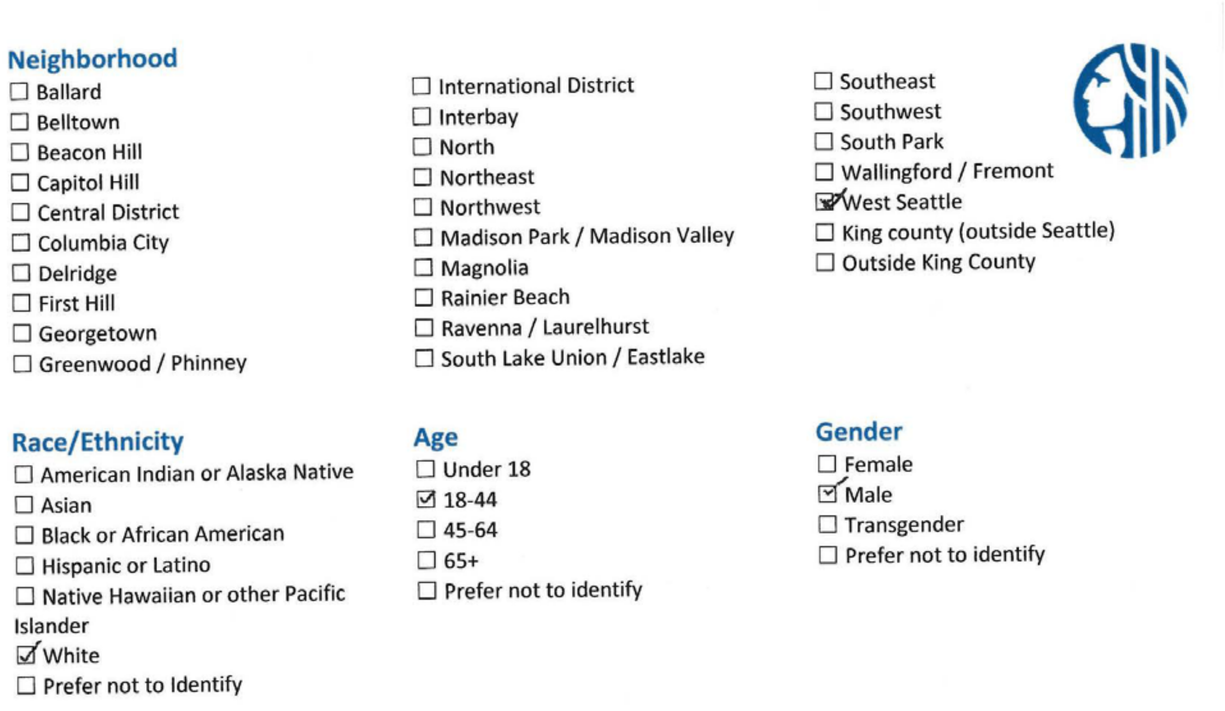
☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☒ White
☐ Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☒ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

□ 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

Race/Ethnicity

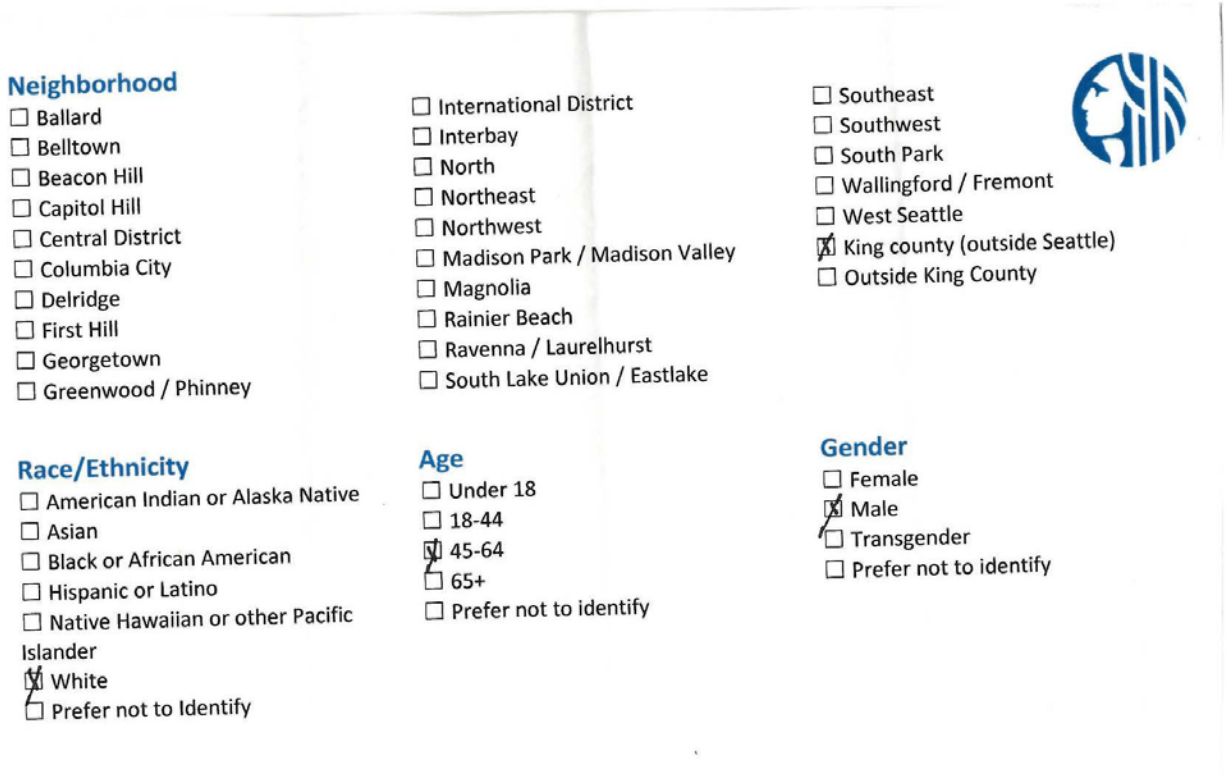
□ American Indian or Alaska Native
□ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
☑ White
□ Prefer not to Identify

Age

□ Under 18
☑ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☑ Male
□ Transgender
□ Prefer not to identify



Neighborhood

□ 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

Race/Ethnicity

□ American Indian or Alaska Native
□ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
☒ White
□ Prefer not to Identify

Age

□ Under 18
□ 18-44
☒ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☒ Male
□ Transgender
□ Prefer not to identify

Neighborhood

- ☐ 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

X

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☒ 18-44
- ☐ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

- ☐ 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

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☒ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☒ 65+
- ☐ Prefer not to identify

Gender

- ☐ Female
- ☒ Male
- ☐ Transgender
- ☐ Prefer not to identify

Neighborhood

□ 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

Race/Ethnicity

□ American Indian or Alaska Native
□ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
☒ White
□ Prefer not to Identify

Age

□ Under 18
☒ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

☒ Female
□ Male
□ Transgender
□ Prefer not to identify

Neighborhood

☒ 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

Race/Ethnicity

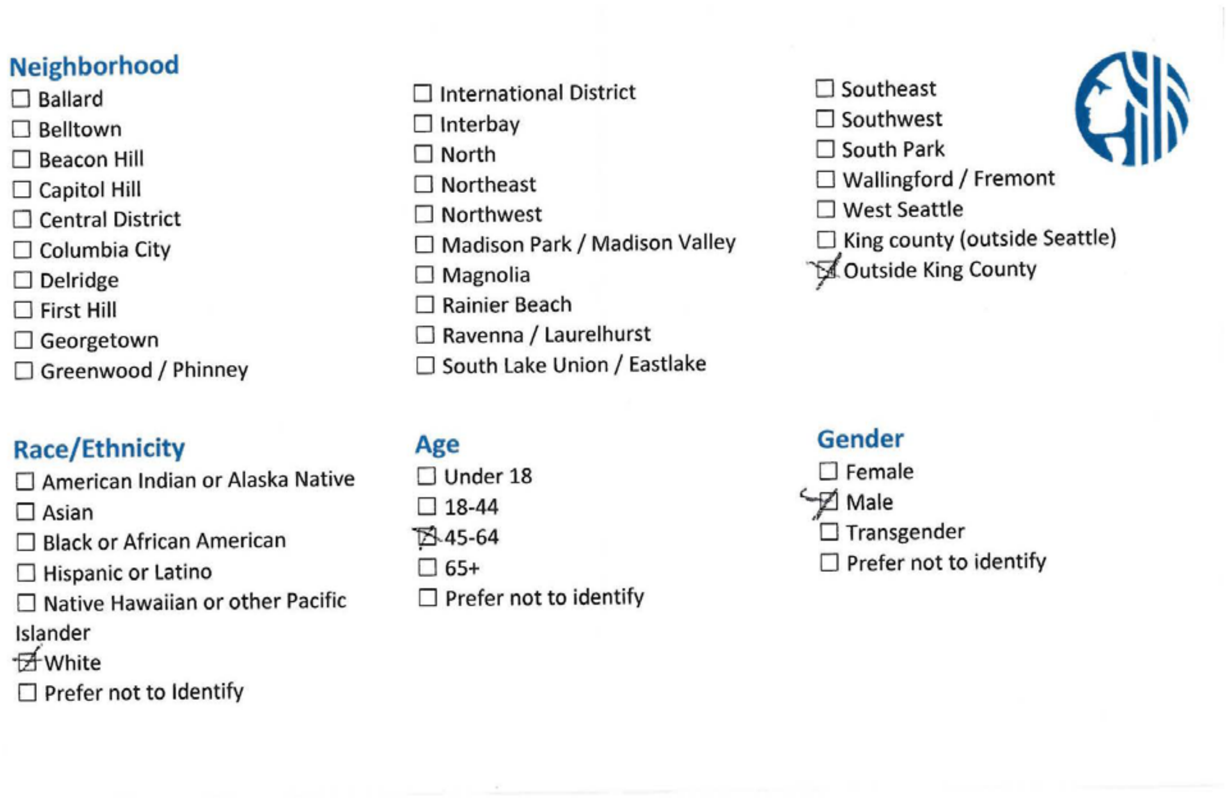
□ American Indian or Alaska Native
□ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
☒ White
□ Prefer not to Identify

Age

□ Under 18
☒ 18-44
□ 45-64
□ 65+
□ Prefer not to identify

Gender

☒ Female
□ Male
□ Transgender
□ Prefer not to identify



Neighborhood

□ 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

Race/Ethnicity

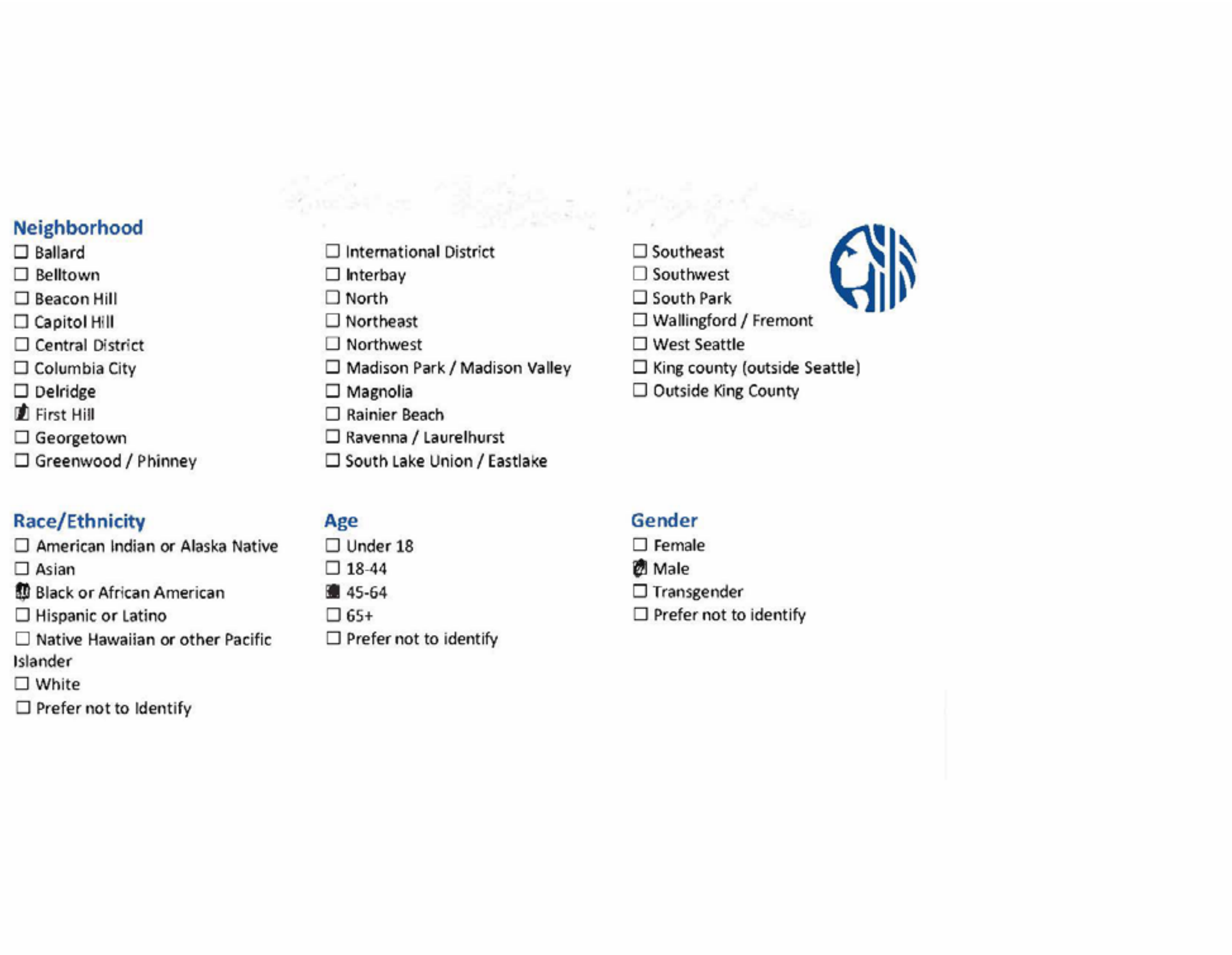
□ American Indian or Alaska Native
□ Asian
□ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
☒ White
□ Prefer not to Identify

Age

□ Under 18
□ 18-44
☒ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☒ Male
□ Transgender
□ Prefer not to identify



Neighborhood

□ 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

Race/Ethnicity

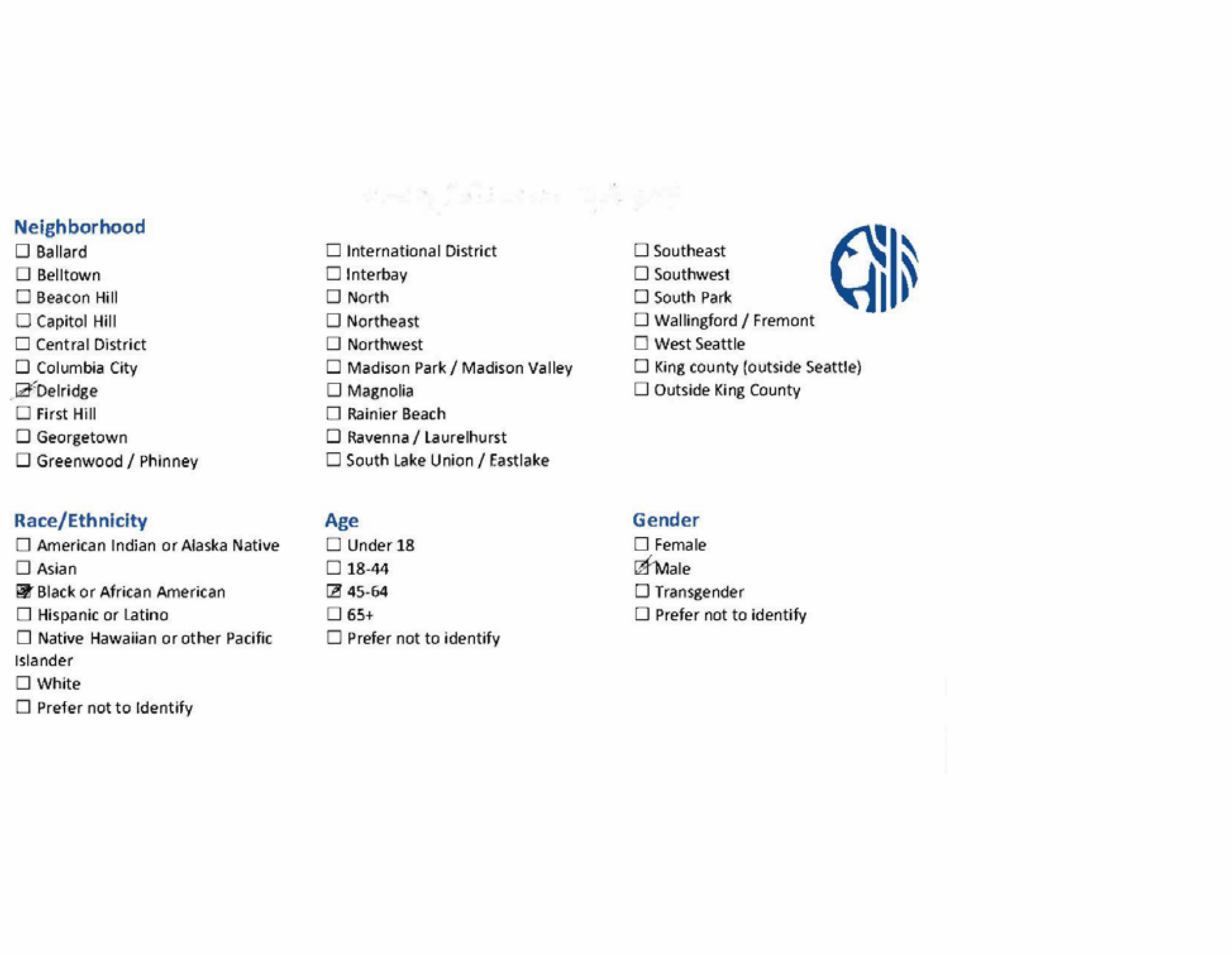
□ American Indian or Alaska Native
□ Asian
☒ Black or African American
□ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
□ White
□ Prefer not to Identify

Age

□ Under 18
□ 18-44
☒ 45-64
□ 65+
□ Prefer not to identify

Gender

□ Female
☒ Male
□ Transgender
□ Prefer not to identify



Neighborhood

☐ 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

Race/Ethnicity

☐ American Indian or Alaska Native
☐ Asian
☑ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☐ Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

leighborhood

] 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
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
☑ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☒ 18-44
☐ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

leighborhood

] 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
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
☑ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify

eighborhood

] 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
☐ Prefer not to identify

ace/Ethnicity

] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify

eighborhood

] Ballard
] Belltown
] Beacon Hill
] Capitol Hill
] Central District
] Columbia City
] Delridge
] First Hill
] Georgetown
] Greenwood / Phinney

SE KING COUNTY

☐ 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
☐ Prefer not to identify

ace/Ethnicity

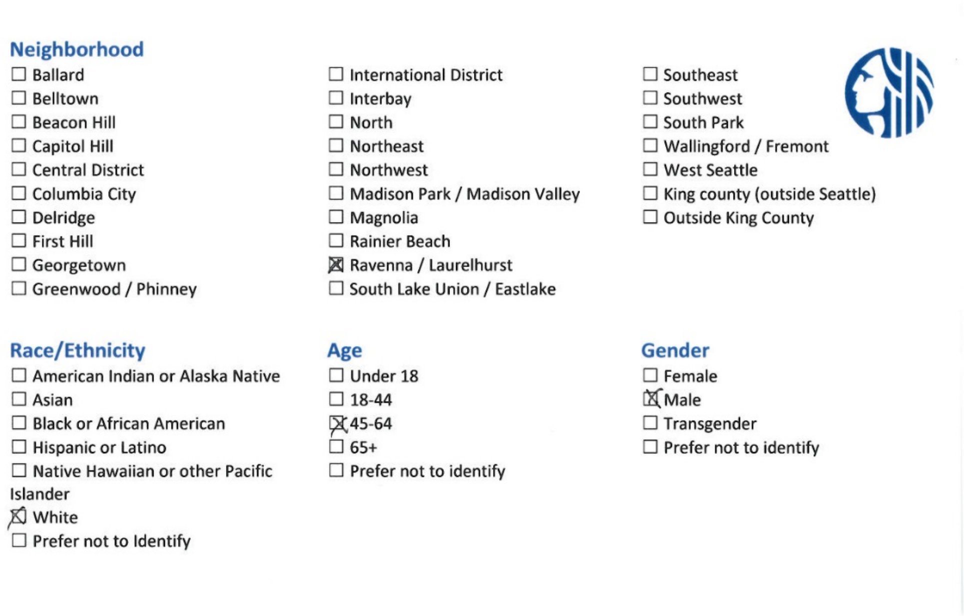
] American Indian or Alaska Native
✓ Asian
] Black or African American
] Hispanic or Latino
] Native Hawaiian or other Pacific lander
] White
] Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☑ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☑ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

☐ 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

Race/Ethnicity

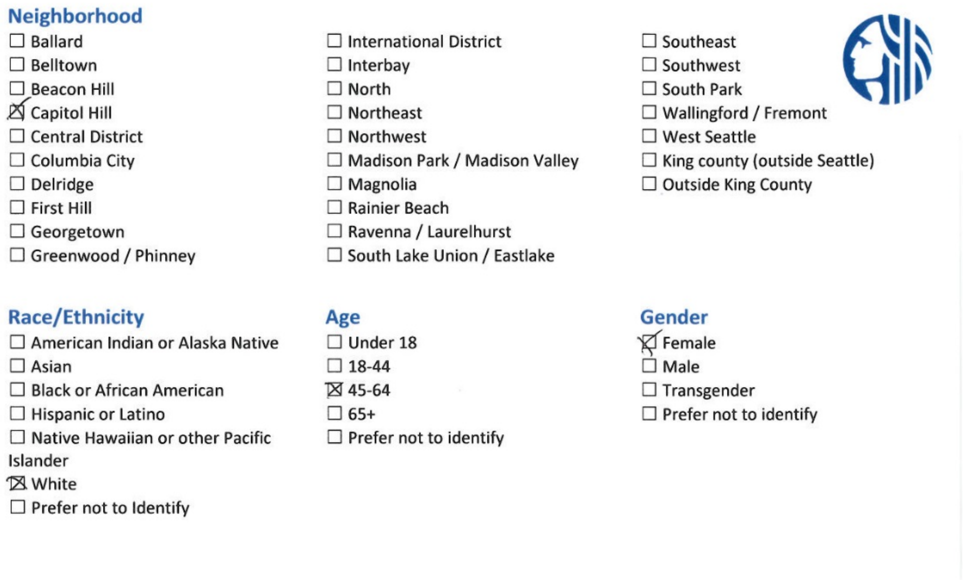
☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☒ White
☐ Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☒ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☐ Female
☒ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

☐ 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

Race/Ethnicity

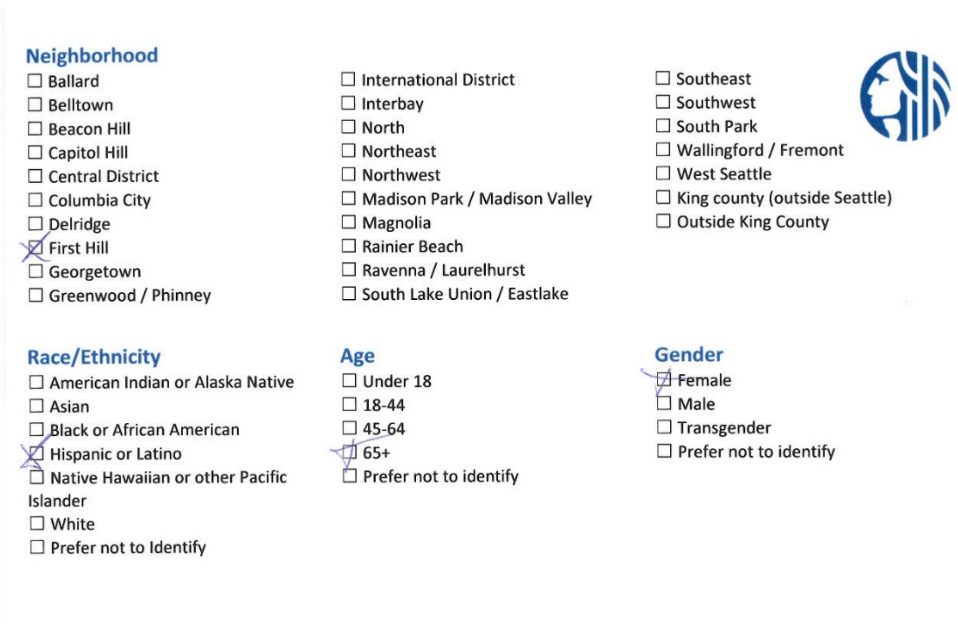
☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☒ White
☐ Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☒ 45-64
☐ 65+
☐ Prefer not to identify

Gender

☒ Female
☐ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

□ 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

Race/Ethnicity

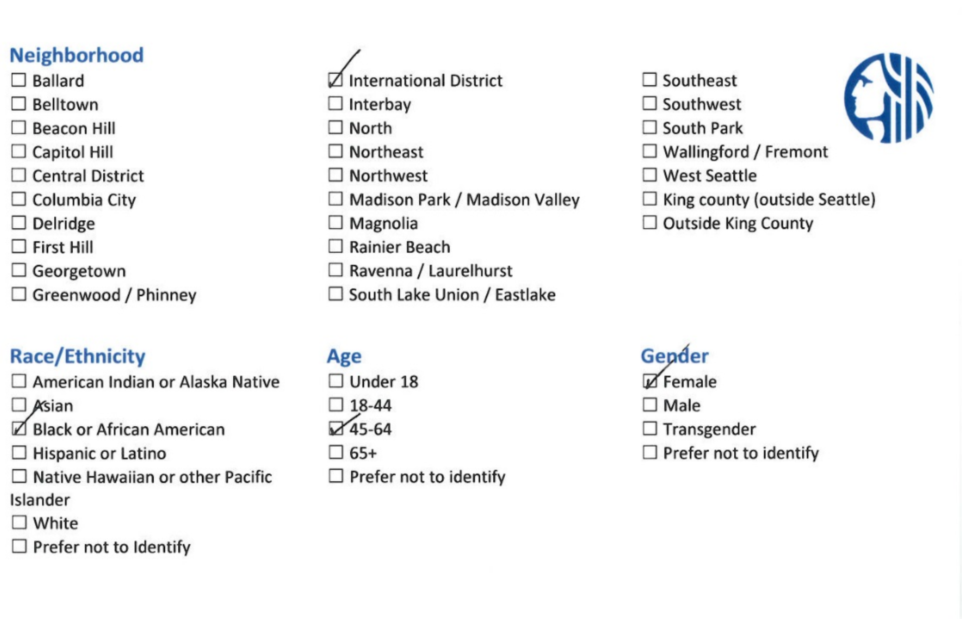
□ American Indian or Alaska Native
□ Asian
□ Black or African American
☒ Hispanic or Latino
□ Native Hawaiian or other Pacific Islander
□ White
□ Prefer not to Identify

Age

□ Under 18
□ 18-44
□ 45-64
☑ 65+
□ Prefer not to identify

Gender

☑ Female
□ Male
□ Transgender
□ Prefer not to identify



Neighborhood

- ☐ 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

Race/Ethnicity

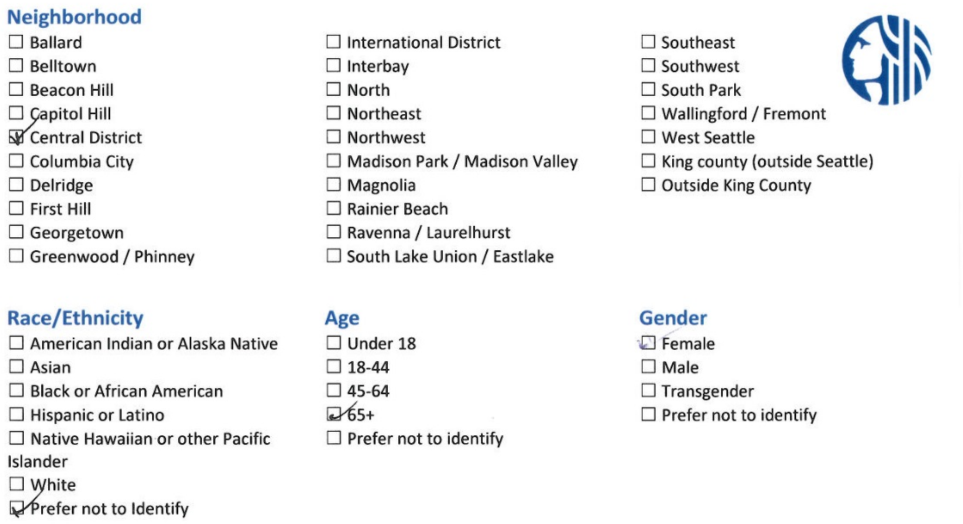
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☑ 45-64
- ☐ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify



Neighborhood

☐ 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

Race/Ethnicity

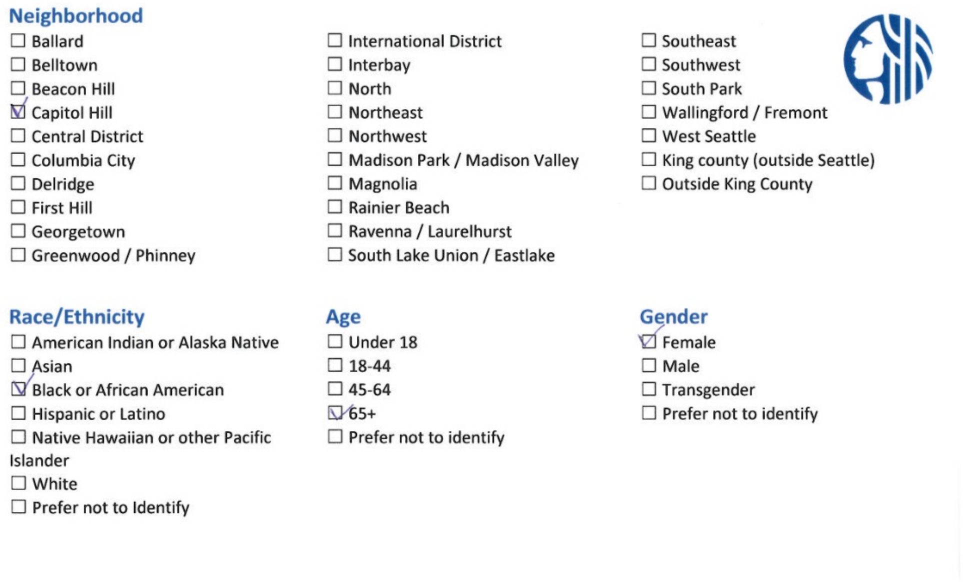
☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Hispanic or Latino
☐ Native Hawaiian or other Pacific Islander
☐ White
☑ Prefer not to Identify

Age

☐ Under 18
☐ 18-44
☐ 45-64
☑ 65+
☐ Prefer not to identify

Gender

☑ Female
☐ Male
☐ Transgender
☐ Prefer not to identify



Neighborhood

- ☐ 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

Race/Ethnicity

- ☐ American Indian or Alaska Native
- ☐ Asian
- ☑ Black or African American
- ☐ Hispanic or Latino
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Prefer not to Identify

Age

- ☐ Under 18
- ☐ 18-44
- ☐ 45-64
- ☑ 65+
- ☐ Prefer not to identify

Gender

- ☑ Female
- ☐ Male
- ☐ Transgender
- ☐ Prefer not to identify

Appendix D: Department of Neighborhood Focus Group Notes

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- Will they keep the data safe on coplogic?
- Can it be hacked?
- What if you report your neighbour and your neighbour hacks the system and find out?
- What is the money amount limit for coplogic / Why is there a limit for coplogic?: (a community member says that she believes that the limit $500 or under, but it’s hard to have a limit because a lot of packages cost more than $500 such as electronics get stolen and you won’t be able to report it online)
- The departement is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it’s not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

What value, if any, do you see in the use of this technology?

- Coplogic has been going on for a few years it's not very effective. The only effective thing is that coplogic is doing saving police hours and time.

What do you want City leadership to consider about the use of this technology?

- Most of the time, our community don’t report things because they don’t trust the system, they often tell someone that they trust a friend. Is there an option that someone and report a crime for someone else?

Other comments:

- The government should be more transparent with the technology system with the public.
- The translation is much far removed from the actual Vietnamese language.

- The translation is very hard to understand, the language is out of context (The flyer is poorly translate)
- Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?
- Police should have a software that connects them to translation and interpretation right away instead of having to call a translator
- How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media? Etc.
- Besides face to face meetings, are there plans to execute this information of the technology and surveillance to the community?
- Will the City of Seattle go to community events, temple, the church to reach out to the community and explain the technologies?
- These technologies are taking a part of our taxes, so everyone should know. It should be for everyone to know, not only catered to one group or population.

Are there any questions you have, or areas you would like more clarification?

- How effective are the tools/technology?
- How many people know of these technologies? Provide statistics
- What are the statistics of the coplogic?
- What is the data and statistics for coplogic and what are people reporting?
- What is the most common crime that they are reporting?
- And how effective is coplogic based on the statistics and data?

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

☐SCL: Binoculars

☐SCL: Sensorlink Ampstik

☐SCL: Sensorlink Transformer Meter (TMS)

☐SDOT: Acyclica

☐SFD: Computer-Aided Dispatch

☒SPD: Computer-Aided Dispatch

☒SPD:9-11 Call Recorder

☐SPD: CopLogic

What concerns, if any, do you have about the use of this technology?

- CAD did not work from experience. A community member said that they reported that they needed assistance at 10:00pm and no one showed up, then had to call 911 at 12:00am and someone finally showed up at 4:30am
- Why create more options and technologies if the police department and government can not support it? It’s a waste of time and money (taxes). Should have enough personals before they implement technology.
- Government should have enough personals to support translation if they choose to translate.

What do you want City leadership to consider about the use of this technology?

- The city should focus on having the community review the technologies that are yet to be implemented.
- The Vietnamese community is not getting the information we need to report crimes

Other comments:

- Engagement is very important. Engaging the community and engaging different demographics.
- Friday night, Saturdays, and Sunday afternoon work the best for the Vietnamese community.
- If the city wants to involve the vietnamese community and engage the Vietnamese community, it is important to accommodate with our community It is important to proofread the translation, have 3 people proofread. Someone
pre 1975, post 1975 and current Vietnamese language. The government clearly does not proofread the translation.

Council on American Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: CopLogic

1. Do you have concerns about this specific technology or how it's used?
    - Having used the system myself the one thing I noted was the type of report you can file, they ask questions like if you knew the suspect, and if you're saying no I don't know who did it. and you check a box that says I understand that no one is going to investigate this
        - What is the point of having a system in place than If no one is going to investigate it
        - It is for common things like my car is broken into and stuff was taken out of my car, you can file it if you need a report for insurance. But if you were to call that and report to the police, they wouldn't come for days
    - So for example if I can be a straight up Islamophobe and I can see a Muslim woman and make a bunch of false reports online, and how long would it take for someone to say I see you making all these reports. Because people can make so many different reports, how do you deal with that
        - There are very limited types of reports that it will accept. So if someone wanted to report graffiti and they were reporting more hate crime related graffiti an officer will review the report
        - So I think the review process would be really important
    - Another barrier is that it's an online system so we need to think about wifi access and there is this assumption that everyone has access to internet and computers. And what I'm hearing is that people can just file a report at a click of their finger. And if these people can do that on their computer what stops them from being able to file all these cases about certain groups and individuals.
    - Additional there have been cases in the past where people are abusing reporting system. This one doesn't allow you to report against known suspect but I could see that happening in the future so I wanted that to be mentioned. The other thing under protection is says all activity can be stored and the data Is monitored by lexis nexus… and this company does a lot of research on crime mapping which brings up some of the concerns on like CVE
        - But what you are saying is that lexis nexus does other mapping that it can use this information for
        - Yes, because I want to clarify what is the technological ambition of SPD because I don't think this would work well in the communities that SPD is supposed to served. And I would want a contract review of what lexis nexus does. Will the info stay on the data and server of lexis nexus, what happens to it
    - Another thing is has SPD given Lexis nexus to use this in any of the research data they do, because they put out a lot of information regarding mapping, and crime control. And what information are they allowed to take
    - We have seen recently people doing interesting things when reporting crimes. I think its important to realize that when reporting crime people have a different perception when reporting crime. People will see you in a certain neighborhood and might think they stole that car, or are doing something bad here. So when we give people the ability to

report online we need to be concerned with accessibility about people being able to report freely… and we saw for a year that if an African American person came to use a swimming pool someone can call and say they don't live here. I think SPD is trying alleviate some of those calls they are getting, but I don't think this is the solution to the problem

- What is the logic behind this overall, because is seems like it presents more cons than pros, and what is analytics database you use to look at these reports. Because when I am using government data base I can see where I need more surveillance etc. so we are getting all these open wholes in the system. Is this a right wing Donald trump agenda to watch neighbors of color and surveillance
- I think im more concerned with where does this information end up and how is it used
- What is the usefulness of the information that is not followed up on. And how does it help the people it's actually serving? So for example someone works for an anti-Muslim white supremacy group and they have people in different areas report issues about different Muslim groups in Seattle how do you prove the validity of these information and make sure they aren't just causing harm

2. What value do you think this brings to our city?
   - I think technology saves time, money, makes filing a report easy, I had to do that once it takes a lot of time.
   - I appreciate that it is easier so something like a hit or run or a car breaking in, that's fine.
3. What worries you about how this is used?
   - The only issues I can think of right now is it seems like it would be very easy to make a fraudulent report or a report that is for a small thing that you can make into a big thing, like the things you see go viral on the internet. So now it seems like the barrier to making a police report is smaller
   - I agree I think the bar is lowered and different people are perceived differently. And we have seen how SPD criminalizes different communities for behaviors that don't need to be criminalizing
   - A lot of different kinds of reports have to do with peoples perceived notion, so my concern comes from how do we make sure that this kind of technology isn't used to map our where Muslims live/are, and there types of religious belief. Or isn't being used to monitor them. How do we ensure that this isn't used to map our communities
   - The only comment I have that in the forms I have filled out is it won't allow you to fill out the form if you are naming a specific individual, you can name a group, but a not a person. The following criteria is there no known suspects, it happens in Seattle, so things like thefts. So you can report, graffiti, identity theft, credit card fraud, simple shop lift. So when I click report it says if you have a suspect it says please call. And when I press report it allows me to report anonymously, so I could report against a community with no follow up
     - Well that doesn't stop them from targeting al-Noor masjid, or Safeway in new holly, or new holly gathering hall, and it can target the people in that community. And people don't feel comfortable with increase police presences, so it targets area if not targeting people
   - When I was buying the house in Dallas (participant currently still lives/works/plays in Seattle) one of the first things I did was looking at a crime map and based off of that if someone is making a lot of reports can that be used for crime mapping because than

that can lower the property value. And if the police isn't following up then how is it being used

- Its definitely possible for people to report inaccurate information

4. What recommendations would you give policy makers at the City about this technology?
   a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
   b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.

5. Can you imagine another way to solve the problem this technology solves?
   - So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
   - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
   - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this

6. Other comments
   a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
    . People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness

    a. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
        - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
    - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.

    b.
2. What value do you think this brings to our city?
    . I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
        - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
    . My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy

    a. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up
        - Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions

- What are the average times for disciplinary actions. How long is the process for a full investigation
- Seattle City Light: It’s a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I’m not sure
- Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don’t have their privacy breach and they are being monitored by a pedophile

4. What recommendations would you give policy makers at the City about this technology?

    . When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a $500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use

5. Can you imagine another way to solve the problem this technology solves?

    . My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.

6. Other comments: (Many comments were discussed over Seattle City Light’s upcoming change from binocular use to automated meter readers)

    . Who opted out was it home owners?

    a. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?

    b. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system

    c. Is there a cost to them to have the new meter.

        - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
        - What I don’t understand is why the new practice is not to just use the new system since that is more accurate and it is doesn’t require binoculars
        - What is the cost of opting out
        - Seattle City Light: There is a flat rate

    - I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves

- Going back to people who make the decision. I want the person who are living in the house to know what decision is being made. So not just the person who owns the house, but the person living in the home. And not everyone it literate and not everyone speaks English. And its really important that you are giving them information they can actually consume. Instead of giving them notices they cant read

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington
Thursday, Feb. 21, 2019
Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
    - Where does this data go? Does it go to SDOT? Google maps?
    - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
    - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
    - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
    - Asking for a greater transparency for how they are doing this
    - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
    - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
    - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
    - I want to ask is this something people opt into
    - People don't even know this is being used

2. What value do you think this brings to our city?
    - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
    - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
    - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
    - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
    - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?

- I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses ways. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
- I don't think this data should be shared with other private agencies, or other interagency programs
- If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
-

5. Can you imagine another way to solve the problem this technology solves?
   - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
   - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
   - Road sensors or ways to count cars
   - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
   - Using vehicle level granularity

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars

☐SCL: Sensorlink Ampstik

☐SCL: Sensorlink Transformer Meter (TMS)

☒SDOT: Acyclica

☐SFD: Computer-Aided Dispatch

☐SPD: Computer-Aided Dispatch

☐SPD:9-11 Call Recorder

☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

El uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

Si vale la pena la inversión

Enfocando al grupo: La tecnología ya está instalada. que les preocupa de su uso?

El tráfico sigue igual.

Quien usa o almacena la información.

La preocupación es la colección de data.

Colección y almacenamiento de información es la mayor preocupación.

No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

El gobierno tiene todos los datos.

No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.
- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

2) What do you want City leadership to consider about the use of this technology?

Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.

La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.

Si es solo para ver el tráfico está bien.

Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Are there any questions you have, or areas you would like more clarification? ●

La tecnología no es un router, sino colección de data para planeaciones urbanas.

Participante: "quiero creer" "convencerme" que los sensores están allí para ayudar con el tráfico.

No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Alternatives to this technology

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.

- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

Entre Hermanos

Please select which technology you wish to comment on:

☒SCL: Binoculars ☒SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☐SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad

Al grupo le incomoda el uso de binoculares

Sensorlynk específicamente la preocupación sería que le quita el trabajo a una persona.

Si es para detectar robo el grupo cree que hay otras maneras de saber quien roba

que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas

2) What value, if any, do you see in the use of this technology?

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

3) What do you want City leadership to consider about the use of this technology?

: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

Are there any questions you have, or areas you would like more clarification? ●

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

Please select which technology you wish to comment on:

☐SCL: Binoculars ☐SCL: Sensorlink Transformer Meter (TMS) ☐SFD: Computer-Aided Dispatch ☐SPD:9-11 Call Recorder

☐SCL: Sensorlink Ampstik ☐SDOT: Acyclica ☐SPD: Computer-Aided Dispatch ☒SPD: CopLogic

1) What concerns, if any, do you have about the use of this technology?

Las fallas electrónicas son preocupantes especialmente en reportes policiacos.

Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.

No todos podrán o saben usar las computadoras.

Fallas de los algoritmos de cada demanda es alarmante.

Que y cuando determina la urgencia de respuesta

Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

2) What value, if any, do you see in the use of this technology?

La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

El uso de computadora está bien para las denuncias.

Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Es otro método para denunciar

Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

3) What do you want City leadership to consider about the use of this technology?
Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Si es usada de manera adecuada y como han dicho está bien.

El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas

What do you think about this technology in particular ?

Grupo están de acuerdo con su uso.

Puede salvar una vida.

Los riesgos y acciones determinan la urgencia de la intermisión policiaca.

Alguna gente se siente más capaz de presentar una queja a través de este sistema, la tecnología en uso tiene validez.

Bueno para la violencia doméstica.

Are there any questions you have, or areas you would like more clarification?

La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.

Gravedad de emergencia es determina por tecnología.

La definición de emergencia es diferente con cada persona.

Cada uno tiene la definición de vigilancia, pero ¿que tal la definición de emergencia?

SITUATIONS TO APPLY ITS USE

Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico

Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.

Los reportes no son anónimos.

Los datos son recolectados aun, a pesar de la opción escogida.

Alternatives to this technology

Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad

Entre Hermanos

City of Seattle
Surveillance

Inicio

Resumen: El departamento de vecindarios quiere saber la opinión de este grupo. Ellos verán videos de un minuto y medio y encontrarán folletos en sus mesas donde encontraran más información sobre lo visto.

Demográficos:

Ocho personas participaron, una de West Seattle, una de First Hill, dos de Ravenna/Laurelhurst y cuatro de King County (outside Seattle).

Cuatro personas se consideraron hispano o latino, una como india americana o nativa de Alaska, y tres no opinaron.

Cinco personas marcaron 18-44 como su rango de edad, dos marcaron 45-64 como el suyo y una no opinó.

Cinco personas marcaron masculino como género, una como transgénero, una como femenino, y otra no opinó.

Otra Información Importante:

- Preguntas serán hechas.
- Habrá una hoja para poder conversar sobre videos de interés
- Se les agradeció por venir.
- El concepto de vigilancia será manejado como la ciudad de Seattle lo maneja.
- Tom: Agradeció a los invitados por venir

Surveillance. In 2017 city council passed an ordinance to see what technology fit the definition of surveillance. The information gathered by these surveillance technologies are as follows: to “observe or analyze the movements, behaviors, or actions of identifiable individuals in a manner” which "is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.”

Presentador: Preguntó si la conversación en inglés fue entendida.

Grupo: Concordó.

Tom: Do not let information on videos stop you from making comments or raising questions.

Presentador: Dio a entender el concepto de vigilancia como ha sido interpretada por la ciudad de Seattle. Fue analizada de esta manera: “La vigilancia es definida como tecnologías que observan o analizan los movimientos, comportamientos, o acciones de individuales identificables de una manera que razonablemente levanta inquietudes sobre libertades civiles, la libertad de expresión o asociación, igualdad racial o justicia social.”

- Los movimientos de la gente son observados a través de esta tecnología y puede que para algunas personas esto sea incómodo.
- Las cámaras de policía no califican como tecnologías de vigilancia en este tema.
- La presentación mostrada en la pantalla a través de los videos será transmitida en inglés.
- Se pidió que todos se traten con respeto y que opinen y que su nombre sea mencionado e incluso la vecindad donde viven.

El Grupo

Participante vino porque quiere obtener más información y dar su opinión. Es de Seattle.

Participante viene de Shoreline/Seattle para ver cuánto la tecnología entra afecta

Participante vino porque quiere saber qué información es colectada por el gobierno y para qué usan esa información. Puede que la información obtenida a través de la tecnología sea usada para perseguir a personas de color/minorías/personas marginadas.

Participante vino de First Hill, porque quiere ver el punto de vista de la ciudad y ver que opiniones surgirán.

Participante viene de Seatac porque tiene interés en el tema y porque la seguridad es importante y quiere saber a dónde llega la información.

Participante vine en Ravenna/Northgate, quiere ver que tan confiable es la tecnología y para qué es utilizada. Perjudicial o beneficial?

Participante vine en Seatac y vino porque es un tema muy interesante ya que se tiene que saber/mantener informado de lo que hacen los gobernantes.

Participante vino de Burien por la importancia del tema y la privacidad.

Presentador: La tecnología no es nueva. Ya está siendo usada. Y quieren saber el formato para que las futuras tecnologías tengan.

El video de Seattle Department of Transportation de Acyclica fue mostrado

Esta tecnología es un sensor que detecta el wifi. Es un sensor que detecta la tecnología wifi.

Seattle Metering Tool fue mostrada

Nadie del grupo sabe del tema más el presentador no hablará a fondo de esto para no influenciar opiniones.

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

Aclaración: Información impresa fue entregada explicando cada una de las tecnologías.

Video de Coplogic fue mostrado

El grupo no conocía que se puede reportar a la policía a través de su página/en línea.

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

Se acordó el análisis de Acyclica, Binoculares/Sensorlink, y Coplogic

Las Preguntas que sea harán serán las siguientes:

> ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
> ¿Cuál creen que sea el aporte de esta tecnología a la cuidad?
> ¿Qué preocupación les causa el uso que se le dará a este sistema?
> ¿Qué recomendarían a el grupo de políticos de la cuidad responsables de tomar las decisiones de implementar estas tecnologías?
> ¿Qué otra manera habría de resolver el problema que esta tecnología esta designada a resolver?

La Acyclica

Pregunta: ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla? (Como se usa y cuál es el uso)

- Bien, la tecnología ayuda con la velocidad o el movimiento de los coches.
- La información se guarda y analizan por donde viajas o cuantas veces cruzas este rastreo.
- Si es solo para ver el tráfico está bien.
- Está bien en algunas partes. Puede que sea algo bueno. Pero puede que esta tecnología pueda compartir información personal que puede ser utilizada de otra forma en especial si hay Hacking (forma negativa, uso de datos).

- La tecnología en sí no es tan grande (de tamaño) para ser algo visualmente desagradable. La información captada a través de estos medios puede que ayude a conducir el tráfico de mejor manera pero también puede que tome información personal.

Pregunta: Qué es lo que aporta esta tecnología a la ciudad?

- Seria algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.

- Participante dice que hay alternativas para esquivar el tráfico.

- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.

- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

Pregunta: Qué preocupaciones tienen con posible uso/uso potencial de esta tecnología?

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.

- Si el potencial puede ser aplicada a la inversión.

Enfocando al grupo: La tecnología ya está instalada, que les preocupa de su uso?

- El tráfico sigue igual.

- Quien usa o almacena la información.

- La preocupación es la colección de data.

Más de la mitad de grupo opina que esa (el almacén y colección de información) es la preocupación.

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.

- El gobierno tiene todos los datos.

- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

La otra preocupación del grupo es que no haya un cambio al problema que se quiere resolver. En el caso de Acrylica sería el mejorar el tráfico.

- Tecnologías como esta necesitan recolectar más opiniones de expertos.

- Sería bueno que la información sea compartida con la comunidad. (Transparencia en fines y objetivos de la tecnología y datos guardados, tácticas implementadas.)

Pregunta: Le dirían algo a los políticos algo del lugar donde se encuentran estos aparatos?

- Hay lugares donde no se necesitan. En algunas partes de Magnolia, Queen Anne, Northgate, no se ocupan.

Seguimiento de pregunta: En las comunidades donde viven los latinos que tanto se ocupa Acyclica?

- Participante no cree que allí se ocupan.

Hablaron sobre la necesitad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

Presentrador: Crees que Acylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.

- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.

- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

Otra pregunta: Alguna otra tecnología que pueda ser utilizada en vez de Acyclica?

Alternativas:

- Alguna pantalla que indique cuáles vías son alternativas puede reemplazar esto.
- Cambios al límite de velocidad puede que alivie el flujo del tráfico.
- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.

- El rediseñar las vías servirá para las futuras generaciones.

Tecnologia #2

Sensorlink/Binoculares

Pregunta: Que opina el grupo de la tecnología?

- Los binoculares son preocupantes si la persona no tiene ética. Es preocupante que una persona vea a través de binoculares a que una tecnología mida el uso de la electricidad.
- Un sensor que detecta la electricidad sería mejor.
- Al grupo le incomoda el uso de binoculares.

Pregunta: Qué opinas sobre la tecnología medidora de electricidad (sensorlink) y que sea usada en tu casa?

- No le incomoda o afecta a dos participantes.
- La preocupación sería que le quita el trabajo a una persona.
- Los binoculares son invasivos.
- Para que usar binoculares si es que se puede llegar a el hogar y ver el medidor en persona, pidiendo permiso? Si la tecnología es usa para ver que las personas se roban la electricidad, creen que no saben quiénes roban?
- El grupo cree que si saben.

Pregunta: Cual creen que sea el aporte que esta tecnología?

- El video dice que 3 millones de dólares son ahorrados.

Pregunta: De qué manera beneficia esto a la cuidad/ciudadanos/comunidad?

- El robo de la luz es preocupante.
- Si ya llevan el record y datos y le hacen saber a la comunidad puede que ahorren dinero.
- Uso de binoculares puede dar trabajo a una persona y dinero puede ser ahorrado con esta tecnología.
- La tecnología trae gasto de electricidad para poder ver gastos de luz? Si pretende evitar el robo entonces los gastos de la factura eléctrica deberían de seguir estables.

Pregunta: La confianza en estos medidores serán confiables? Serán efectivos?

- Ayuda a la precisión, a bajar precios.
- Que quiten los binoculares sería una sugerencia, o usar binoculares que graban con video.
- Si ya tienen récord sobre la energía (consumo, gastos, etc.), el robo de energía no es suficiente para establecer este tipo de tecnología ya que puede ser identificado el robo o alguna otra anomalía dependiendo en el nivel alto o bajo o repentino analizado/visto/detectado por métodos convencionales ya establecidos.
- Otra recomendación: Usar background check, uso de uniforme por trabajadores, cámara en binoculares.
- Un tipo de escáner en los medidores de energía. Poner sensores en un poste de luz para grabar solo la data/información de electricidad
- .La preocupación es que no tan solo será para leer la electricidad sino para obtener otros tipos de información si cámaras fueran usadas.

Tecnologia #3 Coplogic

- Esta tecnología no solo el ahorro de tiempo, sino el ahorro de tiempo policial ya que ellos trabajarían en otras cosas
- El uso de computadora está bien para las denuncias.
- Si personas usan esta tecnología y es analizada en tiempo real por otras personas no hay problema.

Enfoque: Lo que estamos queriendo dialogar es el uso del internet y las denuncias.

- Es otro método para denunciar
- Está de acuerdo con el uso de computadoras para denunciar solo que no todos son capaz de usar este método/tecnología.

Pregunta: En que ayuda a la comunidad?

- Por qué usar estos métodos?
- Grupo están de acuerdo con su uso.
- Puede salvar una vida.

- Los riesgos y acciones determinan la urgencia de la intermisión policiaca.
- Alguna gente se siente más capaz de acudir a través de este sistema la tecnología en uso tiene validez.
- Bueno para la violencia doméstica.
- Las fallas electrónicas son preocupantes especialmente en reportes policiacos.
- Las preocupaciones es que el reporte no salió, no llegó por cualquier razón.
- No todos podrán o saben usar las computadoras.
- Fallas de los algoritmos o cuando o que promueve urgencia de cada demanda es alarmante.
- Criterio de demandas y que clase de preocupación de parámetros son confiables tienen que ser cuestionados/analizados, y que/quien es digno de prioridad o importancia o de ayuda.

Pregunta: De qué manera este uso beneficiaria a la comunidad?

- Personas pueden ser discriminadas
- Las personas le temen a los policías. Y este medio puede ayudar a que el miedo disminuya.
- La computadora decidirá la importancia/urgencia del reporte/emergencia dando a llevar acciones de emergencia.
- Gravedad de emergencia determina uso de tecnología.

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

- La elección automática de cada caso o la manera en que la persona escribió el reporte y la manera en que la computadora lo entendió es alarmante.

Pregunta: En qué situación usarán esta tecnología?

- Una pelea en la calle, un malestar corporal, cuestiones de vida, abuso doméstico
- Cada uno tiene la definición de vigilancia, pero que tal la definición de emergencia?
- La definición de emergencia es diferente con cada persona.
- Si nos basamos en la definición de emergencia sólo en cuanto estemos en peligro inmediato o en tiempos mínimos/ de transcurrencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro

Pregunta: Para qué sirve el reporte de la computadora?

- Para reportar algo que ya sucedió o que son recurrentes.
- Basado en el concepto de emergencia, las personas pueden tomar el método adecuado para reportar su caso y a través del medio necesario.
- Los reportes no son anónimos.
- Los datos son recolectados aun, a pesar de la opción escogida.

Pregunta: Qué les recomendarían a los políticos?

- Que sea multi-idioma, implementar audio, implementar sistemas que ayuden a múltiples personas con diversas capacidades/necesidades

Pregunta: Algún otro comentario en general sobre la tecnología de vigilancia?

- Si es usada de manera adecuada y como han dicho está bien.

- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

- Den información más información sobre lo que están haciendo. (transparencia/divulgación de información)

- Que haya más transparencia.

Ser transparentes sobre la colección de datos, para que haya discusiones y decisiones Informadas, en todas las tecnologías implementadas/por implementar.

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019

1:42 PM

Disclaimer: some of these notes are written in first-person. These should not be considered direct quotes

Videos:

- Acyclica: sensors recognize when a wifi enabled device is in range of it. Attached to street lights
- 911 recorder: records the conversation with the person calling 911, and conversation with the dispatched officers
- CopLogic: Online police report, treated as a regular policy report
- Computer Aided Dispatch
- Seattle City Light: Binoculars for meter readers; sensor to see if someone is stealing electricity

Tom: Read definition of surveillance

Craig: invasion of privacy?

- Electric one: I never even know they had the sensor one.

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology
Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

- Surveillance, I understand the concern, but overall I think it's a good thing. There is good and bad in any location, you'll find people who are taking advantage of it, but hopefully there are systems in place.
- Used to work nights, and catching the bus at night is scary. Having the cameras and police out when catching the bus helps, I appreciate that. No one likes to be watched, but if it's gonna keep people safe, that's a good thing.

Mercy: security is a great safety issue
Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone
Wanda: as long as it's even
Craig: Sometimes it's not even
Both: There are hot spots though

Which of the surveillance technologies do you think could be abused to pinpoint specific communities?

IG: The Computer Aided Dispatch

Talking about the International District:

- Lots of businesses and residential crammed together in a larger space
- Talking about a great community member who died; if they had surveillance technology them, maybe they would have found his killer

"Some neighborhoods need to be watched"

- Gangs; drug use

Tom: getting back to CAD, how do we feel about the information that is stored

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
  - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
  - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
  - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
  - Without my consent.

- Mercy: grew up with the idea that big brother is watching you
    - Tracking how many times I go to the library seems like a waste of money
    - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
    - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

Tom: So acyclica, is it worth it? Some people worried it's tracking, is it something that we can live without?

- Should we put up signs that this road is tracked?
    - Viron: Maybe
    - Mercy: let people out there know that you're on camera.
    - Viron: does it work if your device is not turned on?

Tom: what do you want to tell the city council about tech that is collecting personal information?

- Wanda: they should get our individual consent
- Martha: putting it on the ballot doesn't mean that you are getting individual consent, because if you vote no but it still passes, you didn't give your consent
- Deana: there are some places around Capitol Hill that I don't feel safe at at night
    - Talking about fire department responding to a fire in her building: when one building alarm system goes off, it goes directly to the fire department - affects multiple buildings.
        - Response time is very good.
    - I choose to turn off the GPS tracking, because I don't need people to know where I'm at
        - If others are watching where I'm at, that's an invasion of privacy. I should be able to walk out my front door and go wherever I want without anyone knowing.
- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

Mr. Surveillance: Surveillance is always secret, and it's an aggressive act. It's meant to exert power over others.

Do you think any individual could raise enough concern that it would change anything?

- Resounding no
- Maybe with a larger group
    - Maybe with the whole city

SCL binoculars:

- Craig: they should warn their customers and let them know they are coming into their yard/looking through binoculars.
- Wanda: as long as they aren't looking in people's windows.
    - When we're walking down the street, it's a little different. Certain neighborhoods do need more surveillance than others

Regarding being watched in public:

- Eydie: in public, it depends on how long. If it's a short period of time, that's one thing, but if you're tracked the whole time you're out, it's unreasonable.
    - I don't know what the solutions would be.
    - Even when the meter read just walks into your yard, it's unnerving.
    - What’s the purpose of tracking it this way?
- Mercy: (referring to the acyclica) Why are they doing it all the time? Have they not gotten the information yet?
    - They should already know what the traffic flow would be.
    - We lost a lane to the bicyclist
- Craig: facial recognition used on the street is bad.
- Vyron: sometimes you can't walk down the street and shake someone's hand without getting in trouble
- Mr. Surveillance: The technology has gotten ahead of the law, and it means they have to pay less people

Tom: Are we willing to accept more technology to have less police?

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
    - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.
    - I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
    - But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation
    - Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

Tom: If right now we have lots of technology, and we want a balance, then how do we do that?

- Craig: keep it the way it is but clean up the police department. Make sure the people who are working there are good at their jobs, not biased or discriminating

CopLogic: making police reports online

- Craig: I think it's stupid.
    - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
    - Anonymous reporting of crimes that could target people for things they might not call 911 for

- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
    - Police response when called: maybe you should get a cheaper type of car
    - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn't have to check it.
- Marjorie: I think the online reporting could be abused

Appendix E: All Comments Received from the Public

ID: 10617736557

Submitted Through: Survey Monkey

Date: 3/25/2019 1:49:17 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

There’s a lot of concerns about this technology. Highest Concerns: 1a) Acyclica/FLIR (FLIR acquired Acyclica late last year) is continuously tracking the movement and/or presence of all individuals with wifi-enabled devices within range of the sensors in Seattle. 1b) Keep in mind that the sensors will pick up the MAC addresses of ALL nearby individuals, including non-drivers/riders, such as pedestrians, bicyclists, and people in close structures (apartments/offices/churches/hospitals/etc). The draft SIR does not mention any specific additional privacy considerations that were applied to the technical implementation for these special classes of MAC addresses. 2) Acyclica’s technical implementation means that Acyclica most definitely has access to the original raw MAC addresses (contrary to the wording in the draft SIR). 3a) There doesn’t appear to be any contract between Acyclica/FLIR and SDOT, which means Acyclica/FLIR is not bound to any conditions by the City of Seattle regarding the handling or storage of this tracking data (either raw or aggregate). 3b) Page 14 item 7.2 says "Contractually, Acyclica guarantees that the data gathered is encrypted ..." If there is no contract, then “contractually” should be removed from the SIR. 4) Acyclica/FLIR should revise it’s implementation to no longer ever see or handle raw MAC addresses server-side. Alternatively, Acyclica/FLIR should be bound via contract with the City of Seattle to only ever store/retain encrypted unhashed MAC addresses or raw MAC addresses for at most 24 hours. 5) Because Acyclica/FLIR has access to raw MAC addresses, law enforcement agencies, such as ICE (among others) could issue warrants for this data from them. 6) Throughout the draft SIR, the descriptions of the technical implementation are inaccurate and incongruous. According to my conversation with an SDOT representative at the SIR tech fair (plus the letter SDOT provided there from the Acyclica president), my understanding is that the implementation consists of the sensors sniffing the MAC addresses and encrypting them using GPG software, which are then transmitted to the Acyclica servers, then the Acyclica servers decrypt the encrypted MAC addresses and take the raw MAC address add a salt and then hash them using SHA-256. These hashed MAC addresses are what’s available via the Acyclica APIs (in aggregate). If this is correct, then there are multiple parts of the SIR that are worded wrong: 6a) Page 6 item 2.3 says, "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." The sensors aren’t generating a hash (they’re encrypting the MAC address using GPG software) and Acyclica most definitely can access the original raw MAC addresses of the devices. 6b) Same as 6a but on page 8 item 4.2. 6c) On page 11 item 4.10 says "With Acyclica’s proprietary technology solutions, the salt rotates every 24 hours on the actual sensor device." There is no salting happening on the devices. If the “24 hours” aspect is correct, then this likely is supposed to say that Acyclica rotates the salt every 24 hours on their server-side. 6d) On page 12 item 5.3 says "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." This is confusing. Is Acyclica re-encrypting the hashed MAC addresses? I doubt this. I assume this meant to say that they use of a cryptographic hash function (SHA-256) to obscure the raw MAC address. [Keep in mind that any encryption can be reversed – that's the whole point of encryption (encryption+decryption). And depending on the hashing implementation, it could be easy to pre-compute a look-up table of MAC addresses with known hashes (this is known as a rainbow table). In both cases, this could enable identifying individuals.] 6e) Page 14 item 7.3 says "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." This appears to be the first and only time the SIR accurately describes the data flow (though GPG itself isn't proprietary to Acyclic/FLIR). 7) The SIR never specifies the encryption methodology being used, which is quite odd considering most companies of substance would want to broadly advertise and market their security claims, if they were indeed robust/modern security implementations. The letter from the Acyclica president says they're using GPG, but that's not specified in the SIR. Additionally GPG is just freely available software – it doesn't explain the encryption methodology being used, which should also be specified in the SIR. For example, if Acyclica is using asymmetric encryption with RSA keys, then that should be included in the SIR. Without this information, it's unclear if Acyclica is using a safe encryption scheme. 8) Lack of details regarding the security of salt used in the hashes. SDOT couldn't provide details of how the salt is generated. Depending on how the salt was generated, it wouldn't be that difficult to create a rainbow table for the hashed MAC addresses (thus making it is easy to determine what the raw MAC address was for a given hashed value from the Acyclica APIs). 9) The terms of the procurement order for Western Systems by SDOT is included in the SIR, but there doesn't appear to be a contract between Western Systems and SDOT. 10) There's also basic security questions I had that SDOT could not answer because Western Systems is the one deploying the sensors. For example, these sensors will have egress network access on TCP ports 80 and/or 443. Are there any network-level controls (firewall) that limits the sensors' egress access only to the Acyclica-owned endpoints? Are the sensors listening for any incoming connections on any ports? RoadTrend devices have a default password that is readily available in the public documentation ("temppwd"). Is that default password reset to a secure, non-default value for sensors deployed on behalf of SDOT? (The answers to all of these security questions is unknown since SDOT doesn't manage the devices. Moreover, if there is no contract with the City of Seattle binding the security/privacy expectations here, then Western Systems might not even be legally at fault if they are deploying these sensors in an incompetent manner.) 11) The draft SIR from SDOT doesn't specify why Acyclica is needed in addition to the License Plate Readers (LPRs) that were covered in Group 1, even though they appear to do the same thing (estimate travel times). 12a) The draft SIR doesn't specify what alternatives SDOT considered to Acyclica and why they were dismissed. 12b) Specifically SDOT does not describe why the privacy risk to all Seattle-area people is worth more than relying on traditional loop detectors, which wouldn't pose a privacy risk (assuming they only are installed at locations that consist of multiple dwellings/businesses/etc on that block). 13a) The data retention period is unclear. The SIR says 10 years in one place and 24 hours in another. Page 12 says "there is a 10 year internal deletion requirement per item#42 of the SDOT Public Retention Schedule & Destruction Authorization Schedule" and page 37 says "Additionally, the data is deleted within 24 hours to prevent tracking devices over time." 13b) Additionally, even if Acyclica is choosing to delete either the encrypted unhashed MAC addresses and/or the raw MAC addresses within 24 hours, that would purely be at their prerogative, since there is no binding contract between the City of Seattle and Acyclica/FLIR that requires they delete the data on that timeline. 14) Since FLIR has discontinued the Acyclica RoadTrend sensors (https://www.flir.com/support/products/roadtrend#Specifications), and because the SDOT SIR states “all new traffic signal cabinets will include Acyclica units as part of their standard build.”; presumably SDOT will seek to acquire and have deployed for them one of the many other FLIR sensors available. However, only the Acyclica RoadTrend sensor was in scope and described in this SIR, hence a future SIR should be submitted by SDOT if other sensors are planned to be deployed. Medium Concerns: 1) The letter from the Acyclica president that SDOT handed out at the SIR tech fair is not included in the draft SIR. 2) Since Acyclica has been bought by FLIR, FLIR may have changed the Acyclica technical implementation; and since there’s no contract, they are freely able to do so. (That being said, it would be more work to change the implementation, so they likely have kept the Acyclica implementation the same for now. Who knows about the future though.)

What value, if any, do you see in the use of this technology?

In it’s current state (both the lack of contracts and the technical implementation), I see the list of concerns heavily outweighing the pros for using this technology. The value this technology provides is not offset by the greater risk to privacy. Just use loop detectors.

What do you want City leadership to consider about the use of this technology?

1) There needs to be a contract between the City of Seattle and Acyclica/FLIR. 2) Said contract should specifically define MAC addresses as personal information (as is the case for boilerplate contracts from the City of Seattle). 3) Said contract should explicitly define the data handling of MAC addresses such that: 3a) Acyclica/FLIR changes their implementation to now longer see/handle raw MAC addresses server-side. 3b) Alternatively, Acyclica/FLIR is only allowed to retain/store/possess encrypted unhashed MAC addresses or raw unhashed MAC addresses for at most 24 hours. 3c) That SDOT/the City of Seattle owns this data, not Acyclica/FLIR. 4) City leadership should explicitly require that before any sensor other than the Acyclica RoadTrend is deployed on behalf of SDOT that SDOT first submit a SIR covering that new sensor model. (Note that FLIR has discontinued the Acyclica RoadTrend sensor and SDOT states that “all new traffic signal cabinets will include Acyclica units as part of their standard build.” so surely SDOT would need to use a different sensor in the future, which would not have gone through this review process. 5) IF ALL OF THE ABOVE ITEMS ARE NOT MET THEN: there should be a moratorium on the deployment of any additional sensors (including pre-existing RoadTrend sensors that SDOT has acquired but not yet deployed); and serious effort should be placed on the removal of this technology from Seattle; and transition to traditional loop detectors.

Do you have any other comments?

SDOT’s apparent lack of knowledge about the details of this technology seems to imply a lack of sufficient investigation and understanding on SDOT’s part regarding the privacy/civil liberties implications for deploying this technology. There does not appear to have been sufficient prior rigorous thought placed into this technology, especially given that there is a well-known alternative (loop detectors) that could be used that doesn’t pose these privacy/civil liberties risks.

Are there any questions you have, or areas you would like clarification?

ID: 10617434174

Submitted Through: Survey Monkey

Date: 3/25/2019 11:48:18 AM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

What value, if any, do you see in the use of this technology?

Helps resolve traffic flow problems

What do you want City leadership to consider about the use of this technology?

Start a program to license bikes and have a bike license RFID sticker so bikes can be included in this data.

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 10600654821

Submitted Through: Survey Monkey

Date: 3/18/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

I have serious concerns about how Acyclica anonymizes individual information. Stating that device IDs are "encrypted" gives no indication what is *actually* done with the data, nor what is legally permissible. Some specific issues: 1. "Encrypting" of device data is under-specified. Is this a 1-way hash? HMAC? Public-key encryption? Many of these options are _reversible_, which is a huge privacy concern. The City should be required to subject the technical details of this anonymization to public scrutiny.   2. Given information about a WiFi device, Acyclica will likely be able to identify all previous movements of the device simply by "encrypting" the device data again. This does not provide sufficient privacy.   3. If a device can be identified from its "encrypted" ID(s), it will be possible to see movements from an individual device over time. It will be incredibly easy to identify the individual using the device from this data. This does not provide sufficient privacy.   4. Even if the current system does protect individual data in a way that it can't be traced from day-to-day, there are no positive statements of privacy in this message guaranteeing that privacy will be respected in the future. The City should require a forward-looking, public privacy policy that fixes the above issues.

What value, if any, do you see in the use of this technology?

It is useful for transportation planners to be able to see aggregate, anonymous travel time information.

What do you want City leadership to consider about the use of this technology?

In using technology like this, I would like to see a public privacy policy that legally requires the City to randomly anonymize device data, in both a *temporal* and an *irreversible* sense. Storing identifiable information (e.g. to surveil a suspect) must be the exception, and must require a warrant to even start identifiable collection of such data.   This means that, from day to day, nobody should be able to use anonymized data to identify what routes an individual device took. It also means that, given a device, one cannot identify past routes it took.   It also should mean that, should the City fail to maintain privacy, it would be legally liable.

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 7

Submitted Through: Focus Group

Date: 2/28/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

use of personal devices to track people can target communities of color

What value, if any, do you see in the use of this technology?

traffic timing/info. Is really important and useful

What do you want City leadership to consider about the use of this technology?

to this point. Must have approval. Technology can be used to track device for lifetime? It would be important to know that the data can not be approved for continued use or different purpose.

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

What information from my phone is being transmitted? Is it only SDOT that gets the information?

ID: 1

Submitted Through: Public Meeting

Date: 2/27/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

My concern about this, as with all data about citizens collected by the city, is the potential for invasive abuse not intended at the time of collection.

What value, if any, do you see in the use of this technology?

The use stated in the information sheet about Acyclica seems reasonable.

What do you want City leadership to consider about the use of this technology?

It is imperative to safeguard our future that the City Council implement effective, INDEPENDENT, community oversight (not a rubber stamp for the agency doing the collecting.) This is necessary.

Do you have any other comments?

To make sure data is not sharted with federal or other agencies seeking to harass or intimidate citizens.

Are there any questions you have, or areas you would like clarification?

ID: 10562620750

Submitted Through: Survey Monkey

Date: 2/28/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

The type of tracking done by Acyclica should be banned and uses of this technology should be outlawed. In the case of Acyclica they may be taking appropriate measures to safeguard user data, but storing MAC addresses along with location data without explicit consent from users is a violation of civil rights. I certainly have not agreed for the city of Seattle or any vendors to track the position of my phone as it moves throughout the city whether or not that data is properly anonymized.

What value, if any, do you see in the use of this technology?

Having realtime traffic data is obviously important for the city and for citizens. However, that data must come with the explicit consent of the people generating the data. There are other ways to monitor traffic without invading the privacy of citizens.

What do you want City leadership to consider about the use of this technology?

City leadership should take a strong stand on civil liberties and privacy. The City leadership should ban all uses of Acyclica and similar technologies. Any technology of this nature should be on an explicit opt-in model, meaning that citizens of Seattle must give explicit consent to being tracked before any information is stored.

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 10550708265

Submitted Through: Survey Monkey

Date: 2/23/2019 12:06:47 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

This technology can be manipulated and the data can be sold to third parties the chances of attackers gaining access through hacking are high especially in the tech Advanced city of Seattle.

What value, if any, do you see in the use of this technology?

There are better ways to accurately communicate traffic flows without breaching people's privacy

What do you want City leadership to consider about the use of this technology?

The backlash of this is extremely dangerous especially in a growing technical world where data like this can be manipulated and also used to track and or identify specific groups of people in certain demographics. There are license plate reading Technologies that can also be used. When you take information from people's personal handheld cell phones or wifi-enabled devices what you are sending out is that data which then can be hacked and then could cause one of America's worst infiltration of people's privacy

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 10549573617

Submitted Through: Survey Monkey

Date: 2/22/2019 3:39:08 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

I have concerns over the data use and protection with this technology, specifically over what data is collected, how it is used/shared, and how long it is stored. Also, I personally am a pedestrian and often not in a car, so I have concerns over how the technology would distinguish my device when I am crossing streets.

What value, if any, do you see in the use of this technology?

Providing traffic information is useful, but I think the same result can be achieved another way

What do you want City leadership to consider about the use of this technology?

Data protection and usefulness of detecting wifi devices. Can we instead use other sensors that detect vehicles, rather than devices?

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 10535192314

Submitted Through: Survey Monkey

Date: 2/16/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

Accessing a person’s device and identifying a person/vehicle is tracking them even if it is encrypted to ‘anonymize’ the data. This concerns me.

What value, if any, do you see in the use of this technology?

Helping with the traffic flow is good, Using something that is not potentially a personal device to track the flow needs to be done, and can be done.

What do you want City leadership to consider about the use of this technology?

Changing the tracking technique to something less invasive.

Do you have any other comments?

Thank you for the opportunity to comment.

Are there any questions you have, or areas you would like clarification?

ID: 10534034636

Submitted Through: Survey Monkey

Date: 2/15/2019 6:25:29 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

Can encryption be disabled? You have misled folks - first claiming “ travel times” by tracking WiFi Mac addresses, then only explaining use at intersections. I suspect the tokens are persisted to allow calculations of travel times. What rules do you follow for timely destruction of encrypted tokens and when is such policy excepted?

What value, if any, do you see in the use of this technology?

Good info, if not abused.

What do you want City leadership to consider about the use of this technology?

Publish the truth and facts on encrypted token persistence and possible exposure\tracking of actual MAC addresses. It would be trivial to do so, if not being done already.

Do you have any other comments?

Are you tracking my IP? I suspect so. Maybe we need to all use VPNs. Gawd I hope not.

Are there any questions you have, or areas you would like clarification?

Please Publish the full truth.

ID: 10533818150

Submitted Through: Survey Monkey

Date: 2/15/2019 3:05:03 PM

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

I do not support this technology being used, especially since there is not similar data analysis that is multimodal in nature.

What value, if any, do you see in the use of this technology?

Nothing. It is not people first. It is focused on moving cars, likely at the expense of people.

What do you want City leadership to consider about the use of this technology?

Whether or not this technology is appropriate for dense urban settings that should prioritize people. I don't think it is.

Do you have any other comments?

Please stop using this technology. Instead develop a public policy framework that prioritizes moving people, not cars.

Are there any questions you have, or areas you would like clarification?

ID: 10530586898

Submitted Through: Survey Monkey

Date: 2/14/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

Where to start.... who made this decision? Why was it not put to public vote? Who is maintaining the data? What type of encryption is being used? Were is the transparency and ability to audit statements of data use and deletion? Why does SDOT think they are above City Ordinance 124142? This is not okay by any measure.

What value, if any, do you see in the use of this technology?

None. None whatsover. Governments are supposed to work FOR the people and the people never asked for this. This is an abuse of position, and overreach of authority, and a failure to protect the people of Seattle.

What do you want City leadership to consider about the use of this technology?

Making the public aware!! Increasing transparency and holding SDOT accountable for this egregious breach of public trust. In the best case abandoning the technology altogether. Seattle is slipping into an Orwellian cautionary tale.

Do you have any other comments?

I'm sickened at the state of our leadership in this city.

Are there any questions you have, or areas you would like clarification?

Was this ever put to public vote or opinion prior to spending millions over dollars over multiple years?

ID: 10514717375

Submitted Through: Survey Monkey

Date: 2/6/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

Hashed ("encrypted") MAC addresses do not fully anonymize users.

What value, if any, do you see in the use of this technology?

What do you want City leadership to consider about the use of this technology?

It is unacceptable to track MAC addresses, even in hashed ("encrypted") form.

Do you have any other comments?

Do not implement this technology. To the extent that this technology is already in place, remove it. It is an invasion of Seattle's privacy.

Are there any questions you have, or areas you would like clarification?

Why is this approval process being conducted retroactively? Why was the public not asked BEFORE the technology was built out?

ID: 10513975574

Submitted Through: Survey Monkey

Date: 2/6/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

They record personally identifiable information.

What value, if any, do you see in the use of this technology?

None that could be captured in a different way.

What do you want City leadership to consider about the use of this technology?

Do not use it.

Do you have any other comments?

Are there any questions you have, or areas you would like clarification?

ID: 10513975288

Submitted Through: Survey Monkey

Date: 2/6/2019

Which surveillance technology that is currently open for public comment, do you wish to comment on?

SDOT: Acyclica

What concerns, if any, do you have about the use of this technology?

Acyclica's report states that "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" (section 2.3), which is incorrect (hashed MAC addresses are susceptible to rainbow attack, and therefor deanonymizable). You can find more information about this topic here: https://en.wikipedia.org/wiki/MAC_address_anonymization#Why_this_does_not_work_in_practice

What value, if any, do you see in the use of this technology?

None.

What do you want City leadership to consider about the use of this technology?

The method used by Acyclica to anonymize personally identifiable information is faulty. Please contact some expert on this topic (i.e. cryptography and IT security) to understand the implications of this.

Do you have any other comments?

Privacy is important :)

Are there any questions you have, or areas you would like clarification?

Appendix F: Department Responses to Public Inquiries

The Departmental responses to questions posed are listed below. Referenced materials may be found in Appendix I.

1) For what specific purpose or purposes will Acyclica be used, and what policies state this?

   We have no specific policies guiding our use of Acyclica, but SDOT's intent is to use this data service to deliver travel time, delay, analytics and other traffic data.

   See Section 1.2 of the *Western Systems Purchase Order - Terms and MOU* which states in part:

   1.2. The City has tested the performance of this data service and is satisfied with the ability for this data service to deliver travel time, delay, analytics and other data and data services, as compared to the City's existing approaches to gathering and analyzing the same data.

2) Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?

   SDOT does not have a contract with Acyclica. SDOT established blanket contract #0000003493 (see attached) and a MOU with the *Western Systems Purchase Order - Terms and MOU* (see attached) with Western Systems Inc. to provide Acyclica's data and support as their local distributor.

3) Who owns the raw, non-aggregated data collected by Acyclica devices?

   SDOT owns the raw and aggregated data. See the attached letter *SDOT Acyclica Data Ownership* which clarifies that.

4) What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?

Acyclica / FLIR does not have a limit on data retention. The reason for this policy is that as they develop new methods of analyzing traffic, the analyses are effective as of the date the sensors were first deployed rather than when the feature was first available in the software.

SDOT does have a 10-year retention policy for travel times per item #42 in the attached SDOT Records Retention Schedule, but "Traffic Study Reports" are also designated as Potentially Archival.

5) Provide accurate descriptions of Acyclica's data security practices including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.

Acyclica / FLIR employs both salting, hashing and encryption. The MAC addresses are salted with a key prior to hashing which rotates every 24-hours to eliminate the ability to track an individual from day-to-day. Prior to being transmitted from the sensor in the field to the cloud, the data is encrypted end-to-end using TLS and a 2048-bit encryption certificate and a nominal strength of 256 bits. Acyclica / FLIR utilizes a cryptographic hash function to generate a one-way, fixed size 256-bit hash.

Also refer to section 2.5.1 of the *Western Systems Purchase Order - Terms and MOU* which states, "It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City 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."

6) What third parties will access Acyclica's data, for what purpose, and under what conditions?

Acyclica has given the ability for cities to manage their own users and additionally taken steps to eliminate data sharing unless the owning city has given explicit authorization. Existing users of SDOT's aggregated travel time data include:

1. **SDOT staff conducting engineering studies**
2. **WSDOT and KC Metro staff conducting engineering studies in partnership with SDOT**
3. **Consulting partners who build traffic products on SDOT's behalf**

7) Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?

The sensors without locations either used to be in the field but were replaced at some point or are awaiting initial deployment (53). SDOT does not have a timetable to install those units.

8) Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?

Since the RoadTrend product line was discontinued, we've begun procuring the EDI DA-300 (please see attached data sheet) in its place. The EDI DA-300 will be the model we consistently deploy in the foreseeable future, and there are no plans to consider an alternative at this point. The unit has additional features differentiating it from the RoadTrend such as generating alarms when a traffic cabinet door is opened, and the ability to provide remote access to traffic signals using cellular communication.

9) Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US Department of Transportation)

Please refer to the attachment *Acyclica Travel Time Accuracy & Reliability Analysis.* This report summarizes the comparison of travel time data received from both License Plate Reader Cameras (our standard technology then) and Acyclica units along the same corridor during a 2014 study period. Due to the cost effectiveness and accuracy of travel time information provided by Acyclica, SDOT discontinued the procurement of additional License Plate Reader Cameras and transitioned into contract with Western Systems to receive that data as a service.

Inductive loops are commonly used on freeways to estimate spot (point location) speeds and travel times. To accomplish this, two loops are placed at a fixed distance from one another, forming a speed "station". Attempts to use inductive loops similarly to gather arterial travel times in urban conditions have not proven successful due to the influence of traffic signals and other measures intentionally implemented to slow or stop traffic.

10) How does SDOT plan to reduce the privacy infringements on nondrivers/riders?

Please see the attachment *Seattle Security Assurance Request*. It is a copy of the letter sent to Daniel Benhammou (Acyclica CEO) on 4/20/2015.

In response, Acyclica hired Coalfire System, Inc. to independently audit their security practices. The results of that report state that, "Coalfire was able to confirm the operation effectiveness of Acyclica's device and systems design such that there is no PII retained in any data repository, nor is the non PII MAC address ever presented to customer/clients in an unencrypted, unhashed format. Design effectiveness was confirmed with review, observation and interviews of configuration and code implementation with administrative personnel. Documented processes were also validated as effectively designed and operational as demonstrated by supporting evidence assessed during review of data repositories and device and system configurations."

Acyclica also made changes in response to the three points identified in the memo. These specifically are as follows:

City of Seattle Request #1: Enhance their key management program to reduce the risk that the exposure of a single key would compromise all of their customer data.

Acyclica Response #1: Key management has been enhanced such that every sensor has a unique which can be reset remotely so that should a device be compromised, the key can only be used to access the individual sensor unless it has been invalidated.

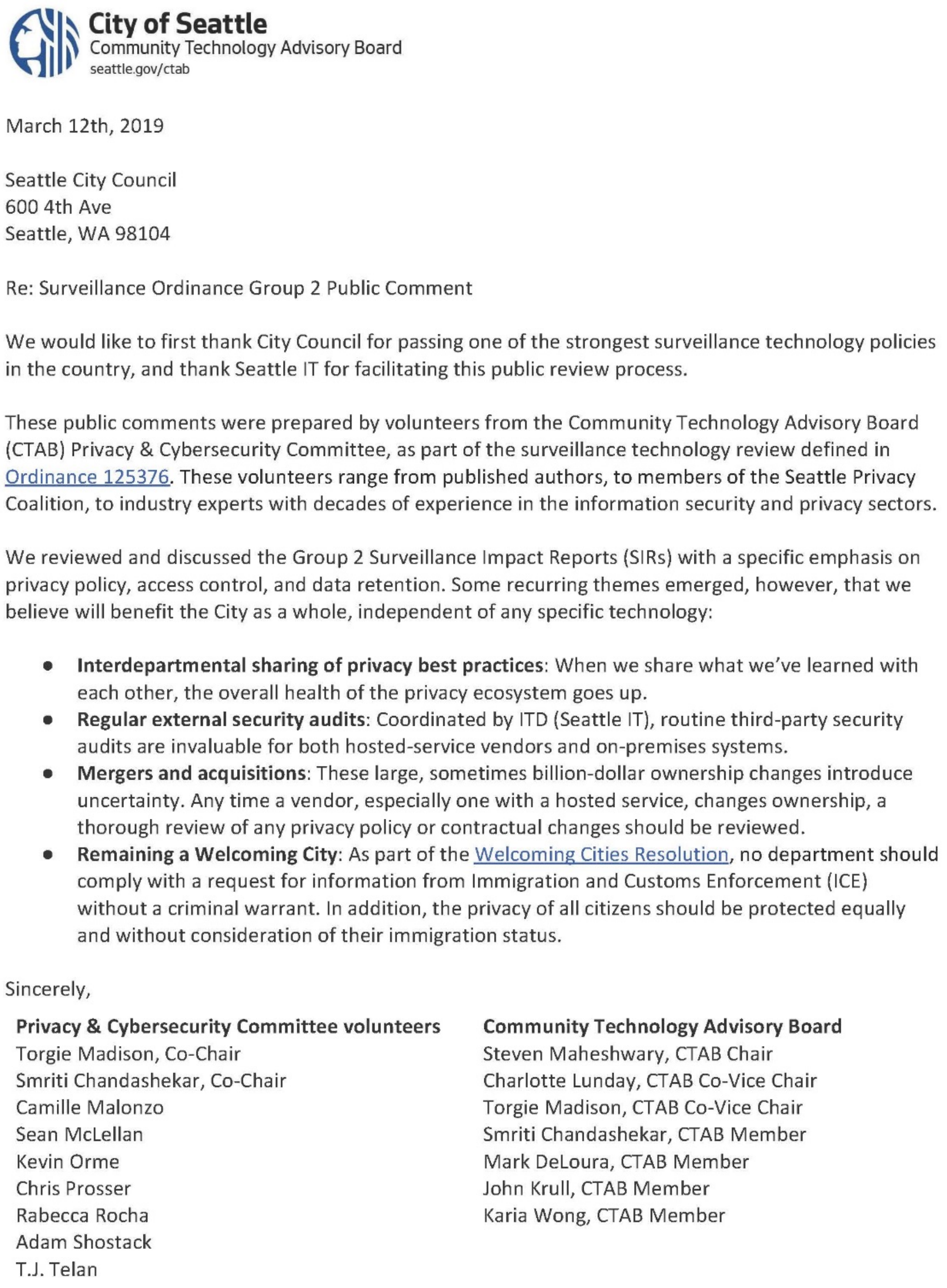
City of Seattle Request #2: Delete detail-level data after a period of time (e.g. 90 days). Aggregated data can be maintained to understand traffic patterns and historical information. Detail-level data likely has minimal value especially as hashing methodologies are changed daily, when prevents the comparison of detailed records across days.

Acyclica Response #2: Acyclica has removed access to all detail-level data from all APIs and software interfaces so that it can only be used for the development of new features. All detail-level data has been encrypted for storage to protect the privacy of such data and access to the encryption keys is limited to several specific individuals.

City of Seattle Request #3: Do not share a city's data without express permission from the owning city.

Acyclica Response #3: Acyclica has given the ability for cities to manage their own users and additionally taken steps to eliminate data sharing unless the owning city has given explicit authorization.

Appendix G: Letters from Organizations or Commissions



City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

March 12th, 2019

Seattle City Council
600 4th Ave
Seattle, WA 98104

Re: Surveillance Ordinance Group 2 Public Comment

We would like to first thank City Council for passing one of the strongest surveillance technology policies in the country, and thank Seattle IT for facilitating this public review process.

These public comments were prepared by volunteers from the Community Technology Advisory Board (CTAB) Privacy & Cybersecurity Committee, as part of the surveillance technology review defined in Ordinance 125376. These volunteers range from published authors, to members of the Seattle Privacy Coalition, to industry experts with decades of experience in the information security and privacy sectors.

We reviewed and discussed the Group 2 Surveillance Impact Reports (SIRs) with a specific emphasis on privacy policy, access control, and data retention. Some recurring themes emerged, however, that we believe will benefit the City as a whole, independent of any specific technology:

- **Interdepartmental sharing of privacy best practices**: When we share what we've learned with each other, the overall health of the privacy ecosystem goes up.
- **Regular external security audits**: Coordinated by ITD (Seattle IT), routine third-party security audits are invaluable for both hosted-service vendors and on-premises systems.
- **Mergers and acquisitions**: These large, sometimes billion-dollar ownership changes introduce uncertainty. Any time a vendor, especially one with a hosted service, changes ownership, a thorough review of any privacy policy or contractual changes should be reviewed.
- **Remaining a Welcoming City**: As part of the Welcoming Cities Resolution, no department should comply with a request for information from Immigration and Customs Enforcement (ICE) without a criminal warrant. In addition, the privacy of all citizens should be protected equally and without consideration of their immigration status.

Sincerely,

Privacy & Cybersecurity Committee volunteers
Torgie Madison, Co-Chair
Smriti Chandashekar, Co-Chair
Camille Malonzo
Sean McLellan
Kevin Orme
Chris Prosser
Rabecca Rocha
Adam Shostack
T.J. Telan

Community Technology Advisory Board
Steven Maheshwary, CTAB Chair
Charlotte Lunday, CTAB Co-Vice Chair
Torgie Madison, CTAB Co-Vice Chair
Smriti Chandashekar, CTAB Member
Mark DeLoura, CTAB Member
John Krull, CTAB Member
Karia Wong, CTAB Member

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SFD: Computer-Aided Dispatch (CAD)

Comments

The use of a centralized Computer-Aided Dispatch (CAD) system is essential to protecting the health and safety for all Seattle citizens. The National Fire Protection Association (NFPA) standards outline specific alarm answering, turnout, and arrival times[1] that could only be accomplished in a city of this size with a CAD system.

In addition, with over 96,000 SFD responses per year (2017)[2], only a computerized system could meet the state's response reporting guidelines established in RCW 35A.92.030[3].

CentralSquare provides the dispatch service used by SFD. CentralSquare is a new entity resulting from the merger of Superion, TriTech, Zuercher, and Aptean[4] in September 2018.

Recommendations

- Tritech, the underlying technology supplying SFD with CAD services, has been in use since 2003 [SIR 4.3], making it 16 years old. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, we recommend conducting a survey into the plausibility of replacing Tritech as SFD's CAD solution.

- Tritech was merged very recently into CentralSquare in one of the largest-ever government technology mergers to date. Due diligence should be exercised to ensure that this vendor is keeping up to date with industry best practices for security and data protection, and that their privacy policies are still satisfactory after the CentralSquare merger. We recommend ensuring that the original contracts and privacy policies have remained unchanged as a result of this merger.

[1] "NFPA Standard 1710." https://services.prod.iaff.org/ContentFile/Get/30541

[2] "2017 annual report - Seattle.gov." https://www.seattle.gov/Documents/Departments/Fire/FINAL%20Annual%20Report_2017.pdf

[3] "RCW 35A.92.030: Policy statement—Service ... - Access WA.gov." https://app.leg.wa.gov/rcw/default.aspx?cite=35A.92.030

[4] "Superion, TriTech, Zuercher, and Aptean's Public Sector Business to " 5 Sep. 2018, https://www.tritech.com/news/superion-tritech-zuercher-and-apteans-public-sector-business-to-form-centra

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SDOT: Acyclica

Comments

Traffic congestion is an increasingly major issue for our city. Seattle is the fastest-growing major city in the US this decade, at 18.7% growth, or 114,00 new residents[5]. Seattle ranks sixth in the nation for traffic congestion[6]. The need for intelligent traffic shaping and development has never been greater. Acyclica, a service provided by Western Systems and now owned by FLIR[7], is an implementation of surveillance technology specifically designed to address this problem.

We were happy to see the 2015 independent audit of Acyclica's systems [SIR 8.2]. This is an excellent industry best practice, and one that we'll be recommending to other departments throughout this document.

In addition, we are pleased to see the hashing function's salt value rotated every 24-hours [SIR 4.10]. This ensures that even the 10-year retention policy [SIR 5.2] cannot be abused to correlate multiple commute sessions and individually identify a person.

Recommendations

- FLIR Systems' acquisition of Acyclica is a recent development (September 2018). We recommend verifying that the Western Systems terms [SIR 3.1] still apply. If they have been superseded by new terms from FLIR Systems, those should be subject to an audit by SDOT and Seattle IT. Specifically, section 2.5.1 of Western Systems' terms must still apply:

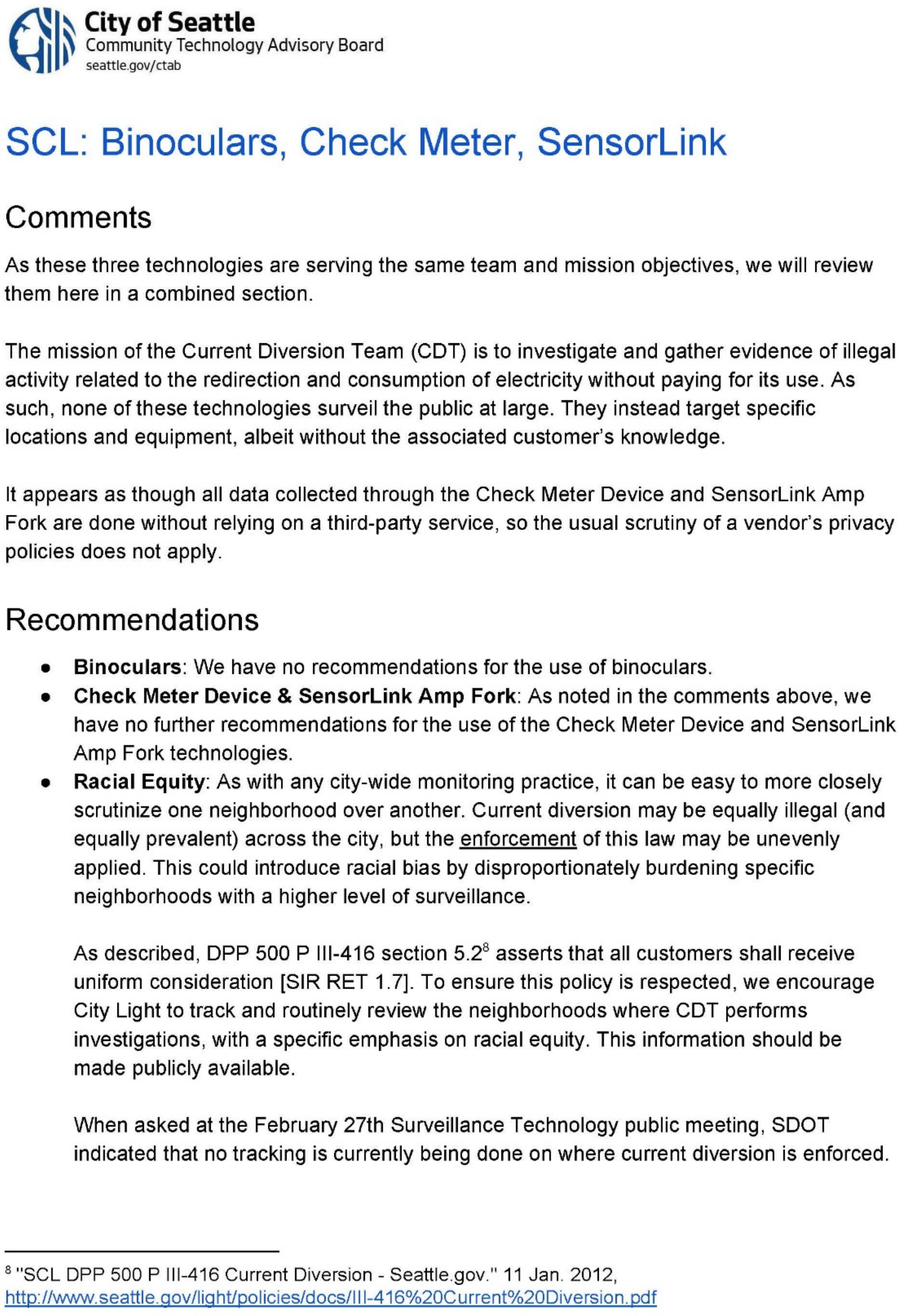
  > 2.5.1. It is the understanding of the City that the data gathered are encrypted to fully eliminate the possibility of identifying individuals or vehicles. In no event shall City or Western Systems and its subcontractors make any use of the data gathered by the devices for any purpose that would identify the individuals or vehicles included in the data.

- FLIR Systems is known primarily as an infrared technology vendor. Special care should be taken if FLIR/Acyclica attempt to couple IR scanning with WiFi/MAC sniffing. Implementation of an IR system would necessitate a new public surveillance review.

[5] "114,000 more people: Seattle now decade's fastest-growing big city in ...." 24 May. 2018, https://www.seattletimes.com/seattle-news/data/114000-more-people-seattle-now-this-decades-fastest-growing-big-city-in-all-of-united-states/

[6] "INRIX Global Traffic Scorecard." http://inrix.com/scorecard/

[7] "FLIR Systems Acquires Acyclica | FLIR Systems, Inc.." 11 Sep. 2018, http://investors.flir.com/news-releases/news-release-details/flir-systems-acquires-acyclica



City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SCL: Binoculars, Check Meter, SensorLink

Comments

As these three technologies are serving the same team and mission objectives, we will review them here in a combined section.

The mission of the Current Diversion Team (CDT) is to investigate and gather evidence of illegal activity related to the redirection and consumption of electricity without paying for its use. As such, none of these technologies surveil the public at large. They instead target specific locations and equipment, albeit without the associated customer's knowledge.

It appears as though all data collected through the Check Meter Device and SensorLink Amp Fork are done without relying on a third-party service, so the usual scrutiny of a vendor's privacy policies does not apply.

Recommendations

- **Binoculars**: We have no recommendations for the use of binoculars.
- **Check Meter Device & SensorLink Amp Fork**: As noted in the comments above, we have no further recommendations for the use of the Check Meter Device and SensorLink Amp Fork technologies.
- **Racial Equity**: As with any city-wide monitoring practice, it can be easy to more closely scrutinize one neighborhood over another. Current diversion may be equally illegal (and equally prevalent) across the city, but the enforcement of this law may be unevenly applied. This could introduce racial bias by disproportionately burdening specific neighborhoods with a higher level of surveillance.

  As described, DPP 500 P III-416 section 5.2[8] asserts that all customers shall receive uniform consideration [SIR RET 1.7]. To ensure this policy is respected, we encourage City Light to track and routinely review the neighborhoods where CDT performs investigations, with a specific emphasis on racial equity. This information should be made publicly available.

  When asked at the February 27th Surveillance Technology public meeting, SDOT indicated that no tracking is currently being done on where current diversion is enforced.

[8] "SCL DPP 500 P III-416 Current Diversion - Seattle.gov." 11 Jan. 2012, http://www.seattle.gov/light/policies/docs/III-416%20Current%20Diversion.pdf

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: 911 Logging Recorder

Comments

This is a technology that the general public would likely already assume is in place. Some of the more sensational 911 call logs have been, for example, played routinely on the news around the country. Since it would not alarm the public to know that 911 call recording is taking place, our recommendations will focus primarily on data use, retention, and access control.

Call logging services are provided by NICE Ltd., an Israeli company founded in 1986. This vendor has had a troubling history with data breaches. For example, a severe vulnerability discovered in 2014 allowed unauthorized users full access to a NICE customer's databases and audio recordings[9]. Again, in 2017, a NICE-owned server was set up with public permissions, exposing phone numbers, names, and PINs of 6 million Verizon customers[10].

Recommendations

- SIR Appendix K includes a CJIS audit performed in 2017. SIR section 4.10 also mentions that ITD (Seattle IT) periodically performs routine monitoring of the SPD systems.

  However, given the problematic history with the quality of the technology vendor, if any of the NICE servers, networks, or applications were installed by the vendor (or installation was overseen/advised by the vendor), we recommend an external audit of the implementation of the call logging technology.

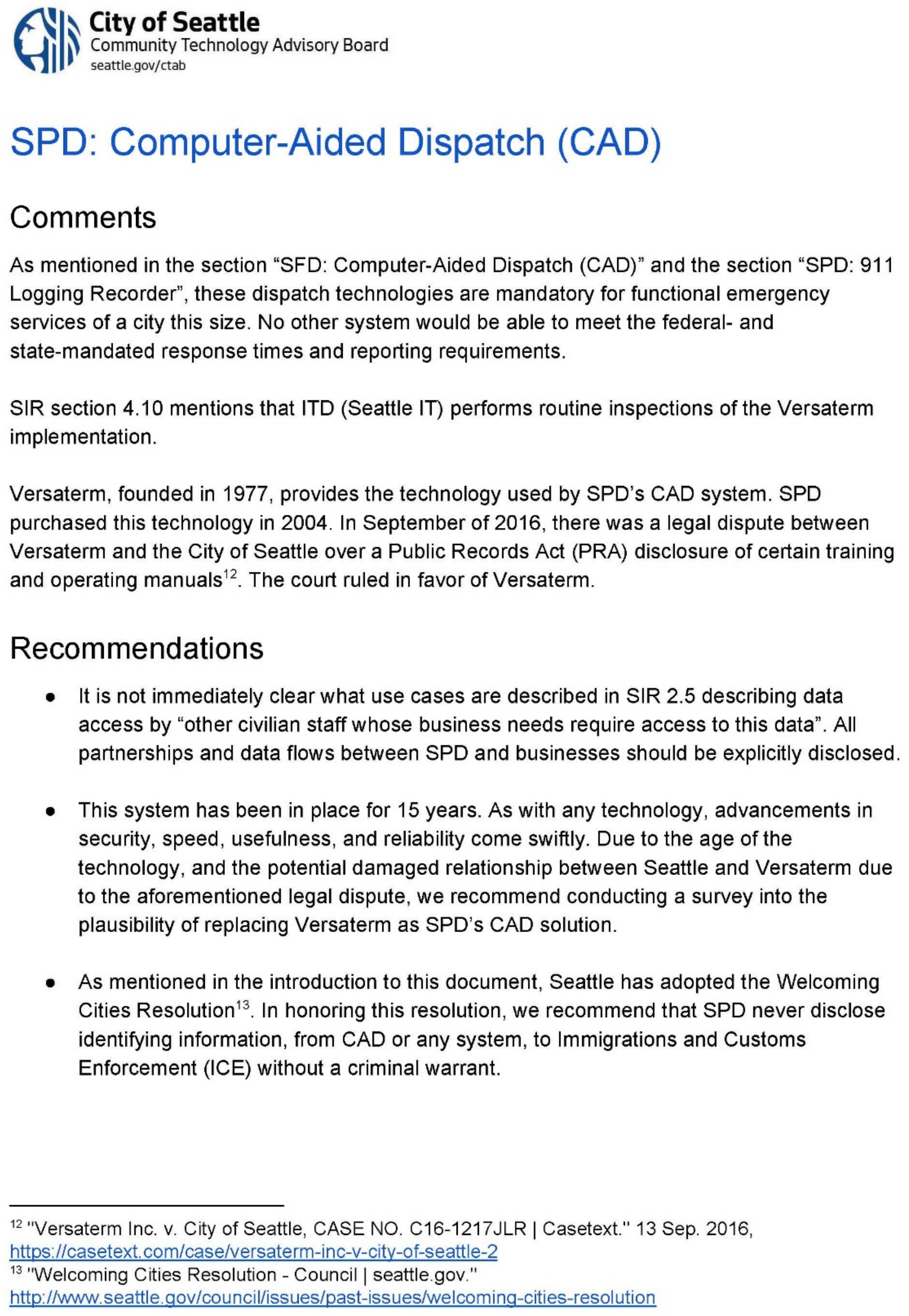
- SIR sections 3.3 and 4.2 outline the SPD-mandated access control and data retention policies, however it is not apparent if there is a policy that strictly locks down the use of this technology to a well-defined list of allowed cases. We recommend formally documenting the allowed 911 Logging use cases, and creating a new SIR for any new desired applications of this technology.

  With a 90-day retention policy [SIR 4.2], and with SPD receiving 900,000 calls per year[11], there are about 220,000 audio recordings existing at any given time. This is enough for a data mining, machine learning, or voice recognition project.

[9] "Backdoor in Call Monitoring, Surveillance Gear — Krebs on Security." 28 May. 2014, https://krebsonsecurity.com/2014/05/backdoor-in-call-monitoring-surveillance-gear/

[10] "Nice Systems exposes 14 million Verizon customers on open AWS ...." 12 Jul. 2017, https://www.techspot.com/news/70106-nice-systems-exposes-14-million-verizon-customers-open.html

[11] "9-1-1 Center - Police | seattle.gov." https://www.seattle.gov/police/about-us/about-policing/9-1-1-center



City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: Computer-Aided Dispatch (CAD)

Comments

As mentioned in the section “SFD: Computer-Aided Dispatch (CAD)” and the section “SPD: 911 Logging Recorder”, these dispatch technologies are mandatory for functional emergency services of a city this size. No other system would be able to meet the federal- and state-mandated response times and reporting requirements.

SIR section 4.10 mentions that ITD (Seattle IT) performs routine inspections of the Versaterm implementation.

Versaterm, founded in 1977, provides the technology used by SPD’s CAD system. SPD purchased this technology in 2004. In September of 2016, there was a legal dispute between Versaterm and the City of Seattle over a Public Records Act (PRA) disclosure of certain training and operating manuals[12]. The court ruled in favor of Versaterm.

Recommendations

- It is not immediately clear what use cases are described in SIR 2.5 describing data access by “other civilian staff whose business needs require access to this data”. All partnerships and data flows between SPD and businesses should be explicitly disclosed.
- This system has been in place for 15 years. As with any technology, advancements in security, speed, usefulness, and reliability come swiftly. Due to the age of the technology, and the potential damaged relationship between Seattle and Versaterm due to the aforementioned legal dispute, we recommend conducting a survey into the plausibility of replacing Versaterm as SPD’s CAD solution.
- As mentioned in the introduction to this document, Seattle has adopted the Welcoming Cities Resolution[13]. In honoring this resolution, we recommend that SPD never disclose identifying information, from CAD or any system, to Immigrations and Customs Enforcement (ICE) without a criminal warrant.

[12] "Versaterm Inc. v. City of Seattle, CASE NO. C16-1217JLR | Casetext." 13 Sep. 2016, https://casetext.com/case/versaterm-inc-v-city-of-seattle-2

[13] "Welcoming Cities Resolution - Council | seattle.gov." http://www.seattle.gov/council/issues/past-issues/welcoming-cities-resolution

City of Seattle
Community Technology Advisory Board
seattle.gov/ctab

SPD: CopLogic

Comments

Track 1 - Public reporting of no-suspect, no-evidence, non-emergency crimes

CTAB understands that in cases where no evidence or suspect is available, a crime should be reported (for statistical or insurance purposes) but does not require the physical appearance of an SPD officer.

Track 2 - Retail Loss Prevention

This track is more problematic, as it could be used by retailers as a method to unreasonably detain, intimidate, or invade the privacy of a member of the public accused of, but not proven guilty of, shoplifting.

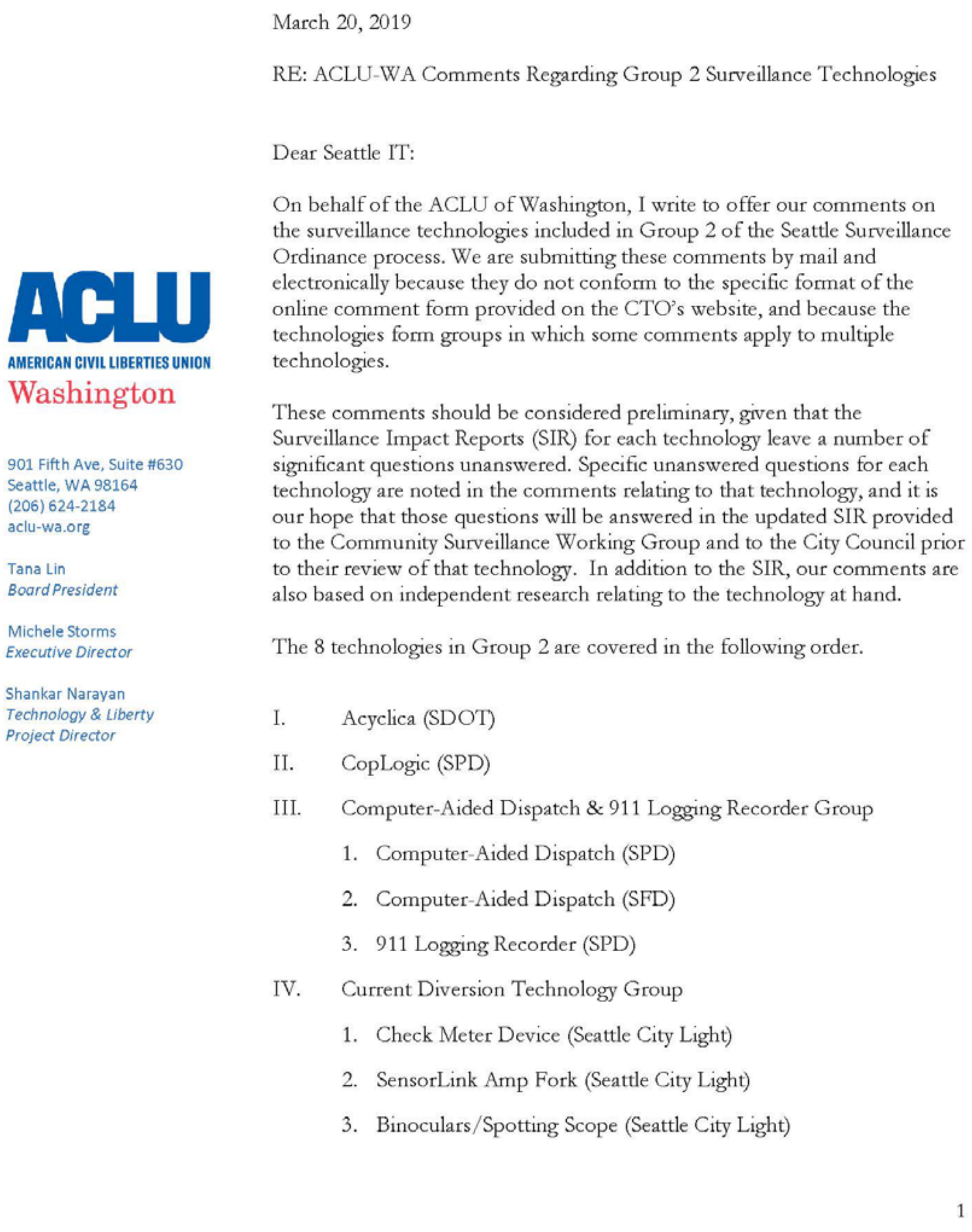
Recommendations

- **Track 2**: If not already done, retailers should be trained and informed that having a CopLogic login does not allow them to act as if they are law enforcement officers. Members of the public suspected of shoplifting need to have an accurate description of their rights in order to make informed decisions before providing identifying information. Retailers are also held to a lower standard than SPD regarding racial bias. It is virtually guaranteed that people of color are disproportionately apprehended and entered into the retail track of CopLogic.

  We recommend discontinuing Track 2 entirely.

- **Track 1 & 2**: If not already done, SPD, in coordination with Seattle IT, should perform or hire a company to perform an audit of the vendor's systems. If this audit has not been performed in the 8 years since purchasing this system, it should absolutely be done before the 10-year mark in 2020.
- **Track 1 & 2**: It is not immediately clear in the SIR or LexisNexis's Privacy Policy what CopLogic does with these records long-term, after SPD has imported them into their on-premises system. A written statement from LexisNexis on how this data is used, mined, or sold to affiliates/partners should be acquired by SPD.
- **Track 1 & 2**: We recommend migrating CopLogic to an on-premises solution. We found the LexisNexis privacy policy to be obfuscated and vague[14]. Such sensitive information should not be protected by trust alone.

[14] "Privacy Policy | LexisNexis." 7 May. 2018, https://www.lexisnexis.com/en-us/terms/privacy-policy.page



AMERICAN CIVIL LIBERTIES UNION
Washington

901 Fifth Ave, Suite #630
Seattle, WA 98164
(206) 624-2184
aclu-wa.org

Tana Lin
Board President

Michele Storms
Executive Director

Shankar Narayan
Technology & Liberty Project Director

March 20, 2019

RE: ACLU-WA Comments Regarding Group 2 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer our comments on the surveillance technologies included in Group 2 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail and electronically because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the Community Surveillance Working Group and to the City Council prior to their review of that technology. In addition to the SIR, our comments are also based on independent research relating to the technology at hand.

The 8 technologies in Group 2 are covered in the following order.

I. Acyclica (SDOT)

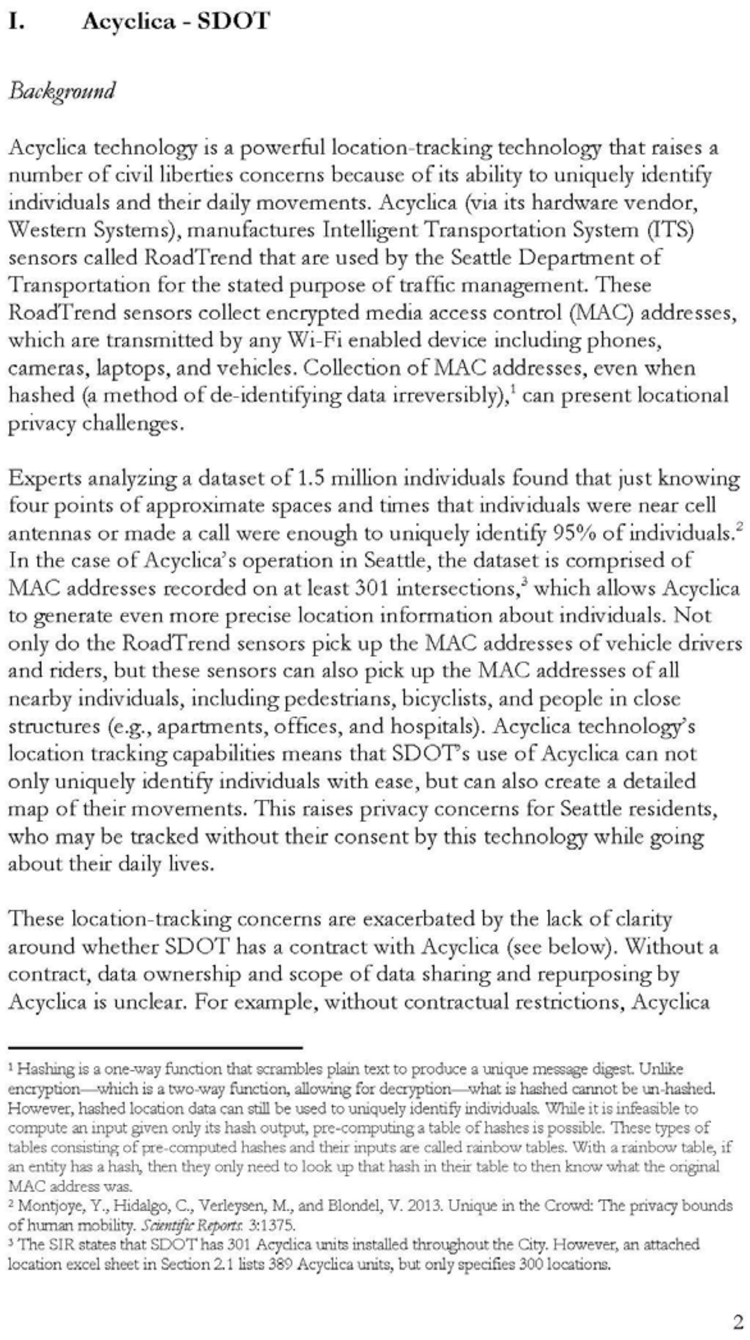
II. CopLogic (SPD)

III. Computer-Aided Dispatch & 911 Logging Recorder Group

1. Computer-Aided Dispatch (SPD)
2. Computer-Aided Dispatch (SFD)
3. 911 Logging Recorder (SPD)

IV. Current Diversion Technology Group

1. Check Meter Device (Seattle City Light)
2. SensorLink Amp Fork (Seattle City Light)
3. Binoculars/Spotting Scope (Seattle City Light)



I. Acyclica - SDOT

Background

Acyclica technology is a powerful location-tracking technology that raises a number of civil liberties concerns because of its ability to uniquely identify individuals and their daily movements. Acyclica (via its hardware vendor, Western Systems), manufactures Intelligent Transportation System (ITS) sensors called RoadTrend that are used by the Seattle Department of Transportation for the stated purpose of traffic management. These RoadTrend sensors collect encrypted media access control (MAC) addresses, which are transmitted by any Wi-Fi enabled device including phones, cameras, laptops, and vehicles. Collection of MAC addresses, even when hashed (a method of de-identifying data irreversibly),[1] can present locational privacy challenges.

Experts analyzing a dataset of 1.5 million individuals found that just knowing four points of approximate spaces and times that individuals were near cell antennas or made a call were enough to uniquely identify 95% of individuals.[2] In the case of Acyclica's operation in Seattle, the dataset is comprised of MAC addresses recorded on at least 301 intersections,[3] which allows Acyclica to generate even more precise location information about individuals. Not only do the RoadTrend sensors pick up the MAC addresses of vehicle drivers and riders, but these sensors can also pick up the MAC addresses of all nearby individuals, including pedestrians, bicyclists, and people in close structures (e.g., apartments, offices, and hospitals). Acyclica technology's location tracking capabilities means that SDOT's use of Acyclica can not only uniquely identify individuals with ease, but can also create a detailed map of their movements. This raises privacy concerns for Seattle residents, who may be tracked without their consent by this technology while going about their daily lives.

These location-tracking concerns are exacerbated by the lack of clarity around whether SDOT has a contract with Acyclica (see below). Without a contract, data ownership and scope of data sharing and repurposing by Acyclica is unclear. For example, without contractual restrictions, Acyclica

[1] Hashing is a one-way function that scrambles plain text to produce a unique message digest. Unlike encryption—which is a two-way function, allowing for decryption—what is hashed cannot be un-hashed. However, hashed location data can still be used to uniquely identify individuals. While it is infeasible to compute an input given only its hash output, pre-computing a table of hashes is possible. These types of tables consisting of pre-computed hashes and their inputs are called rainbow tables. With a rainbow table, if an entity has a hash, then they only need to look up that hash in their table to then know what the original MAC address was.

[2] Montjoye, Y., Hidalgo, C., Verleysen, M., and Blondel, V. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports.* 3:1375.

[3] The SIR states that SDOT has 301 Acyclica units installed throughout the City. However, an attached location excel sheet in Section 2.1 lists 389 Acyclica units, but only specifies 300 locations.

would be able to share the raw data (i.e., the non-aggregated, hashed data before it is summarized and sent to SDOT) with any third parties, and these third parties would be able to use the data in any way they see fit, including combining the data with additional data such as license plate reader or facial recognition data. Acyclica could also share the data with law enforcement agencies that may repurpose the data, as has happened with other City data. For example, in 2018, U.S. Immigration and Customs Enforcement (ICE) approached Seattle City Light with an administrative subpoena demanding information on a particular customer location, including phone numbers and information on related accounts.[4] ICE also now has agency-wide access to a nationwide network of license plate readers controlled by Vigilant Solutions,[5] indicating the agency may seek additional location data for immigration enforcement purposes in the future. Data collected via Acyclica should never be used for law enforcement purposes.

The uncertainty around the presence or absence of a contract contributes to two key issues: (1) lack of a clearly defined purpose of use of Acyclica technology; and (2) lack of clear restrictions on the use of Acyclica technology that track that purpose. With no contract, SDOT cannot enforce policies restricting the use of Acyclica technology to the intended purpose.

There are also a number of contradictory statements in the SIR concerning the operation of Acyclica technology,[6] as well as discrepancies between the SIR, the information shared at the technology fair (the first public meeting to discuss the Group 2 technologies),[7] and ACLU-WA's conversation with the President of Acyclica, Daniel Benhammou. All these leave us with concerns over whether SDOT fully understands (and the SIR reflects) the capabilities of the technology. In addition, there remain a number of critical unanswered questions that the final SIR must address (set forth below).

Of additional concern is the recent acquisition of Acyclica by FLIR Systems, an infrared and thermal imaging company funded by the U.S. Department of Defense.[8] As of March 2019, FLIR has discontinued Acyclica RoadTrend sensors.[9] Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR—but if the sensors used will change, the SIR should make clear how that will impact the technology.

a. *Specific Concerns*

- *Inadequate Policies Defining Purpose of Use.* Policies cited in the SIR are vague,

[4] https://crosscut.com/2018/02/immigration-officials-subpoena-city-light-customer-info

[5] https://www.theverge.com/2018/3/1/17067188/ice-license-plate-data-california-vigilant-solutions-alpr-sanctuary

[6] Explained in further detail in 1. Acyclica – SDOT *Major Concerns* below.

[7] http://www.seattle.gov/tech/initiatives/privacy/events-calendar#/?i=3

[8] https://www.crunchbase.com/acquisition/flir-systems-acquires-acyclica--e6043a1a#section-overview

[9] https://www.flir.com/support/products/roadtrend#Specifications

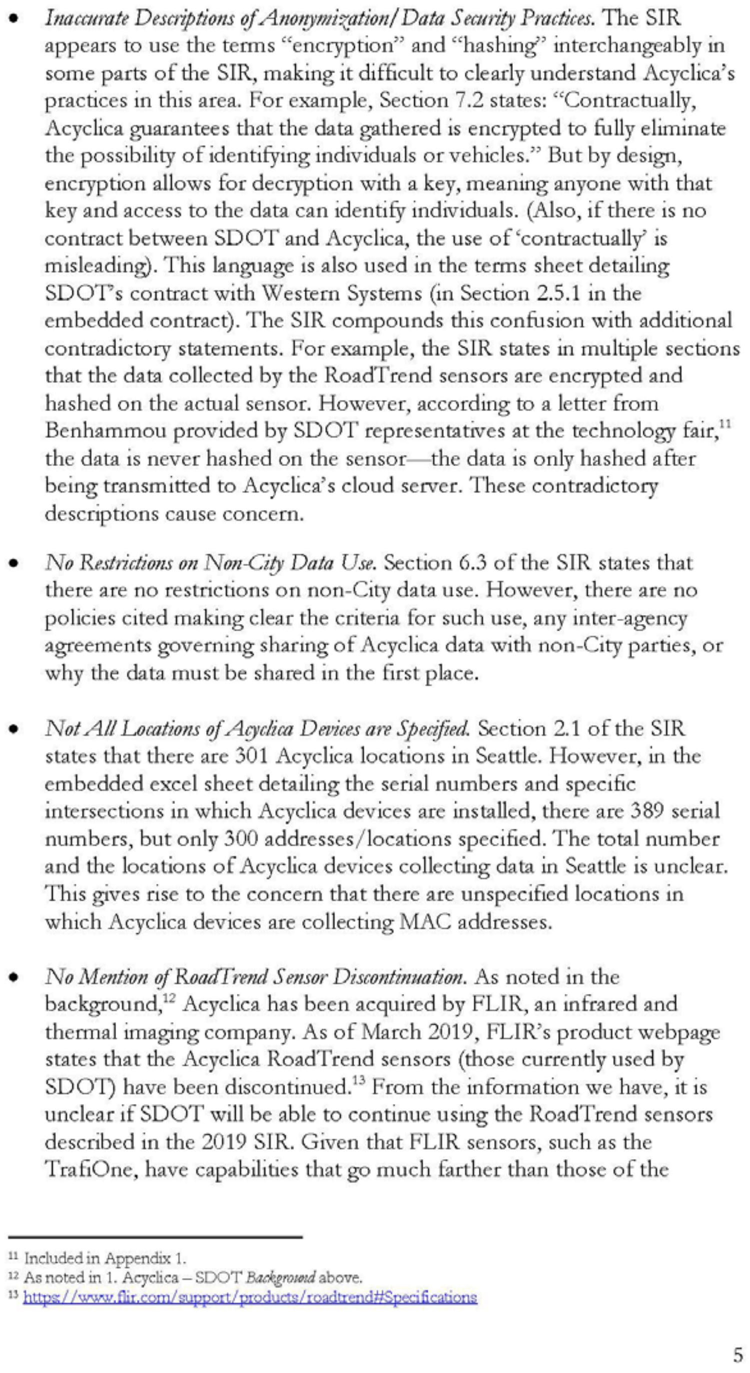
short, and impose no meaningful restrictions on the purposes for which Acyclica devices may be used.[10] Section 1.1 of the abstract set forth in the SIR states that Acyclica is used by over 50 agencies to "to help to monitor and improve traffic congestion." Section 2.1 is similarly vague, providing what appear to be examples of some types of information the technology produces (e.g., calculated average speeds) in order to facilitate outcomes (correcting traffic signal timing, providing information to travelers about expected delays, and allowing SDOT to meet traffic records and reporting requirements)—but it's not clear this list is exhaustive. Section 2.1 fails to describe the purpose of use, all the types of information Acyclica provides, and all the types of work that Acyclica technology facilitates. All these must be clarified.

- *Lack of Clarity on Whether Acyclica and SDOT have a Written Contract.* The SIR does not state that any contract exists, and in the 2018 conversation ACLU-WA had with Benhammou, he stated that there was no contract between the two parties. However, at the 2019 technology fair, the SDOT representative affirmatively stated that SDOT has a contract with Acyclica. As previously mentioned, the lack of a contract limits SDOT's ability to restrict the scope of data sharing and repurposing. The only contractual document provided appears to be a terms sheet in Section 3.0 detailing SDOT's terms of service with Western Systems (the hardware vendor that manufactures the Acyclica RoadTrend sensors), which states that Western Systems only deals with the maintenance and replacement of the hardware used to gather the data, and not the data itself.

- *Lack of Clarity on Data Ownership.* At the technology fair, the SDOT representative stated that SDOT owns all the data collected (including the raw data), but the SIR only states that the aggregated traffic data is owned by SDOT. In the 2018 conversation, Benhammou stated that Acyclica owns all the raw data. There is an apparent lack of clarity between SDOT and Acyclica concerning ownership of data that must be addressed.

- *Data Retention Periods are Unclear.* Section 5.2 of the SIR states that there is a 10-year internal deletion requirement for the aggregated traffic data owned by SDOT, but pg. 37 of the SIR states that "the data is deleted within 24 hours to prevent tracking devices over time." In the 2018 interview, Benhammou stated that Acyclica retains all non-aggregated data indefinitely. It is unclear whether the different retention periods stated in the SIR are referring to different types of data. The lack of clarity on data retention periods also relates to the lack of clarity on data ownership given that data retention periods may depend on data ownership.

[10] As noted in 1. Acyclica – SDOT *Background* above.



- *Inaccurate Descriptions of Anonymization/Data Security Practices.* The SIR appears to use the terms "encryption" and "hashing" interchangeably in some parts of the SIR, making it difficult to clearly understand Acyclica's practices in this area. For example, Section 7.2 states: "Contractually, Acyclica guarantees that the data gathered is encrypted to fully eliminate the possibility of identifying individuals or vehicles." But by design, encryption allows for decryption with a key, meaning anyone with that key and access to the data can identify individuals. (Also, if there is no contract between SDOT and Acyclica, the use of 'contractually' is misleading). This language is also used in the terms sheet detailing SDOT's contract with Western Systems (in Section 2.5.1 in the embedded contract). The SIR compounds this confusion with additional contradictory statements. For example, the SIR states in multiple sections that the data collected by the RoadTrend sensors are encrypted and hashed on the actual sensor. However, according to a letter from Benhammou provided by SDOT representatives at the technology fair,[11] the data is never hashed on the sensor—the data is only hashed after being transmitted to Acyclica's cloud server. These contradictory descriptions cause concern.

- *No Restrictions on Non-City Data Use.* Section 6.3 of the SIR states that there are no restrictions on non-City data use. However, there are no policies cited making clear the criteria for such use, any inter-agency agreements governing sharing of Acyclica data with non-City parties, or why the data must be shared in the first place.

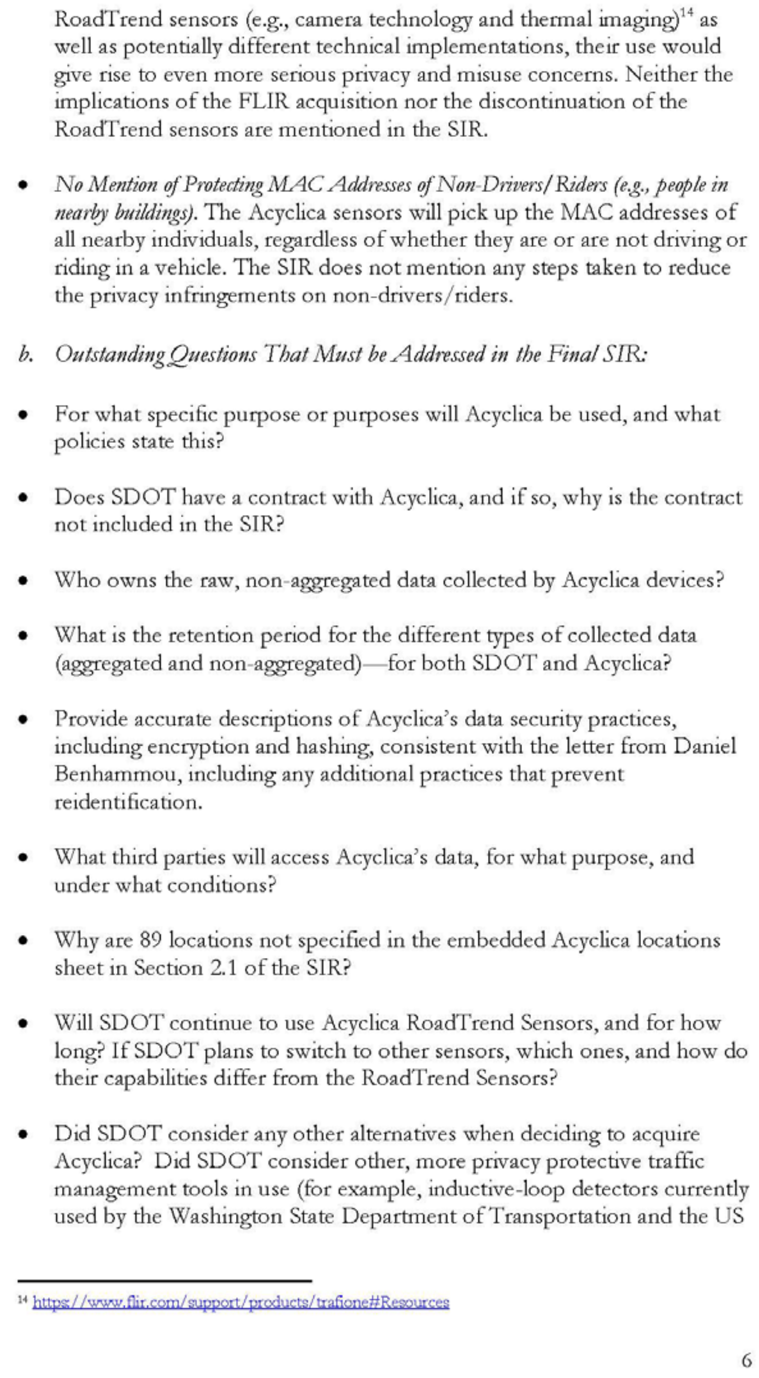
- *Not All Locations of Acyclica Devices are Specified.* Section 2.1 of the SIR states that there are 301 Acyclica locations in Seattle. However, in the embedded excel sheet detailing the serial numbers and specific intersections in which Acyclica devices are installed, there are 389 serial numbers, but only 300 addresses/locations specified. The total number and the locations of Acyclica devices collecting data in Seattle is unclear. This gives rise to the concern that there are unspecified locations in which Acyclica devices are collecting MAC addresses.

- *No Mention of RoadTrend Sensor Discontinuation.* As noted in the background,[12] Acyclica has been acquired by FLIR, an infrared and thermal imaging company. As of March 2019, FLIR's product webpage states that the Acyclica RoadTrend sensors (those currently used by SDOT) have been discontinued.[13] From the information we have, it is unclear if SDOT will be able to continue using the RoadTrend sensors described in the 2019 SIR. Given that FLIR sensors, such as the TrafiOne, have capabilities that go much farther than those of the

[11] Included in Appendix 1.

[12] As noted in 1. Acyclica – SDOT *Background* above.

[13] https://www.flir.com/support/products/roadtrend#Specifications



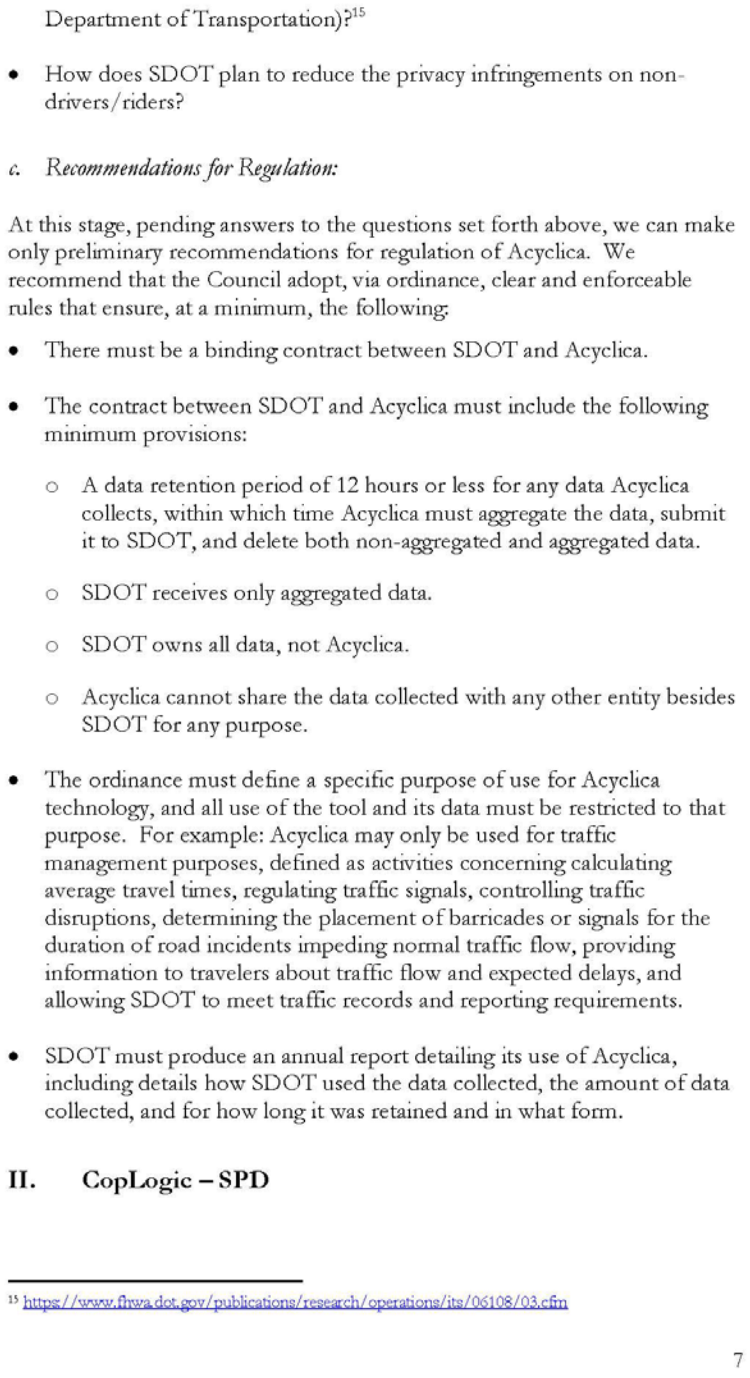
RoadTrend sensors (e.g., camera technology and thermal imaging)[14] as well as potentially different technical implementations, their use would give rise to even more serious privacy and misuse concerns. Neither the implications of the FLIR acquisition nor the discontinuation of the RoadTrend sensors are mentioned in the SIR.

- *No Mention of Protecting MAC Addresses of Non-Drivers/Riders (e.g., people in nearby buildings).* The Acyclica sensors will pick up the MAC addresses of all nearby individuals, regardless of whether they are or are not driving or riding in a vehicle. The SIR does not mention any steps taken to reduce the privacy infringements on non-drivers/riders.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- For what specific purpose or purposes will Acyclica be used, and what policies state this?
- Does SDOT have a contract with Acyclica, and if so, why is the contract not included in the SIR?
- Who owns the raw, non-aggregated data collected by Acyclica devices?
- What is the retention period for the different types of collected data (aggregated and non-aggregated)—for both SDOT and Acyclica?
- Provide accurate descriptions of Acyclica's data security practices, including encryption and hashing, consistent with the letter from Daniel Benhammou, including any additional practices that prevent reidentification.
- What third parties will access Acyclica's data, for what purpose, and under what conditions?
- Why are 89 locations not specified in the embedded Acyclica locations sheet in Section 2.1 of the SIR?
- Will SDOT continue to use Acyclica RoadTrend Sensors, and for how long? If SDOT plans to switch to other sensors, which ones, and how do their capabilities differ from the RoadTrend Sensors?
- Did SDOT consider any other alternatives when deciding to acquire Acyclica? Did SDOT consider other, more privacy protective traffic management tools in use (for example, inductive-loop detectors currently used by the Washington State Department of Transportation and the US

[14] https://www.flir.com/support/products/trafione#Resources



Department of Transportation)?[15]

- How does SDOT plan to reduce the privacy infringements on non-drivers/riders?

c. *Recommendations for Regulation:*

At this stage, pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of Acyclica. We recommend that the Council adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

- There must be a binding contract between SDOT and Acyclica.

- The contract between SDOT and Acyclica must include the following minimum provisions:

  - A data retention period of 12 hours or less for any data Acyclica collects, within which time Acyclica must aggregate the data, submit it to SDOT, and delete both non-aggregated and aggregated data.

  - SDOT receives only aggregated data.

  - SDOT owns all data, not Acyclica.

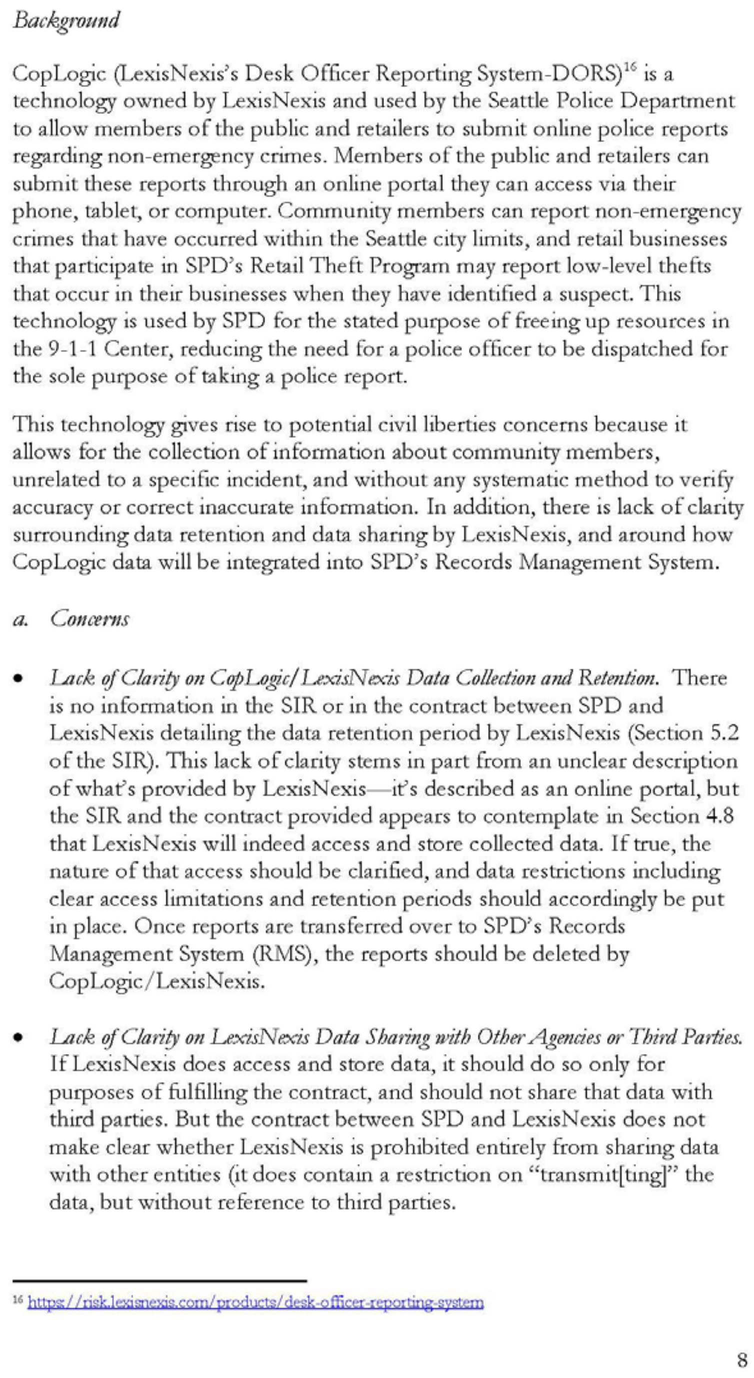
  - Acyclica cannot share the data collected with any other entity besides SDOT for any purpose.

- The ordinance must define a specific purpose of use for Acyclica technology, and all use of the tool and its data must be restricted to that purpose. For example: Acyclica may only be used for traffic management purposes, defined as activities concerning calculating average travel times, regulating traffic signals, controlling traffic disruptions, determining the placement of barricades or signals for the duration of road incidents impeding normal traffic flow, providing information to travelers about traffic flow and expected delays, and allowing SDOT to meet traffic records and reporting requirements.

- SDOT must produce an annual report detailing its use of Acyclica, including details how SDOT used the data collected, the amount of data collected, and for how long it was retained and in what form.

II. CopLogic – SPD

[15] https://www.fhwa.dot.gov/publications/research/operations/its/06108/03.cfm



Background

CopLogic (LexisNexis's Desk Officer Reporting System-DORS)[16] is a technology owned by LexisNexis and used by the Seattle Police Department to allow members of the public and retailers to submit online police reports regarding non-emergency crimes. Members of the public and retailers can submit these reports through an online portal they can access via their phone, tablet, or computer. Community members can report non-emergency crimes that have occurred within the Seattle city limits, and retail businesses that participate in SPD's Retail Theft Program may report low-level thefts that occur in their businesses when they have identified a suspect. This technology is used by SPD for the stated purpose of freeing up resources in the 9-1-1 Center, reducing the need for a police officer to be dispatched for the sole purpose of taking a police report.

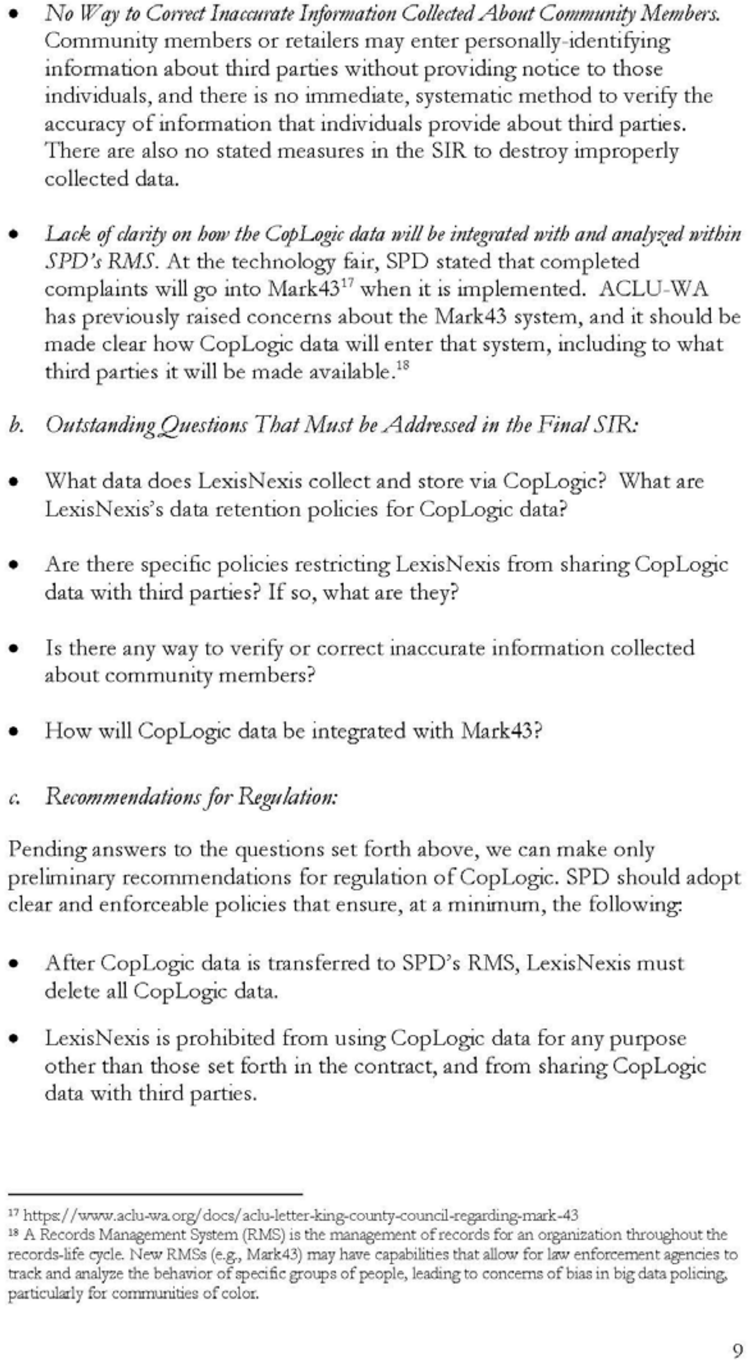
This technology gives rise to potential civil liberties concerns because it allows for the collection of information about community members, unrelated to a specific incident, and without any systematic method to verify accuracy or correct inaccurate information. In addition, there is lack of clarity surrounding data retention and data sharing by LexisNexis, and around how CopLogic data will be integrated into SPD's Records Management System.

a. *Concerns*

- *Lack of Clarity on CopLogic/LexisNexis Data Collection and Retention.* There is no information in the SIR or in the contract between SPD and LexisNexis detailing the data retention period by LexisNexis (Section 5.2 of the SIR). This lack of clarity stems in part from an unclear description of what's provided by LexisNexis—it's described as an online portal, but the SIR and the contract provided appears to contemplate in Section 4.8 that LexisNexis will indeed access and store collected data. If true, the nature of that access should be clarified, and data restrictions including clear access limitations and retention periods should accordingly be put in place. Once reports are transferred over to SPD's Records Management System (RMS), the reports should be deleted by CopLogic/LexisNexis.

- *Lack of Clarity on LexisNexis Data Sharing with Other Agencies or Third Parties.* If LexisNexis does access and store data, it should do so only for purposes of fulfilling the contract, and should not share that data with third parties. But the contract between SPD and LexisNexis does not make clear whether LexisNexis is prohibited entirely from sharing data with other entities (it does contain a restriction on "transmit[ting]" the data, but without reference to third parties.

[16] https://risk.lexisnexis.com/products/desk-officer-reporting-system



- *No Way to Correct Inaccurate Information Collected About Community Members.* Community members or retailers may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systematic method to verify the accuracy of information that individuals provide about third parties. There are also no stated measures in the SIR to destroy improperly collected data.

- *Lack of clarity on how the CopLogic data will be integrated with and analyzed within SPD's RMS.* At the technology fair, SPD stated that completed complaints will go into Mark43[17] when it is implemented. ACLU-WA has previously raised concerns about the Mark43 system, and it should be made clear how CopLogic data will enter that system, including to what third parties it will be made available.[18]

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What data does LexisNexis collect and store via CopLogic? What are LexisNexis's data retention policies for CopLogic data?

- Are there specific policies restricting LexisNexis from sharing CopLogic data with third parties? If so, what are they?

- Is there any way to verify or correct inaccurate information collected about community members?

- How will CopLogic data be integrated with Mark43?

c. Recommendations for Regulation:

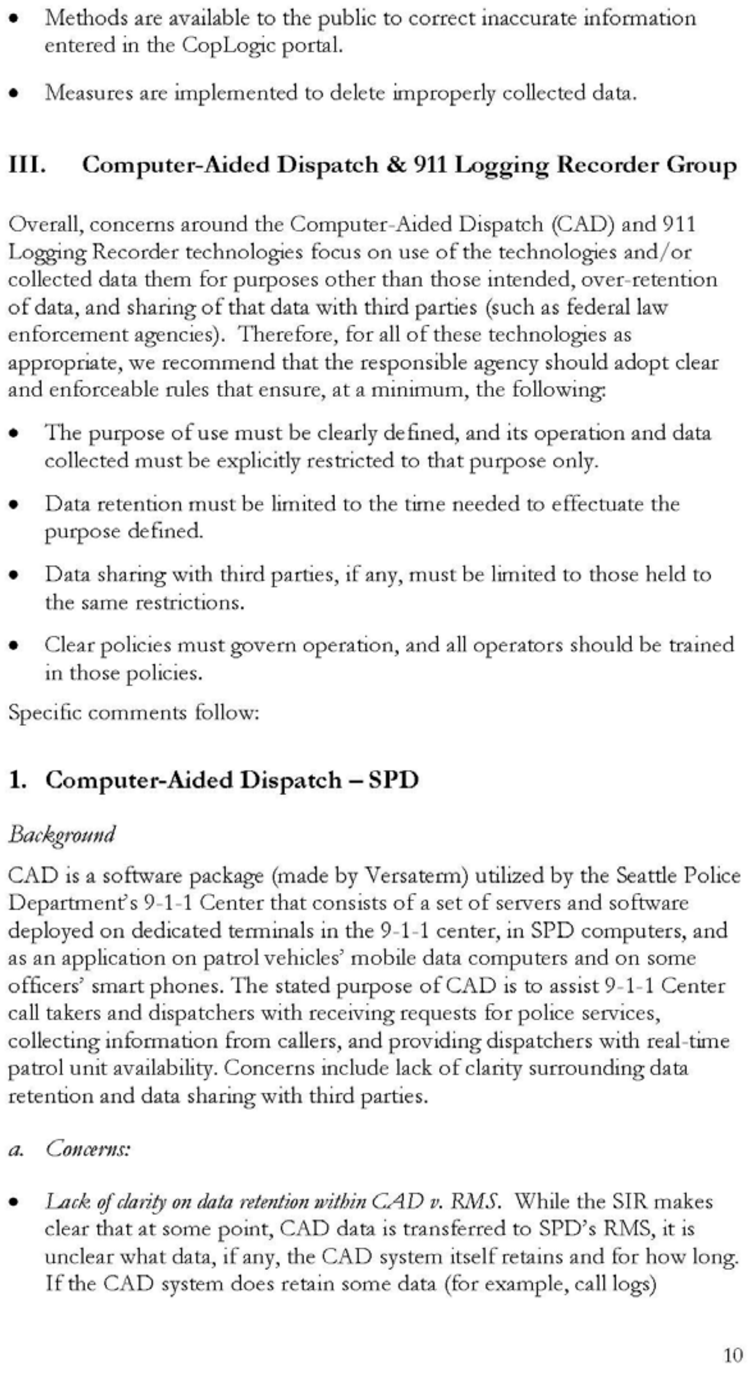
Pending answers to the questions set forth above, we can make only preliminary recommendations for regulation of CopLogic. SPD should adopt clear and enforceable policies that ensure, at a minimum, the following:

- After CopLogic data is transferred to SPD's RMS, LexisNexis must delete all CopLogic data.

- LexisNexis is prohibited from using CopLogic data for any purpose other than those set forth in the contract, and from sharing CopLogic data with third parties.

[17] https://www.aclu-wa.org/docs/aclu-letter-king-county-council-regarding-mark-43

[18] A Records Management System (RMS) is the management of records for an organization throughout the records-life cycle. New RMSs (e.g., Mark43) may have capabilities that allow for law enforcement agencies to track and analyze the behavior of specific groups of people, leading to concerns of bias in big data policing, particularly for communities of color.



- Methods are available to the public to correct inaccurate information entered in the CopLogic portal.
- Measures are implemented to delete improperly collected data.

III. Computer-Aided Dispatch & 911 Logging Recorder Group

Overall, concerns around the Computer-Aided Dispatch (CAD) and 911 Logging Recorder technologies focus on use of the technologies and/or collected data them for purposes other than those intended, over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). Therefore, for all of these technologies as appropriate, we recommend that the responsible agency should adopt clear and enforceable rules that ensure, at a minimum, the following:

- The purpose of use must be clearly defined, and its operation and data collected must be explicitly restricted to that purpose only.
- Data retention must be limited to the time needed to effectuate the purpose defined.
- Data sharing with third parties, if any, must be limited to those held to the same restrictions.
- Clear policies must govern operation, and all operators should be trained in those policies.

Specific comments follow:

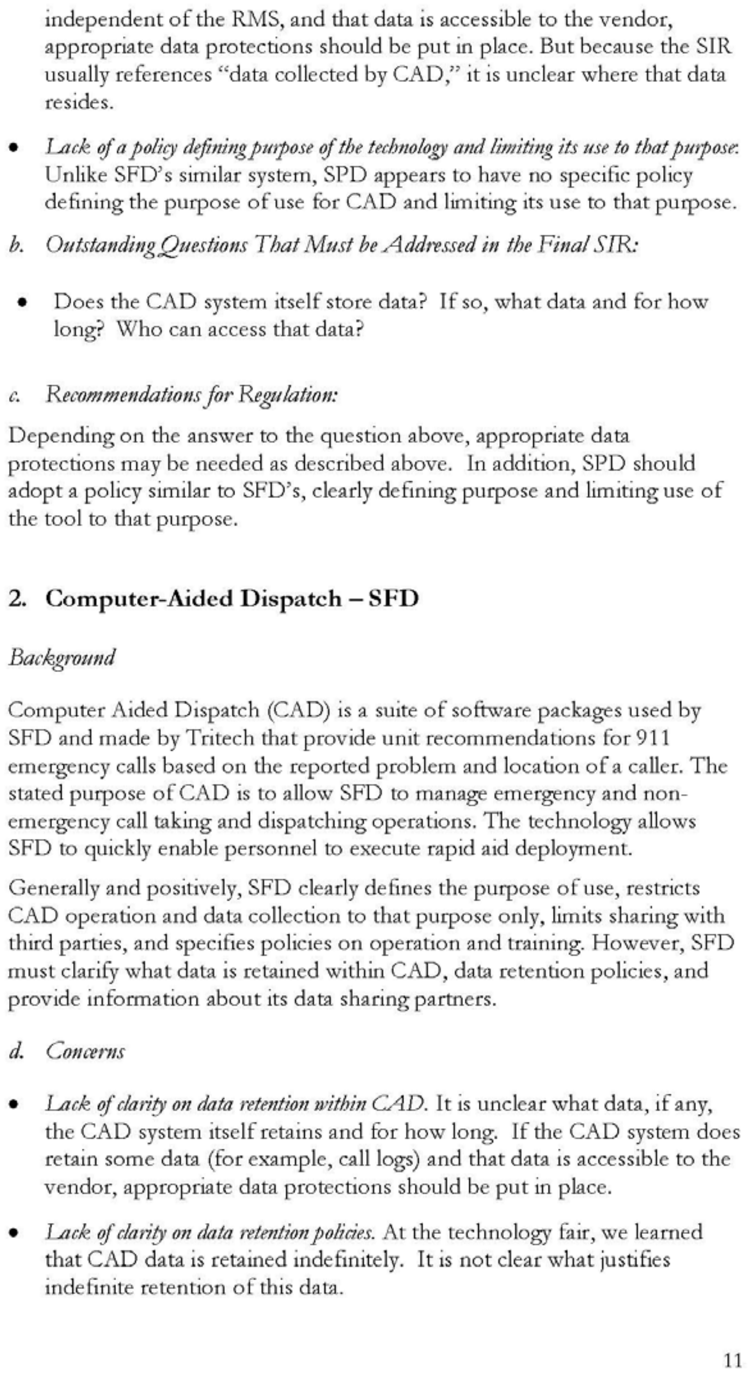
1. Computer-Aided Dispatch – SPD

Background

CAD is a software package (made by Versaterm) utilized by the Seattle Police Department's 9-1-1 Center that consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, in SPD computers, and as an application on patrol vehicles' mobile data computers and on some officers' smart phones. The stated purpose of CAD is to assist 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from callers, and providing dispatchers with real-time patrol unit availability. Concerns include lack of clarity surrounding data retention and data sharing with third parties.

a. Concerns:

- *Lack of clarity on data retention within CAD v. RMS.* While the SIR makes clear that at some point, CAD data is transferred to SPD's RMS, it is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs)



independent of the RMS, and that data is accessible to the vendor, appropriate data protections should be put in place. But because the SIR usually references "data collected by CAD," it is unclear where that data resides.

- *Lack of a policy defining purpose of the technology and limiting its use to that purpose*: Unlike SFD's similar system, SPD appears to have no specific policy defining the purpose of use for CAD and limiting its use to that purpose.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?

c. Recommendations for Regulation:

Depending on the answer to the question above, appropriate data protections may be needed as described above. In addition, SPD should adopt a policy similar to SFD's, clearly defining purpose and limiting use of the tool to that purpose.

2. Computer-Aided Dispatch – SFD

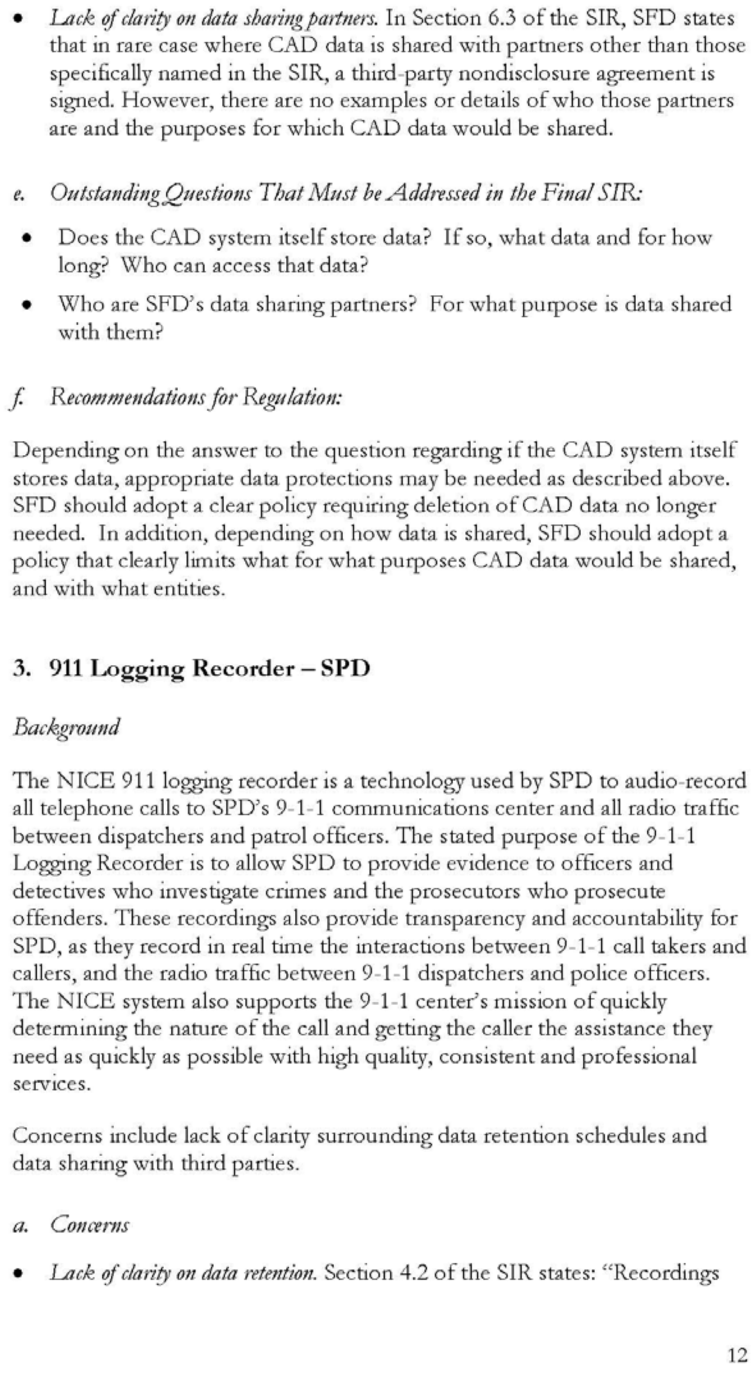
Background

Computer Aided Dispatch (CAD) is a suite of software packages used by SFD and made by Tritech that provide unit recommendations for 911 emergency calls based on the reported problem and location of a caller. The stated purpose of CAD is to allow SFD to manage emergency and non-emergency call taking and dispatching operations. The technology allows SFD to quickly enable personnel to execute rapid aid deployment.

Generally and positively, SFD clearly defines the purpose of use, restricts CAD operation and data collection to that purpose only, limits sharing with third parties, and specifies policies on operation and training. However, SFD must clarify what data is retained within CAD, data retention policies, and provide information about its data sharing partners.

d. Concerns

- *Lack of clarity on data retention within CAD.* It is unclear what data, if any, the CAD system itself retains and for how long. If the CAD system does retain some data (for example, call logs) and that data is accessible to the vendor, appropriate data protections should be put in place.
- *Lack of clarity on data retention policies.* At the technology fair, we learned that CAD data is retained indefinitely. It is not clear what justifies indefinite retention of this data.



- *Lack of clarity on data sharing partners.* In Section 6.3 of the SIR, SFD states that in rare case where CAD data is shared with partners other than those specifically named in the SIR, a third-party nondisclosure agreement is signed. However, there are no examples or details of who those partners are and the purposes for which CAD data would be shared.

e. Outstanding Questions That Must be Addressed in the Final SIR:

- Does the CAD system itself store data? If so, what data and for how long? Who can access that data?
- Who are SFD's data sharing partners? For what purpose is data shared with them?

f. Recommendations for Regulation:

Depending on the answer to the question regarding if the CAD system itself stores data, appropriate data protections may be needed as described above. SFD should adopt a clear policy requiring deletion of CAD data no longer needed. In addition, depending on how data is shared, SFD should adopt a policy that clearly limits what for what purposes CAD data would be shared, and with what entities.

3. 911 Logging Recorder – SPD

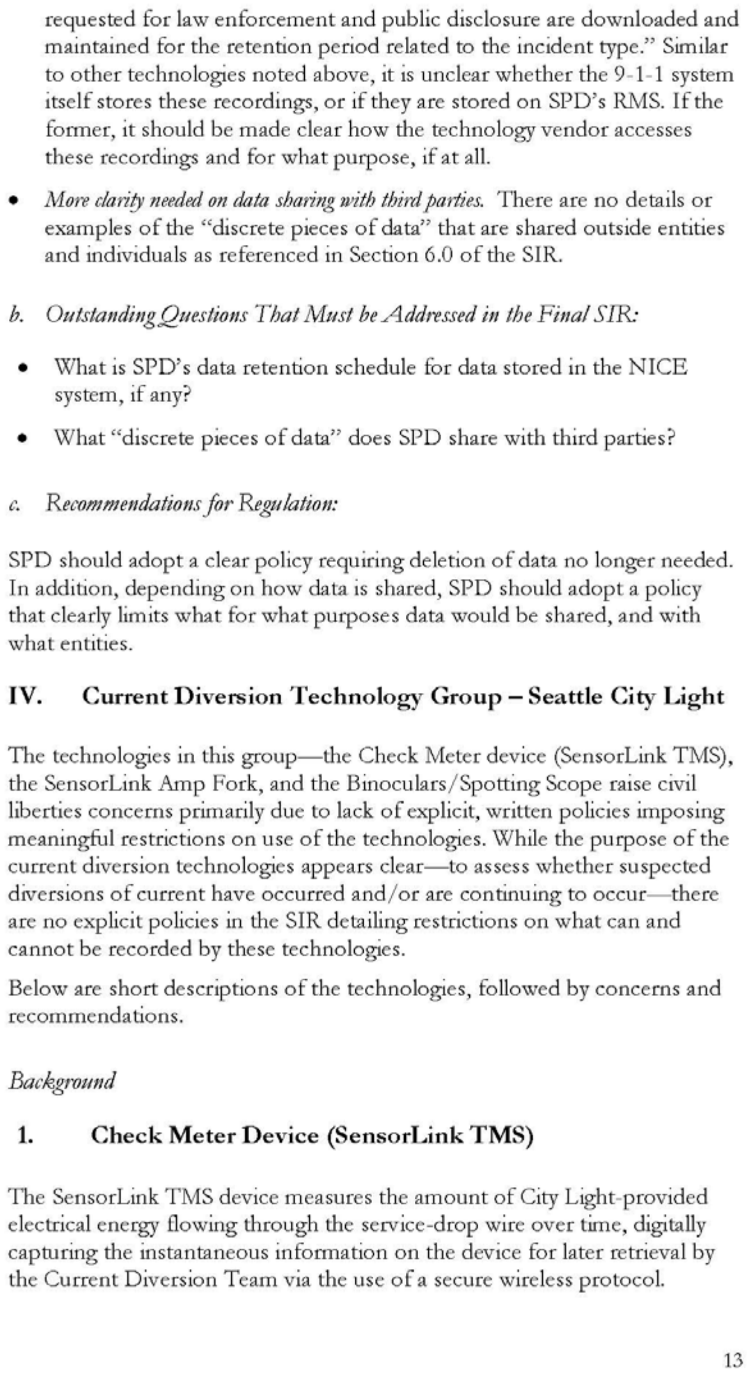
Background

The NICE 911 logging recorder is a technology used by SPD to audio-record all telephone calls to SPD's 9-1-1 communications center and all radio traffic between dispatchers and patrol officers. The stated purpose of the 9-1-1 Logging Recorder is to allow SPD to provide evidence to officers and detectives who investigate crimes and the prosecutors who prosecute offenders. These recordings also provide transparency and accountability for SPD, as they record in real time the interactions between 9-1-1 call takers and callers, and the radio traffic between 9-1-1 dispatchers and police officers. The NICE system also supports the 9-1-1 center's mission of quickly determining the nature of the call and getting the caller the assistance they need as quickly as possible with high quality, consistent and professional services.

Concerns include lack of clarity surrounding data retention schedules and data sharing with third parties.

a. Concerns

- *Lack of clarity on data retention.* Section 4.2 of the SIR states: "Recordings



requested for law enforcement and public disclosure are downloaded and maintained for the retention period related to the incident type." Similar to other technologies noted above, it is unclear whether the 9-1-1 system itself stores these recordings, or if they are stored on SPD's RMS. If the former, it should be made clear how the technology vendor accesses these recordings and for what purpose, if at all.

- *More clarity needed on data sharing with third parties.* There are no details or examples of the "discrete pieces of data" that are shared outside entities and individuals as referenced in Section 6.0 of the SIR.

b. Outstanding Questions That Must be Addressed in the Final SIR:

- What is SPD's data retention schedule for data stored in the NICE system, if any?
- What "discrete pieces of data" does SPD share with third parties?

c. Recommendations for Regulation:

SPD should adopt a clear policy requiring deletion of data no longer needed. In addition, depending on how data is shared, SPD should adopt a policy that clearly limits what for what purposes data would be shared, and with what entities.

IV. Current Diversion Technology Group – Seattle City Light

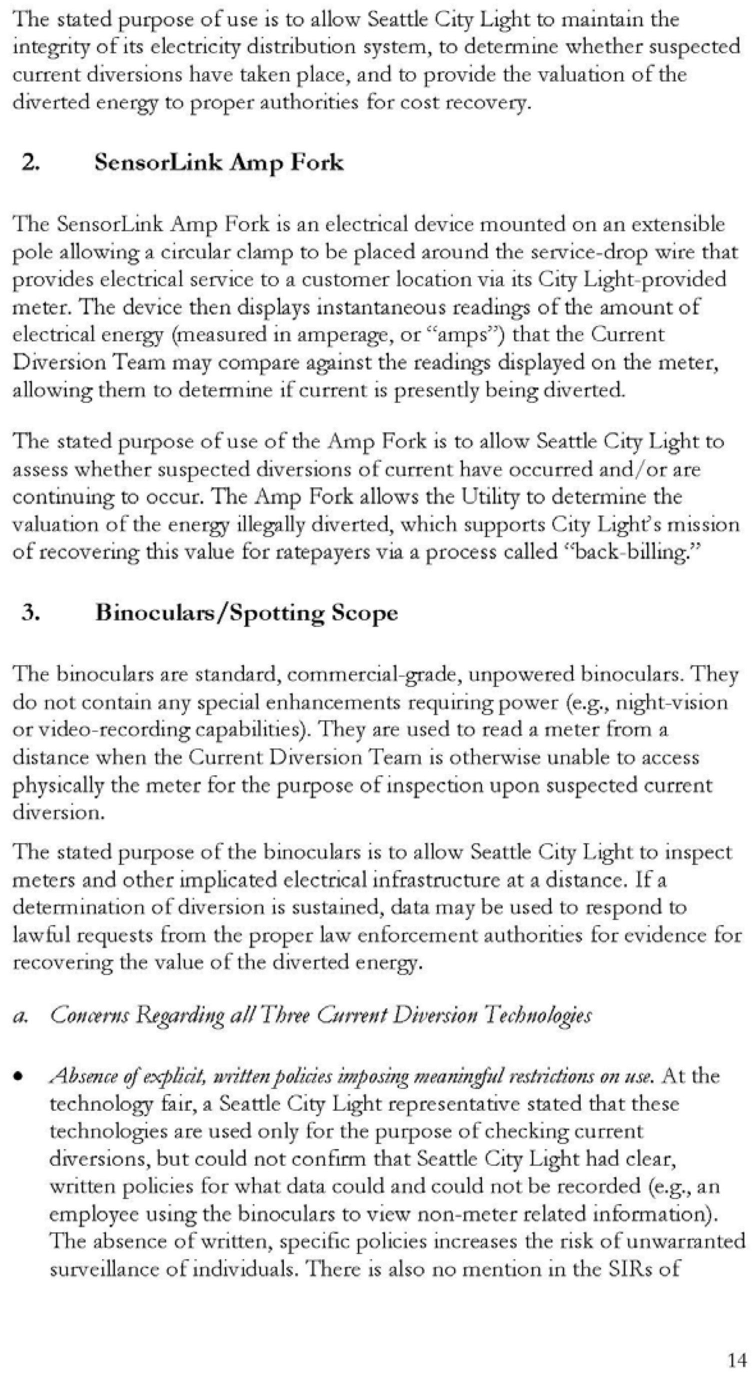
The technologies in this group—the Check Meter device (SensorLink TMS), the SensorLink Amp Fork, and the Binoculars/Spotting Scope raise civil liberties concerns primarily due to lack of explicit, written policies imposing meaningful restrictions on use of the technologies. While the purpose of the current diversion technologies appears clear—to assess whether suspected diversions of current have occurred and/or are continuing to occur—there are no explicit policies in the SIR detailing restrictions on what can and cannot be recorded by these technologies.

Below are short descriptions of the technologies, followed by concerns and recommendations.

Background

1. Check Meter Device (SensorLink TMS)

The SensorLink TMS device measures the amount of City Light-provided electrical energy flowing through the service-drop wire over time, digitally capturing the instantaneous information on the device for later retrieval by the Current Diversion Team via the use of a secure wireless protocol.



The stated purpose of use is to allow Seattle City Light to maintain the integrity of its electricity distribution system, to determine whether suspected current diversions have taken place, and to provide the valuation of the diverted energy to proper authorities for cost recovery.

2. SensorLink Amp Fork

The SensorLink Amp Fork is an electrical device mounted on an extensible pole allowing a circular clamp to be placed around the service-drop wire that provides electrical service to a customer location via its City Light-provided meter. The device then displays instantaneous readings of the amount of electrical energy (measured in amperage, or "amps") that the Current Diversion Team may compare against the readings displayed on the meter, allowing them to determine if current is presently being diverted.

The stated purpose of use of the Amp Fork is to allow Seattle City Light to assess whether suspected diversions of current have occurred and/or are continuing to occur. The Amp Fork allows the Utility to determine the valuation of the energy illegally diverted, which supports City Light's mission of recovering this value for ratepayers via a process called "back-billing."

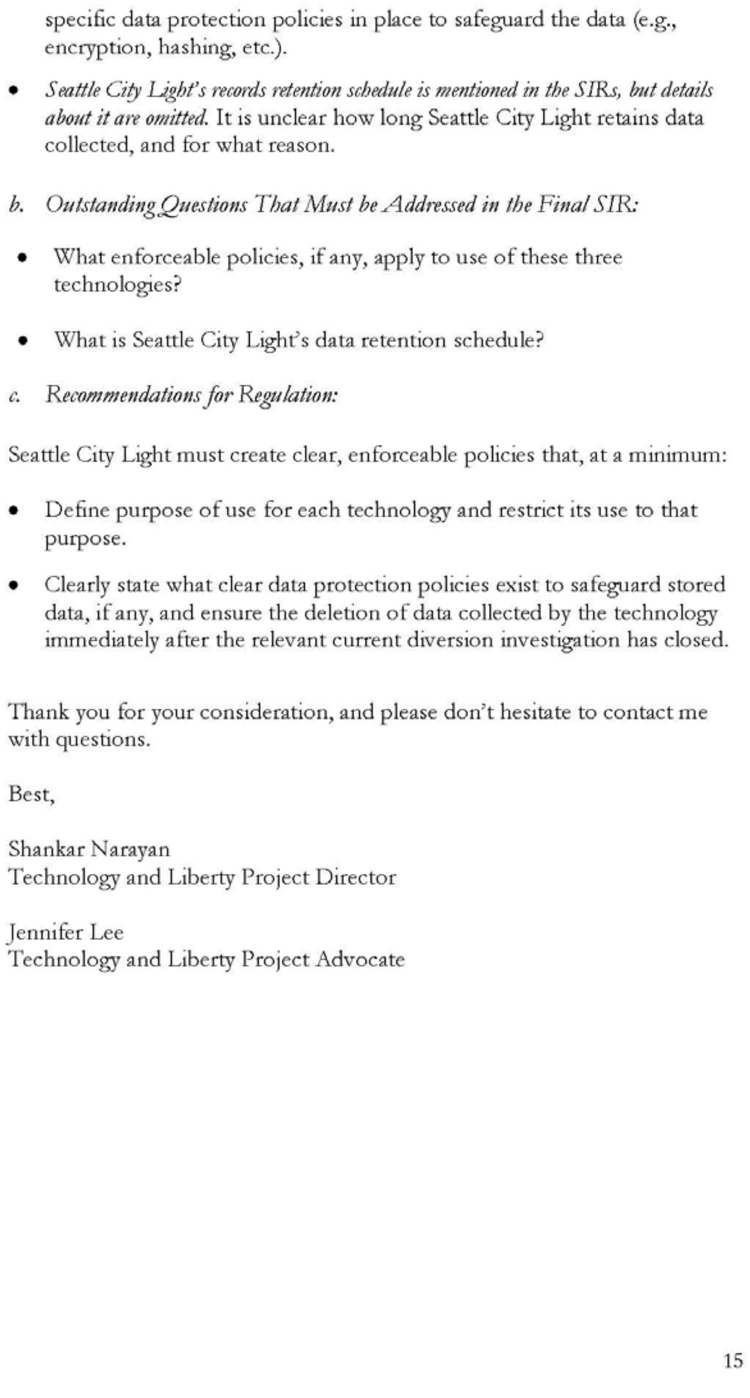
3. Binoculars/Spotting Scope

The binoculars are standard, commercial-grade, unpowered binoculars. They do not contain any special enhancements requiring power (e.g., night-vision or video-recording capabilities). They are used to read a meter from a distance when the Current Diversion Team is otherwise unable to access physically the meter for the purpose of inspection upon suspected current diversion.

The stated purpose of the binoculars is to allow Seattle City Light to inspect meters and other implicated electrical infrastructure at a distance. If a determination of diversion is sustained, data may be used to respond to lawful requests from the proper law enforcement authorities for evidence for recovering the value of the diverted energy.

a. Concerns Regarding all Three Current Diversion Technologies

- *Absence of explicit, written policies imposing meaningful restrictions on use.* At the technology fair, a Seattle City Light representative stated that these technologies are used only for the purpose of checking current diversions, but could not confirm that Seattle City Light had clear, written policies for what data could and could not be recorded (e.g., an employee using the binoculars to view non-meter related information). The absence of written, specific policies increases the risk of unwarranted surveillance of individuals. There is also no mention in the SIRs of



specific data protection policies in place to safeguard the data (e.g., encryption, hashing, etc.).

- *Seattle City Light's records retention schedule is mentioned in the SIRs, but details about it are omitted.* It is unclear how long Seattle City Light retains data collected, and for what reason.

b. *Outstanding Questions That Must be Addressed in the Final SIR:*

- What enforceable policies, if any, apply to use of these three technologies?
- What is Seattle City Light's data retention schedule?

c. *Recommendations for Regulation:*

Seattle City Light must create clear, enforceable policies that, at a minimum:

- Define purpose of use for each technology and restrict its use to that purpose.
- Clearly state what clear data protection policies exist to safeguard stored data, if any, and ensure the deletion of data collected by the technology immediately after the relevant current diversion investigation has closed.

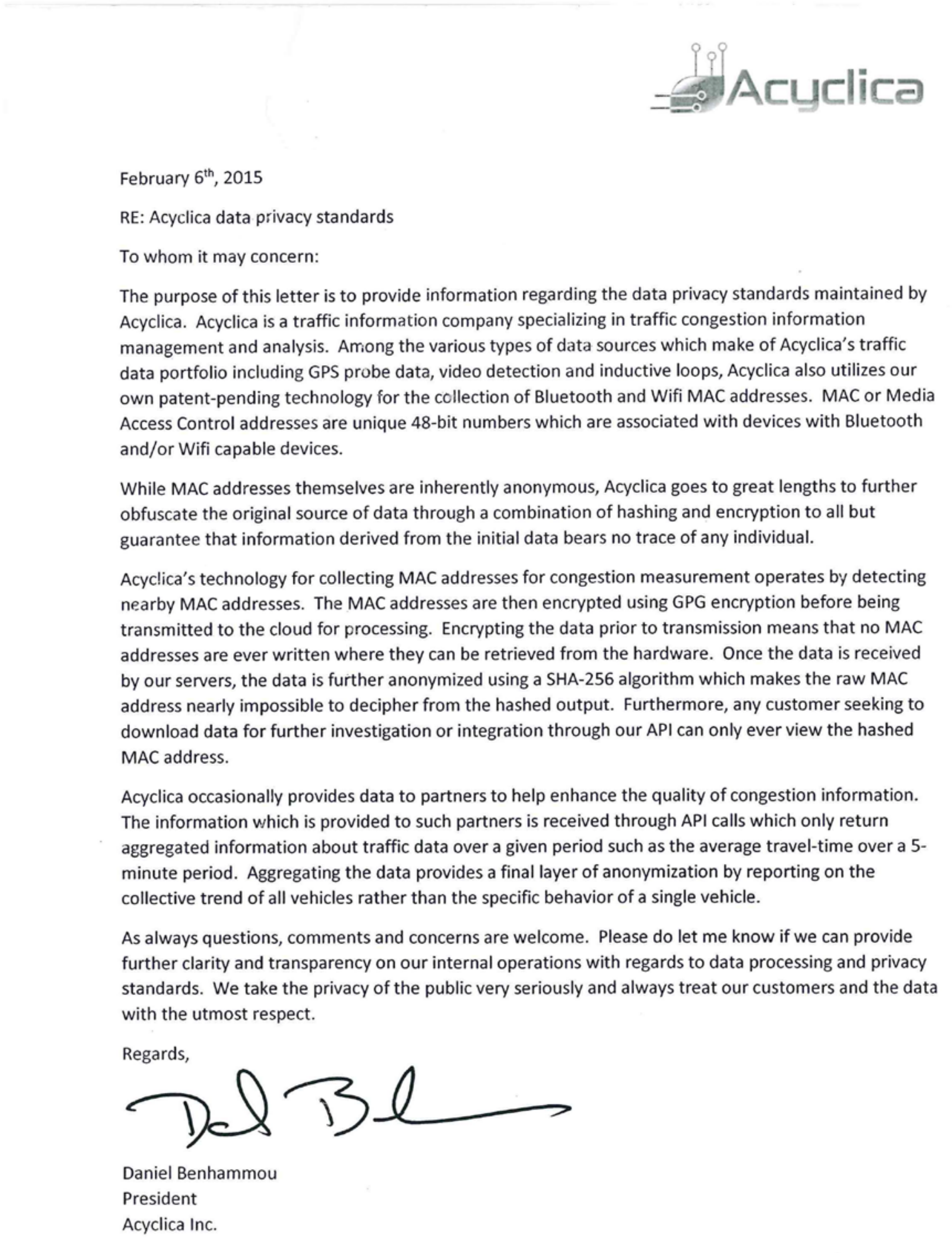
Thank you for your consideration, and please don't hesitate to contact me with questions.

Best,

Shankar Narayan
Technology and Liberty Project Director

Jennifer Lee
Technology and Liberty Project Advocate

Appendix 1: Benhammou Letter



Acyclica

February 6th, 2015

RE: Acyclica data privacy standards

To whom it may concern:

The purpose of this letter is to provide information regarding the data privacy standards maintained by Acyclica. Acyclica is a traffic information company specializing in traffic congestion information management and analysis. Among the various types of data sources which make of Acyclica's traffic data portfolio including GPS probe data, video detection and inductive loops, Acyclica also utilizes our own patent-pending technology for the collection of Bluetooth and Wifi MAC addresses. MAC or Media Access Control addresses are unique 48-bit numbers which are associated with devices with Bluetooth and/or Wifi capable devices.

While MAC addresses themselves are inherently anonymous, Acyclica goes to great lengths to further obfuscate the original source of data through a combination of hashing and encryption to all but guarantee that information derived from the initial data bears no trace of any individual.

Acyclica's technology for collecting MAC addresses for congestion measurement operates by detecting nearby MAC addresses. The MAC addresses are then encrypted using GPG encryption before being transmitted to the cloud for processing. Encrypting the data prior to transmission means that no MAC addresses are ever written where they can be retrieved from the hardware. Once the data is received by our servers, the data is further anonymized using a SHA-256 algorithm which makes the raw MAC address nearly impossible to decipher from the hashed output. Furthermore, any customer seeking to download data for further investigation or integration through our API can only ever view the hashed MAC address.

Acyclica occasionally provides data to partners to help enhance the quality of congestion information. The information which is provided to such partners is received through API calls which only return aggregated information about traffic data over a given period such as the average travel-time over a 5-minute period. Aggregating the data provides a final layer of anonymization by reporting on the collective trend of all vehicles rather than the specific behavior of a single vehicle.

As always questions, comments and concerns are welcome. Please do let me know if we can provide further clarity and transparency on our internal operations with regards to data processing and privacy standards. We take the privacy of the public very seriously and always treat our customers and the data with the utmost respect.

Regards,

Daniel Benhammou
President
Acyclica Inc.

Appendix H: Comment Analysis Methodology

Overview

The approach to comment analysis includes combination of qualitative and quantitative methods. A basic qualitative text analysis of the comments received, and a subsequent comparative analysis of results, were validated against quantitative results. Each comment was analyzed in the following ways, to observe trends and confirm conclusions:

1. Analyzed collectively, as a whole, with all other comments received
2. Analyzed by technology
3. Analyzed by technology and question

A summary of findings are included in Appendix B: Public Comment Demographics and Analysis. All comments received are included in Appendix E: All Individual Comments Received.

Background on Methodological Framework

A modified Framework Methodology was used for qualitative analysis of the comments received, which "*…approaches [that] identify commonalities and differences in qualitative data, before focusing on relationships between different parts of the data, thereby seeking to draw descriptive and/or explanatory conclusions clustered around themes" (Gale, N.K., et.al, 2013).* Framework Methodology is a coding process which includes both inductive and deductive approaches to qualitative analysis.

The goal is to classify the subject data so that it can be meaningfully compared with other elements of the data and help inform decision-making. Framework Methodology is "not designed to be representative of a wider population, but purposive to capture diversity around a phenomenon" (*Gale, N.K., et.al, 2013).*

Methodology

Step One: Prepare Data

1. Compile data received.
   a. Daily collection and maintenance of 2 primary datasets.
      i. Master dataset: a record of all raw comments received, questions generated at public meetings, and demographic information collected from all methods of submission.
      ii. Comment analysis dataset: the dataset used for comment analysis that contains coded data and the qualitative codebook. The codebook contains the qualitative codes used for analysis and their definitions.
2. Clean the compiled data.
   a. Ensure data is as consistent and complete as possible. Remove special characters for machine readability and analysis.
   b. Comments submitted through SurveyMonkey for "General Surveillance" remained in the "General Surveillance" category for the analysis, regardless

of content of the comment. Comments on surveillance generally, generated at public meetings, were categorized as such.

c. Filter data by technology for inclusion in individual SIRs.

Step Two: Conduct Qualitative Analysis Using Framework Methodology

1. Become familiar with the structure and content of the data. This occurred daily compilation and cleaning of the data in step one.
2. Individually and collaboratively code the comments received, and identify emergent themes.
   - I. Begin with deductive coding by developing pre-defined codes derived from the prescribed survey and small group facilitator questions and responses.
   - II. Use clean data, as outlined in Data Cleaning section above, to inductively code comments.
     - A. Each coder individually reviews the comments and independently codes them.
     - B. Coders compare and discuss codes, subcodes, and broad themes that emerge.
     - C. Qualitative codes are added as a new field (or series of fields) into the Comments dataset to derive greater insight into themes, and provide increased opportunity for visualizing findings.
   - III. Develop the analytical framework.
     - A. Coders discuss codes, sub-codes, and broad themes that emerge, until codes are agreed upon by all parties.
     - B. Codes are grouped into larger categories or themes.
     - C. The codes are be documented and defined in the codebook.
   - IV. Apply the framework to code the remainder of the comments received.
   - V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

1. Identify frequency of qualitative codes for each technology overall, by questions, or by themes:
   - I. Analyze results for single word codes.
   - II. Analyze results for word pair codes (for context).
2. Identify the most commonly used words and word pairs (most common and least common) for all comments received.
   - I. Compare results with qualitative code frequencies and use to validate codes.
   - II. Create network graph to identify relationships and frequencies between words used in comments submitted. Use this graph to validate analysis and themes.

3. Extract CSVs of single word codes, word pair codes, and word pairs in text of the comments, as well as the corresponding frequencies for generating visualizations in Tableau.

Step Four: Summarization

1. Visualize themes and codes in Tableau. Use call out quotes to provide context and tone.
2. Included summary information and analysis in the appendices of each SIR.

Appendix I: Supporting Policy Documentation

The following supporting documentation can be found on the following pages:

- Western Systems Contract
- SDOT Record Retention Schedule
- Western Systems Terms and MOU
- SDOT Data Ownership
- EDI DA-300 Data Sheet
- Acyclica Travel Time Accuracy & Reliability Analysis
- Seattle Security Assurance Request

Appendix J: 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

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