City of Seattle

2019 Surveillance Impact Report

CopLogic

Seattle Police Department

DRAFT

Table of Contents

Submitting Department Memo 3
Surveillance Impact Report ("SIR") overview 5
Privacy Impact Assessment 6
Financial Information 25
Expertise and References 27
Racial Equity Toolkit ("RET") and Engagement for Public Comment Worksheet 28
Privacy and Civil Liberties Assessment 43
CTO Response to Privacy and Civil Liberties Assessment 44
Appendix A: Glossary 45
Appendix B: Meeting Notice(s) 47
Appendix C: Meeting Sign-in Sheet(s) 55
Appendix D: Department of Neighborhood Focus Group Notes 78
Appendix E: All Comments Received from Members of the Public 110
Appendix F: Department Responses to Public Inquiries(PDF) 117
Appendix G: Letters from Organizations or Commissions 121
Appendix H: Comment Analysis Methodology 145
Appendix I: Supporting Policy Documentation 148
Appendix J: CTO Notification of Surveillance Technology 154

DRAFT

City of Seattle

Submitting Department Memo

Memo

Date: April 29, 2019
To: City Council
From: Deputy Chief GarthGreen, Seattle Police Department
Subject: Cover Memo - CopLogic

Description

CopLogic is a crime reporting software tool that allows members of the public to submit police reports online through a web-based interface. CopLogic is a Software as a Service (SaaS) owned and maintained by LexisNexis. SPD utilizes this technology in two ways: 1) An online public interface allows individuals to report a low-level crime in which no known or describable suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), without waiting for an officer to dispatch and take a report; 2) An online password-protected interface allows retailers to enter information about retail theft on their property in which a suspect is known and suspect information is available.

Purpose

CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still reap the benefits of reporting an incident, for instance, obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. In 2017, 14,356 crimes were reported via CopLogic, freeing resources in the 9-1-1 Center, ensuring that 9-1-1 call takers and SPD officers are available for more serious incidents.

Benefits to the Public

CopLogic benefits both the community and the Seattle Police Department by freeing resources in the 9-1-1 center, eliminating the need for patrol officers to respond in person to take some crime reports, and providing community members with a secure, convenient, and timely way to interact with police. Community members also receive a no-cost copy of their police report when they complete their report with the CopLogic system. CopLogic saves over 20,000 patrol officer hours annually, freeing patrol resources for more serious incidents and saving the Department over $1,000,000 each year.

DRAFT

Privacy and Civil Liberties Considerations

During the public comment period, SPD heard concerns about privacy from community members. They raised concerns around the perceived ability for the public to make complaints about specific people or communities through the system, the lack of access to online reporting for marginalized communities, what kinds of crimes can be reported using the system, how long records are retained, how secure the collected information is, and who has access to the information – particularly what access the vendor, LexisNexis, has to the information collected by the CopLogic system.

By not allowing the community to report crimes with known or describable suspects via the CopLogic system, SPD has mitigated the concerns that the system allows for collection of information and malicious reporting directed at specific individuals or communities. The agreement between SPD and LexisNexis limits the use and storage of all information collected by or on behalf of the City to only purposes used for providing the service in the CopLogic contract and consultant agreement. They are prohibited from using City data or personal information collected by the system to engage or enable another party to engage in marketing or targeted advertising. Additionally, no access or information shall be provided to any employee or agent of any federal immigration agency without prior review and consent of the City. Additionally, per the agreement between SPD and LexisNexis, reports that are generated in the CopLogic system are imported into SPD's records management system and then auto-deleted from the LexisNexis servers after 120 days. Reports that are rejected by the SPD officers who review the reports are deleted immediately and notification is sent to the community member.

SPD acknowledges that there are barriers to online reporting for some community members. The CopLogic system is, like much of the City of Seattle web presence, not translated into other languages. The system requires the reporter to have access to the internet on either a computer or smart phone and have an email address, both of which may not be available to all members of the community, particularly among traditionally marginalized communities and homeless individuals. Kiosk computers have been installed at SPD precincts which allow community members access to CopLogic online reporting, and the system is available from other public-access computers like those available at libraries. The CopLogic online crime reporting system does not replace other methods of contacting SPD for services and reporting crimes. Community members who need services in languages other than English, do not have access to the internet or an email address, or are uncomfortable making a report online are still able to contact SPD via the telephone or by making a report at an SPD Precinct.

Summary

CopLogic is an opt-in online crime reporting system that benefits the community, SPD, the 9-1-1 Center, and the City of Seattle. CopLogic saves over 20,000 patrol officer hours annually, freeing patrol resources for more serious incidents and saving the Department and the City over $1,000,000 each year. Online reporting allows community members to report certain crimes in a secure, convenient, and frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents. Only authorized SPD personnel can access the information provided by the individuals through the online reporting tool and all activity in the system is logged and auditable. The vendor, LexisNexis, cannot access the information for any reason other than providing SPD with the online reporting services and is not permitted to share the information with any third party.

DRAFT

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle it policy pr-02, the "surveillance policy".

How this Document is Completed

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

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

Surveillance Ordinance Review Process

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

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

DRAFT

Privacy Impact Assessment

Purpose

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

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

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

1.0 Abstract

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

CopLogic is crime reporting tool that allows individuals to submit police reports online. SPD utilizes this technology for two purposes: (1) community members may report specific low-level, non-emergency crimes that have occurred within the Seattle city limits, in which there are no known suspects or additional information that would allow for investigation of the crime; and (2) 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. CopLogic provides efficient customer service to community members who may need proof of police reporting (i.e., for insurance purposes) without needing to call 9-1-1 then waiting for an officer to respond and take a report. CopLogic frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents and frees patrol officer resources by eliminating the need for a police officer to be dispatched for the sole purpose of taking a police report.

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

CopLogic is an opt-in system; it is used only when an individual chooses to utilize it. However, individuals may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systemic method to verify the accuracy of information that individuals provide about those third parties.

DRAFT

2.0 Project / Technology Overview

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

2.1 Describe the benefits of the project/technology.

CopLogic has two tracks:

1) An online public interface allows individuals to report a crime in which no known suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), without waiting for an officer to dispatch and take a report.
2) An online password-protected interface allows retailers to enter information about retail theft on their property in which a suspect known and suspect information is available.

CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still reap the benefits of reporting an incident, for instance, obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. Last year, 14,356 crimes were reported via CopLogic which is 14,356 fewer 9-1-1 calls taken by the 9-1-1 Center. This technology frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers are available for more serious incidents.

DRAFT

2.2 Provide any data or research demonstrating anticipated benefits.

Research Studies:

- Loss Prevention Technology Case Study "*Using Technology to Enhance the Relationship between Loss Prevention and Local Law Enforcement"*
- Travis Taniguchi and Christopher Salvatore, "Citizen Perceptions of Online Crime Reporting Systems," *The Police Chief* 82 (June 2015): 48–52. http://www.policechiefmagazine.org/citizen-perceptions-of-online-crime-reporting-systems/?ref=3e3a108ad4f36c878bb398b470385dcc

Research shows that allowing individuals to report certain non-urgent crimes and for trained retail loss prevention employees to streamline the shoplifting reporting process provided through online tools such as CopLogic delivers benefits to both the department by eliminating the need for patrol officers to respond in person to take such reports, and providing community members with a secure, convenient, and timely way to interact with police.

SPD has collected data about CopLogic's effectiveness since 2012. The use of CopLogic has increased each year, and it saves numerous police hours by eliminating the need for a patrol officer to respond. The data shows:

	Reports	Hours Saved	Money Saved
2012	7,652	11,478	$573,900.00
2013	9,527	14,290	$714,525.00
2014	12,575	18,862	$943,125.00
2015	12,365	18,547	$927,375.00
2016	13,379	20,068	$1,003,425.00
2017	14,356	21,534	$1,076,700.00
2018*	13,571	20,356	$1,017,825.00

*(2018 Data is calculated through the end of October.)

DRAFT

2.3 Describe the technology involved.

CopLogic is a Software as a Service (SaaS) owned and maintained by LexisNexis. It is used in two ways:

1) Public Interface: Individuals wishing to file a report visit Seattle Police Department's Online Reporting page (https://www.seattle.gov/police/need-help/online-reporting) and follow the prompts to enter information about low-level, non-emergency crimes for which no known suspects exist. CopLogic then generates a report and the reporter receives a temporary unique identification number. An SPD employee, the reviewer, verifies that the report is sufficient and complete. If further information or clarification is needed, the reviewer generates a generic email to the reporter, informing them that the report is missing information that must be included before the file is officially submitted, and providing a link to follow for updates. Once a reviewer determines that the report is complete, the information is electronically transferred into SPD's records management system and receives a general offense (GO) number. This GO number is then provided to the reporter for their records and for insurance purposes.
2) Retail Theft Interface: Retailers who participate in the Seattle Police Department's Retail Theft Program and wish to report a theft first contact the Seattle Police Department's non-emergency number to receive a case number. Then, they access the Retail Theft online page with unique password-protected login information and fill out the Retail Theft online report, which includes information about the retailer, the theft, and the suspect. In most circumstances, retailer security has detained the suspect and included copies of identification with the report that they then submit online.

After a report is made into the Public Interface or the Retail Theft Interface, police officers assigned to the Internet and Telephone Reporting Unit (I-TRU) log in to the CopLogic web portal, utilizing individual user log-in IDs, to access the submitted reports. Once the report is screened by an officer in the I-TRU unit, SPD utilizes an integration server to transfer reports generated in the CopLogic tool into SPD's Records Management System.

DRAFT

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

SPD's mission is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. CopLogic allows for the user, either an individual or a retail store, to report crimes at their own convenience. CopLogic is available 24 hours per day, seven days per week. When users decide that they do not need a police officer to respond to the scene, they may still benefit from reporting an incident, for instance, by quickly obtaining a case number for insurance purposes or requesting criminal charges for a theft in their business. CopLogic also eliminates the need for individuals to call 9-1-1 to report a crime and have a report taken. Last year, 14,356 crimes were reported via CopLogic which is 14,356 fewer 9-1-1 calls taken by the 9-1-1 Center. This technology frees resources in the 9-1-1 Center, ensuring that 9-1-1 call takers, and then patrol officers, are available for more serious incidents.

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

SPD reviewers within the I-TRU unit have access to the reports for the purposes of verifying accuracy and initiating the process of transferring the approved reports into the records management system with a case number (as is assigned to all SPD reports).

Additionally, Seattle IT provides client services and operational support for IT technologies and applications. In supporting SPD systems, operational and application services deploy and service SPD technology systems. Details about the IT department are found in the appendix of this SIR.

DRAFT

3.0 Use Governance

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

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

CopLogic is used by the public, including retailers, and, thus, its use is triggered whenever an individual instigates the submission of an online report. The SPD reviewer checks the submission for completion and does one of the following:

1) Sends a generic email to the submitter asking for additional information; or
2) Pushes the report to SPD's records management system, providing the report a General Offense ("GO") number, which is then sent back to the submitter.

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

Individuals may use CopLogic to report a crime online when:

1) The crime is within one of these categories of crime:
    a. Property crimes including property destruction, graffiti, car break ins, theft of auto accessories, theft, shoplifting; or
    b. Drug activity, harassing phone calls, credit card fraud, wage theft, identity theft, or lost property
2) The situation is non-emergent
3) The crime occurred within Seattle city limits (exception for identity theft); and
4) No known suspects or information about the crime would allow for additional investigation.

Retailers may use CopLogic to report a retail theft on their property when:

1) The retailer participates in SPD's Retail Theft Program and has obtained a unique login identifier and password;
2) They have detained the suspect;
3) The suspect does not have any outstanding warrants; and
4) They verify the identification of the suspect and upload copies of the suspect's identification, if available.

DRAFT

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.

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Once data is input by individuals and retail users of CopLogic on the public-facing website, it is accessed and used on SPD's password-protected network.

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

SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

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

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements." This MCA document may be found in Appendix K.

DRAFT

4.0 Data Collection and Use

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

No information is collected from a source other than the individual instigating the submission of a report.

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

Before anyone is permitted to file a report online, they are prompted to answer a series of questions to determine if online reporting is appropriate for the event they wish to report. In addition, the Seattle Police Department provides guidelines to individuals reporting an event about what information they will need to submit to file a report online. Finally, an authorized SPD employee reviews each submission before accepting the report to ensure that appropriate and adequate information has been provided.

Retail security collects only information that is necessary to document and investigate the crime as required on the Retail Theft Reporting form. No other information is requested.

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?

CopLogic is an online portal that is available for individuals to utilize at any time. It was implemented in the fall of 2011.

Retailers have access to a Retail Theft portal with unique password-protected login information.

CopLogic is a Software as a Service. It utilizes server integration so reports can be transferred to SPD's Records Management System.

4.4 How often will the technology be in operation?

The online portal is continuously in operation, so individuals can instigate and submit reports at any time.

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

CopLogic is a permanent installation.

DRAFT

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?

CopLogic is an online portal, not a physical object. As such, the portal is visible to the public when they visit the online page (https://www.seattle.gov/police/need-help/online-reporting), but is not otherwise visible. The online page contains City of Seattle and SPD branding and contact information. There is also specific text on the web page letting the public know what kind of crimes they may report using this technology.

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

Only authorized SPD users can access the system, technology, or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Collected data is securely viewed on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel within the I-TRU unit. Once a reported incident has been reviewed by SPD personnel, it is electronically transferred into the SPD records management system.

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

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles that may be associated with client services for City Departments can be found in Appendix K.

ITD client services interaction with SPD systems is governed by the terms of the 2018 Management Control Agreement (MCA) between ITD and SPD. The MCA document may be found in Appendix K.

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

CopLogic is owned and maintained by Lexis Nexis. There are no data sharing agreements between SPD and any other entities for CopLogic data. Further, the contract between the City and LexisNexis provides that LexisNexis may only "use, transmit, distribute, modify, reproduce, display, and store the City Data solely for the purposes of (i) providing the Services as contemplated in [its contract with the City]; and (ii) enforcing its rights under [the contract]." A link to the LexisNexis privacy policy can be found here: https://risk.lexisnexis.com/privacy-policy

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

DRAFT

SPD reviewers must access the reports to check for accuracy and approve reports so that the report can be transferred into SPD's records management system with an appropriately assigned case number. Once the information is entered into the records management system, the information can be accessed by authorized SPD personnel at any time, as it relates to a specific investigation, just as is the case with any information stored within the records management system.

Incidental data access may occur through delivery of technology client services. All ITD employees are required to comply with appropriate regulatory requirements regarding security and background review. Information on the ITD roles associated with client services for City Departments can be found in Appendix K.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix K.

DRAFT

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

CopLogic data is stored remotely and managed by the technology provider, Lexis Nexis. Lexis Nexis is Privacy Shield Certified and adheres to the RELX Group Privacy Shield Principles. Per Lexis Nexis: "We use a variety of administrative, physical and technical security measures to help safeguard your personal information." Additionally, SPD's contract with Lexis Nexis includes a clause for audit, in which the "Consultant shall permit the City and any other governmental agency funding the Work, to inspect and audit all pertinent books and records."

SPD personnel can only access CopLogic data when authorized and provided a username and password for the system. CopLogic creates an audit log that records all activity in the system with usernames and timestamps.

ITD client services interaction with SPD systems is governed according to the terms of the 2018 Management Control Agreement between ITD and SPD, which states that:

"Pursuant to Seattle Municipal Code (SMC) 3.23, ITD provides information technology systems, services and support to SPD and is therefore required to support, enable, enforce and comply with SPD policy requirements, including the FBIs Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix K.

DRAFT

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

CopLogic is a web-hosted solution provided by Lexis Nexis and all information entered into the system is stored on the LexisNexis platform. Per Lexis Nexis: "We use a variety of administrative, physical and technical security measures to help safeguard your personal information." Additionally, Lexis Nexis is Privacy Shield Certified and adheres to the RELX Group Privacy Shield Principles.

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

DRAFT

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any system at any time. The Office of Inspector General and the federal monitor can also access all data and can audit for compliance at any time.

Additionally, SPD's contract with Lexis Nexis includes a clause for audit, in which the "Consultant shall permit the City and any other governmental agency funding the Work, to inspect and audit all pertinent books and records."

Seattle Information Technology

City of Seattle Information Technology Department

With

Lexis Nexis Risk Solutions

CONSULTANT AGREEMENT

Title: Project Management for Lexis Nexis

AGREEMENT NUMBER: C3-0201-18

This Agreement is made and entered into by and between the City of Seattle ("the City"), a Washington municipal corporation, through its Department of Information Technology as represented by the Chief Technology Officer; and Lexis Nexis Risk Solutions ("Consultant"), a corporation of the State of Pennsylvania, and authorized to do business in the State of Washington.

The purpose of this contract is to provide the City of Seattle with Project Management Services for Lexis Nexis Desk Officer Reporting System Interface Implementation for Mark43 Cobalt RMS. This project is valued less than $52,000.00. As a result, the Department selected this Consultant through Direct Select.

In consideration of the terms, conditions, covenants and performance of the Scope of Work contained herein, the City and Consultant mutually agree as follows:

1. TERM OF AGREEMENT.
The term of this Agreement begins when fully executed by all parties and ends on October 31, 2018 unless amended by written agreement or terminated earlier under termination provisions.

2. TIME OF BEGINNING AND COMPLETION.
The Consultant shall begin the work outlined in Quote 20180427 - "Scope of Work" ("Work") upon receipt of written notice to proceed from the City. The City will acknowledge in writing when the Work is complete. Time limits established under this Agreement shall not be extended because of delays for which the Consultant is responsible, but may be extended by the City, in writing, for the City's convenience or conditions beyond the Consultant's control.

3. SCOPE OF WORK.
The Scope of Work for this Agreement and the time schedule for completion of such Work are described in Attachment A, which is attached to and made a part of this Agreement.

The Work is subject to City review and approval. The Consultant shall confer with the City periodically and prepare and present information and materials (e.g. detailed outline of completed Work) requested by the City to determine the adequacy of the Work or Consultant's progress.

4. EXPANSION FOR NEW WORK.
This Agreement scope may be expanded for new work. Any expansion for New Work (work not specified within the original Scope of Work Section of this Agreement, and/or not specified in the original RFP as intended work for the Agreement) must comply with all the following limitations and requirements: (a) the

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

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

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

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

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

DRAFT

6.0 Data Sharing and Accuracy

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

SPD has no data sharing partners for CopLogic. No person, outside of SPD, has direct access to the application or the data and all requests for information from CopLogic are processed based on existing SPD policies, legal guidelines, and as required by law.

As Seattle IT supports the CopLogic system on behalf of SPD, a Management Control Agreement exists between SPD and Seattle IT. The agreement outlines the specifications for compliance, and enforcement related to supporting the CopLogic system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

Discrete pieces of information obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

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

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

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

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

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the system.

DRAFT

6.2 Why is data sharing necessary?

Data sharing is not an automatic component of CopLogic reporting. Instead, discrete pieces of information gleaned from the reports are shared only within the context of the situations outlined in 6.1.

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

Yes ☒ No ☐

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

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

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

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

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

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

The CopLogic system does not automatically check for accuracy. Instead, a reviewer from the I-TRU unit ensures that all fields are completed appropriately by those submitting the report before assigning a General Offense number and approving the report. If necessary information has not been included, the reviewer will contact the reporting party to obtain additional information before the data is electronically transferred into SPD's record management system.

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

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

DRAFT

7.0 Legal Obligations, Risks and Compliance

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

SPD's use of CopLogic is governed by legal requirements and policies as outlined in 3.1, 3.2, 3.3, 4.2, 4.6, and 5.3 of this SIR.

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

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

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.

Privacy risks may arise when information is collected about citizens, unrelated to a specific incident. These concerns are mitigated by the requirement that all SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

CopLogic is to be utilized under specific circumstances, as outlined in 3.2 above. Each report is reviewed to ensure both the accuracy of the report, as well as that it meets the requirements of online reporting (again, as outlined in 3.2 above).

Additionally, SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose." Additionally, officers must take care "when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them."

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Finally, see 5.3 for a detailed discussion about procedures related to noncompliance.

DRAFT

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 privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of CopLogic.

The largest privacy risk is the un-authorized release of reported information deemed private or offensive in the RCW. To mitigate this risk, the technology falls under the current SPD policies around dissemination of Department data and information reflected in 6.1.

DRAFT

8.0 Monitoring and Enforcement

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

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

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

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.

DRAFT

Financial Information

Purpose

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

1.0 Fiscal Impact

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

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
2010	2010	$33,000	N/A	N/A	SPD Budget

Notes:

N/A

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
$10,365	N/A	N/A	N/A	SPD Budget

Notes:

2018 Cost (after-tax) per the Contracts Renewal Log

DRAFT

1.3 Cost savings potential through use of the technology

SPD has collected data about CopLogic's effectiveness since 2012. The use of CopLogic has increased each year, and it saves numerous police hours. The data shows:

	Reports	Hours Saved	Money Saved
2012	7,652	11,478	$573,900.00
2013	9,527	14,290	$714,525.00
2014	12,575	18,862	$943,125.00
2015	12,365	18,547	$927,375.00
2016	13,379	20,068	$1,003,425.00
2017	14,356	21,534	$1,076,700.00
2018*	13,571	20,356	$1,017,825.00

*(2018 Data is calculated through the end of October.)

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

This question is not applicable.

DRAFT

Expertise and References

Purpose

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

1.0 Other Government References

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

Agency, municipality, etc.	Primary contact	Description of current use
King County Sheriff's Office	King County Sheriff's Office Communications Center Phone: (206) 296-3311 Fax: (206) 205-7956	King County uses CopLogic similarly to SPD, allowing the public to report specific non-emergency crimes to the Sheriff's Office.

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
N/A	N/A	N/A

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
Using Technology to Enhance the Relationship between Loss Prevention and Local Law Enforcement	Loss Prevention Magazine. (Sept-Oct. 2015)	LPPORTAL.COM
Citizen Perceptions of Online Crime Reporting Systems	*The Police Chief* 82 (June 2015): 48–52.	http://www.policechiefmagazine.org/citizen-perceptions-of-online-crime-reporting-systems/?ref=3e3a108ad4f36c878bb398b470385dcc

DRAFT

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

Purpose

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

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

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

Racial Equity Toolkit Overview

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

1.0 Set Outcomes

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

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

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

The potential impacts of this system on civil liberties are minimal. The risk with this technology is that this information could be disseminated for use in ways that could negatively impact peoples' civil liberties. CopLogic is an opt-in system; it is used only when an individual chooses to utilize it. However, individuals may enter personally-identifying information about third parties without providing notice to those individuals, and there is no immediate, systemic method to verify the accuracy of information that individuals provide about those third parties.

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

Additionally, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other data sharing.

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.

Because the information received through the CopLogic portal comes from community members there is a risk that racial or ethnicity-based biased information may be entered. All the information entered is screened by authorized and trained SPD personnel. SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

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

DRAFT

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.

N/A

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

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

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?

This technology is web-based and available for use by anyone within the city of Seattle with access to the internet, including mobile devices.

DRAFT

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

The Aspen Institute on Community Change defines *structural racism* as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity."[1] Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

No person outside of SPD has direct access to the CopLogic data. Data obtained by the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. See section 6.0 for more details about data sharing.

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?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. Because the use of this technology is an opt-in decision by its community users, the risks of improper or biased usage are limited. All information, once reviewed by authorized SPD employees, is electronically transferred into SPD's records management system. The SPD employees tasked with this review are bound by SPD policies pertaining to electronic communications, computer and data usage, and bias-based policing.

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.

The potential unintended consequences include individuals using the CopLogic system incorrectly in attempt to contact SPD (for example: when an emergency response is appropriate), and the dissemination of information through negligence or misconduct (intentional and unintentional). These are mitigated by documentation and function within the public website portal, review of entered information by SPD personnel, and the application of existing SPD policy.

[1] Aspen Institue Roundtable on Community Change. 2008. "Dismantling Structural Racism: A Racial Equity Theory of Change." Washington D.C.: The Aspen Institute.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

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

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

DRAFT

2.2 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.

DRAFT

2.3 Additional Department Meetings

Department	Date	Meeting Name	Number in Attendance	Description of Engagement
SPD	2/6/2019	South Seattle Crime Prevention Council	8	Deputy Chief GarthGreen presented the three SPD Group 2 surveillance technologies. One-page summaries and event flyer were distributed. DC GarthGreen and Policy Advisor fielded questions about the technologies. Attendees were directed to the public BKL event and seattle.gov/privacy to provide comment. No physical comment sheets were collected at the event.
SPD	2/7/2019	Fabulous Forum	40	Officer Ritter presented this meeting to approximately 40 members of the public. The public meeting flyer was distributed, paired with a brief introduction to the information around SPD's technologies currently open for public comment through 3-5. The Fabulous Forums are designed to provide valuable educational information to the public regarding a variety of topics ranging from the SPD's cultural history, to how the SPD works at enhancing the relationships between Seattle's police and population it serves, employment opportunities, hate crimes education, self defense and much more.
SPD	3/14/2019	East African Advisory Council	7	A brief presentation on SPD's group 2 surveillance technologies was given. One-page overviews of the technologies were handed out as resources in both English and translated into Somali. Attendees were directed to seattle.gov/privacy to provide comments on the technologies.
SPD	2/19/2019	NA		East African Community Senior Lunch
SPD	2/28/2019	East Precinct Advisory Council at Seattle University	17	A high level overview of the Surveillance Ordinance was provided. A brief introduction to SPD's group 2 technologies (CopLogic, CAD, 911 Logging Recorder) was also provided. One page overviews of each technology were distributed and attendees were directed to seattle.gov/privacy to provide public comment on the technology.

DRAFT

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

DRAFT

2.4 Scheduled Focus Group Meeting(s)

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

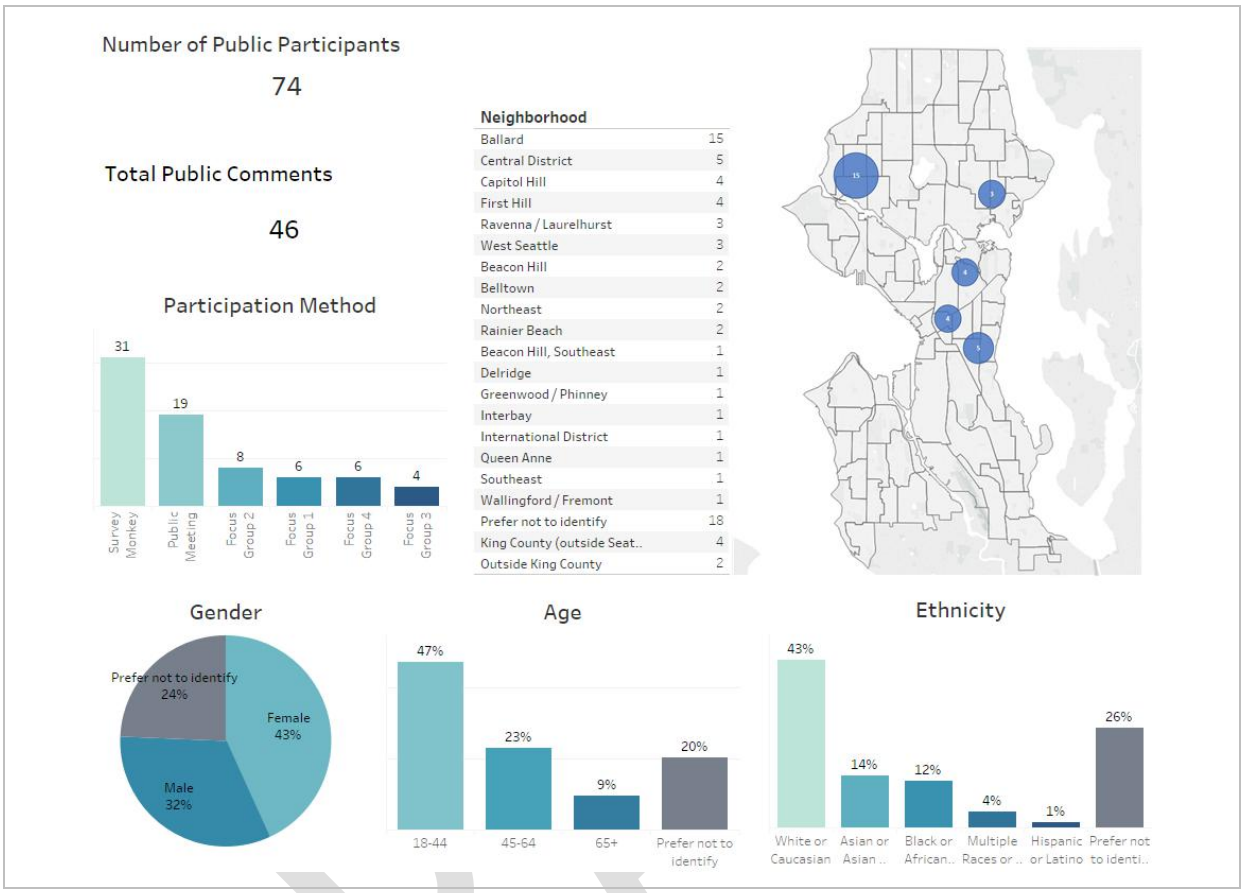
Meeting 4

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

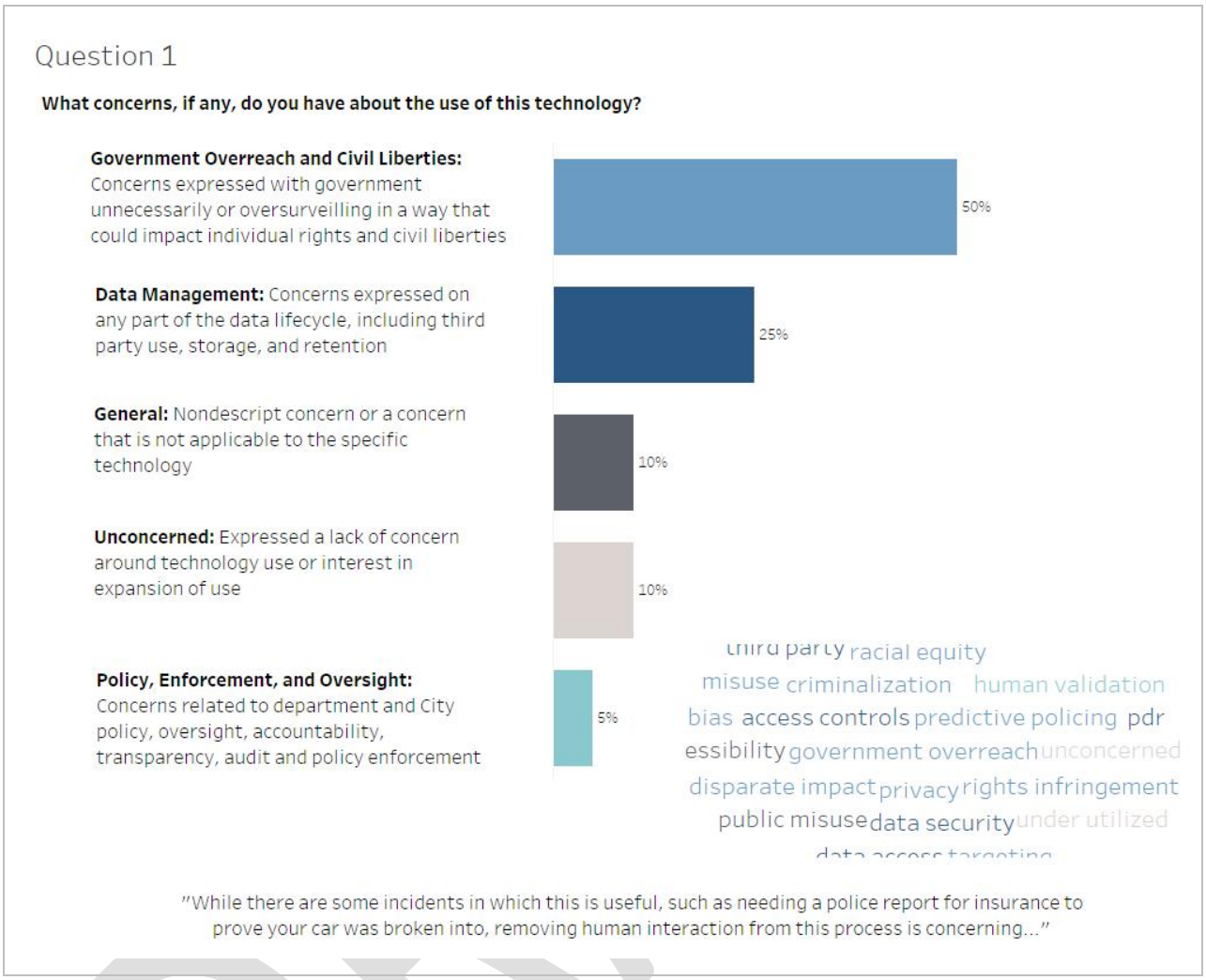
DRAFT

3.0 Public Comment Analysis

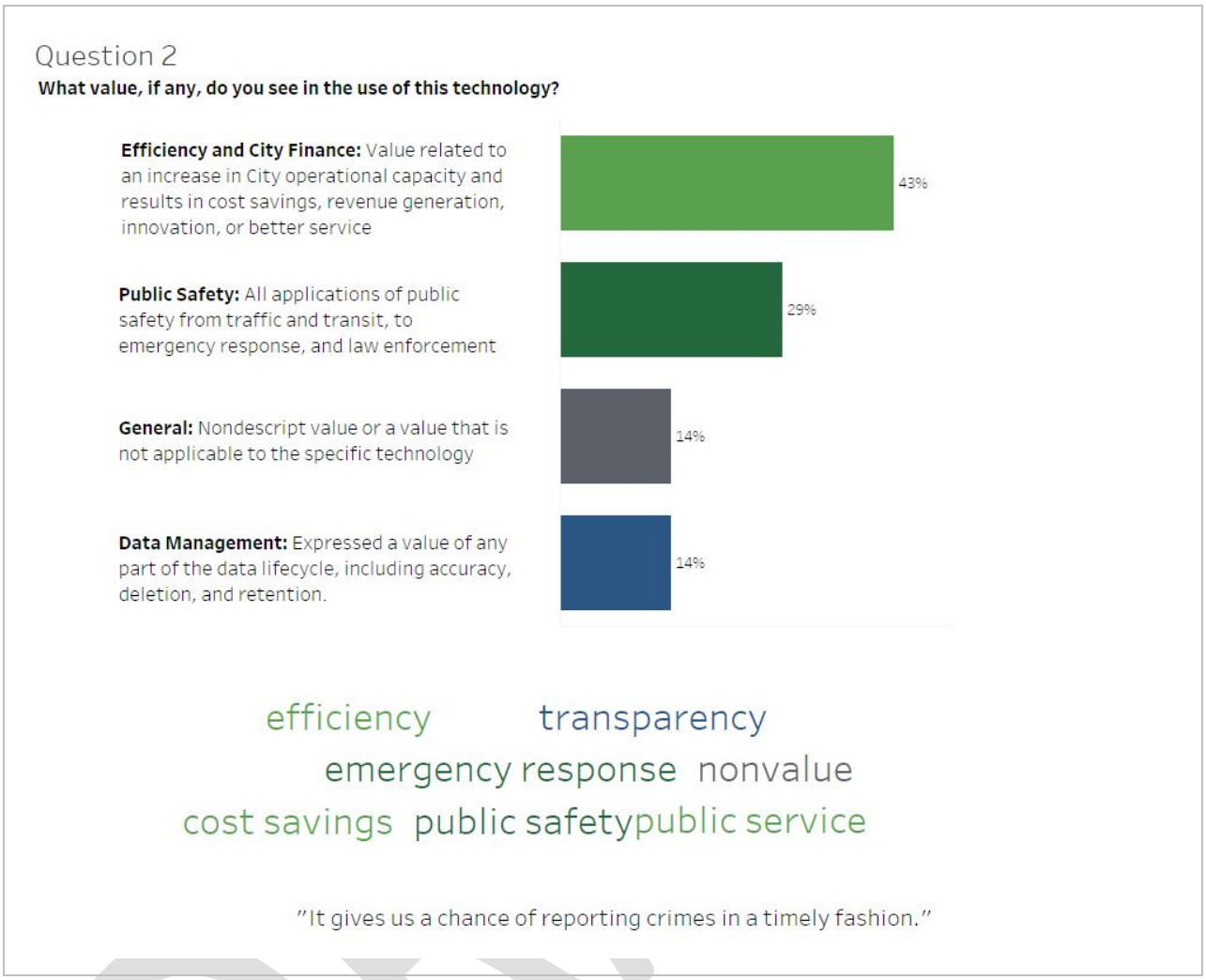
3.1 Summary of Response Volume and Demographic Information



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

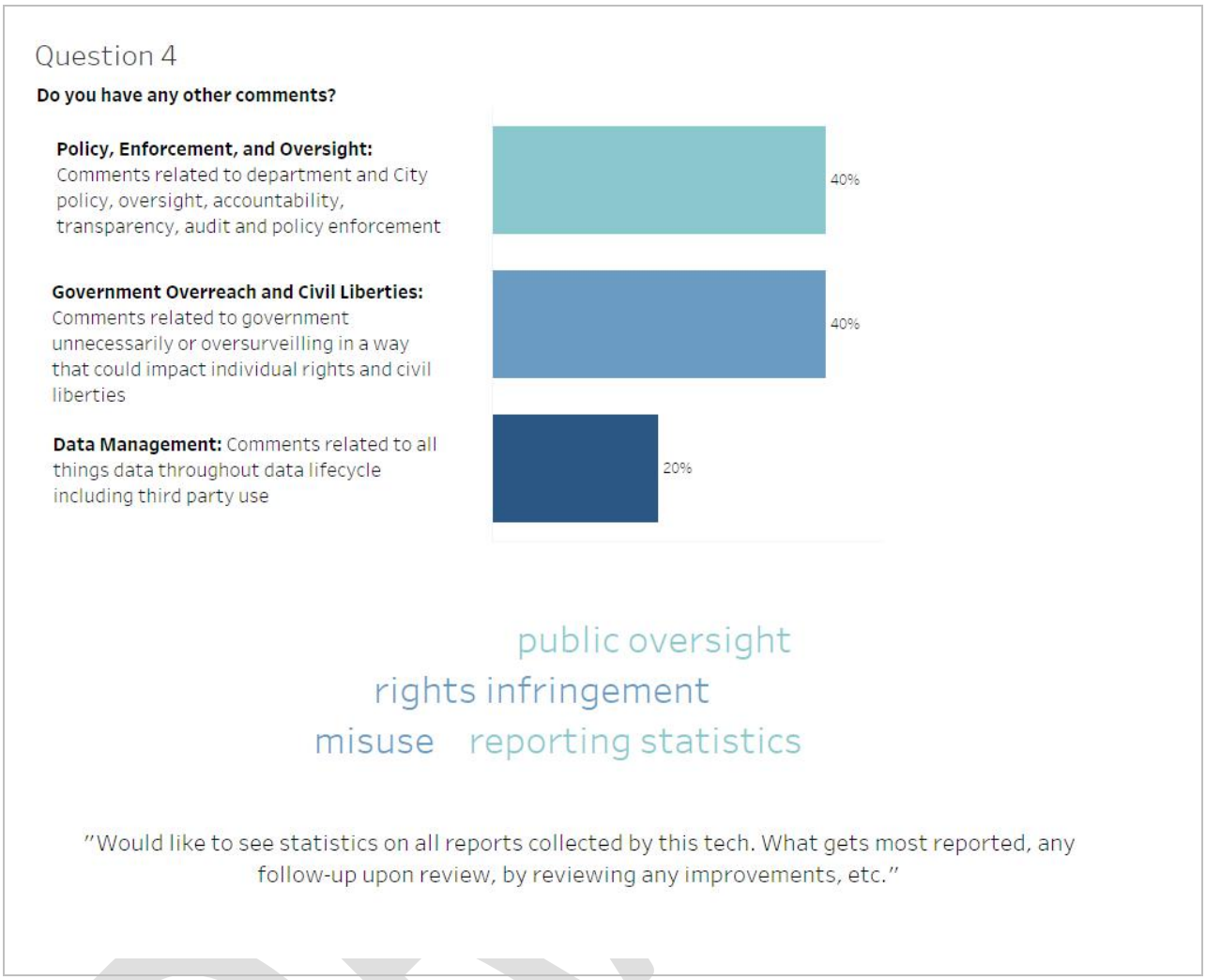


3.3 Question Two: What value, if any, do you see in the use of this technology?



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

3.5 Question Four: Do you have any other comments?



4.0 Equity Annual Reporting

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

The Seattle Police Department is currently working to finalize these metrics.

DRAFT

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

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

Working Group Privacy and Civil Liberties Assessment

Respond here.

DRAFT

CTO Response to Privacy and Civil Liberties Assessment

Respond here.

DRAFT

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

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

DRAFT

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

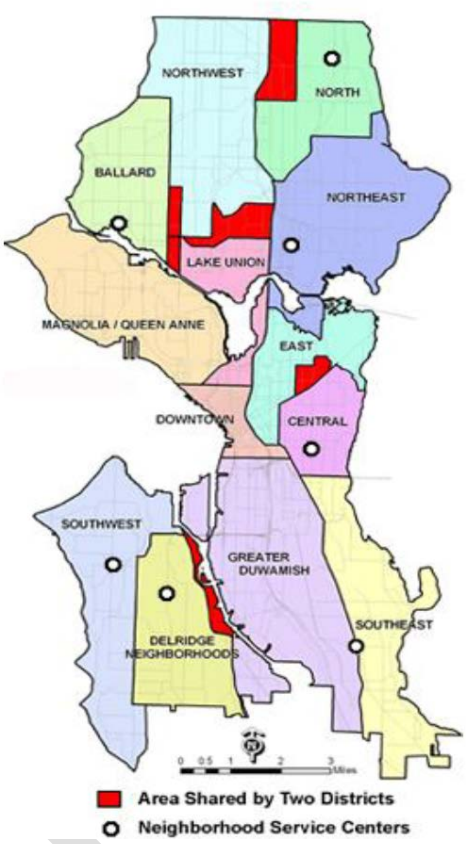
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

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



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

DRAFT

Appendix B: Meeting Notice(s)

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

- [x] 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
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [x] 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
- [x] 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
- [x] White
- [ ] Prefer not to Identify

Age

- [ ] Under 18
- [x] 18-44
- [ ] 45-64
- [ ] 65+
- [ ] Prefer not to identify

Gender

- [ ] Female
- [x] 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

DRAFT

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

DRAFT

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

☐ 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

SE KING COUNTY

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

DRAFT

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

DRAFT

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)

DRAFT

- 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?

DRAFT

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?

- 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.

DRAFT

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

DRAFT

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

DRAFT

- 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

DRAFT

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?
    0. 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
    1. 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.
    2.
2. What value do you think this brings to our city?
    0. 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?
    0. 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
    1. 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

DRAFT

- 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?
    0. 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?
    0. 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)
    0. Who opted out was it home owners?
    1. 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?
    2. 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
    3. 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

DRAFT

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

DRAFT

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?

DRAFT

- 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

DRAFT

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?

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?

DRAFT

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.

DRAFT

- Dejar de construir tanto.
- Rediseño de calles ayudaría flujo de tráfico.
- El rediseñar las vías servirá para las futuras generaciones.

DRAFT

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

Entre Hermanos

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? ●

DRAFT

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

DRAFT

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.

DRAFT

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.

DRAFT

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

DRAFT

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.

DRAFT

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

DRAFT

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.

DRAFT

- 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.

DRAFT

- 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.

DRAFT

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.

DRAFT

- 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

DRAFT

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.

DRAFT

- 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

DRAFT

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

DRAFT

- 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

DRAFT

Appendix E: All Comments Received from Members of the Public

ID: 10617696279

Submitted Through: Survey Monkey

Date: 3/25/2019 1:32:51 PM

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

SPD: CopLogic

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

Higher Concerns: 1) Software-as-a-Service (SaaS) solution instead of locally (Seattle IT/SPD) hosting CopLogic. Since this is hosted/managed by LexisNexis, LexisNexis has control of the data (either for legal usage of the data as outlined in the contract with them or for possible exposure if they were to have a security breach). 2) Data retention period for data entered into CopLogic isn't specified in the SIR or the IT/LexisNexis contract. It is unclear what happens to a report on the CopLogic side after it is submitted to the SPD RMS by an officer. Is it automatically deleted from CopLogic then? More broadly, regardless on whether a report is submitted to the SPD RMS, how long is that data retained in CopLogic? 3) No special data handling/security/privacy requirements for "personal information" are placed on LexisNexis. The Seattle IT/LexisNexis contract defines "personal information" (and with a reasonably good definition from the privacy side) but the contract does NOT go on to state any special requirements for "personal information". Per the contract, LexisNexis can handle "personal information" in the same manner as it handles "city data". 4) Citizens with lower technical skills, citizens without Internet access, and/or citizens with confusing/expensive Internet plans may be unable or dissuaded from submitting reports to SPD. People who are most likely to fall into those categories are likely already disadvantaged in other areas of life as well (older citizens, minorities, low-income, disabled, etc.). Lesser Concerns: 1) No 2-step-verification/2-factor-authentication (2SV/2FA) for officer login to CopLogic, but, per SPD, the officer-login side of CopLogic is not Internet-facing (you have to be on SPD's network to access it) so the risk is reduced. 2) Per the response at the SIR tech fair, CopLogic's access back to the SPD RMS is one-way, write-only. However, it is unclear how credentials are scoped and if that means CopLogic's RMS creds could be used to write to any arbitrary records in the SPD RMS or if it can only impact CopLogic-generated records in the RMS. That being said, even if the creds have overly scoped permissions, this would be a security issue, not a privacy issue (since the creds supposedly don't have read access). 3) Email addresses is a required field when submitting a report via CopLogic, whereas it would be optional for an in-person report. However, at least the Seattle IT/LexisNexis contract prohibits the use of the data entered via CopLogic from being used for targeted advertising. 4) Accidental release of personal information of citizens via PRA requests. However, per the SPD rep at the SIR tech fair, SPD redacts names, addresses, phone numbers, building access codes, etc. as a matter of practice when responding to PRA requests, so the likelihood of release seems low here. 5) From the draft SIR 6.3.1, "Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content." This sentence was unclear to me, specifically, for example, if SPD released the records for a non-citizen to that non-citizen, would that then mean SPD could freely

DRAFT

share those same records with ICE? But the SPD rep at the tech fair, said that SPD would only ever release records they are authorized to do so (their behavior doesn't change post-PRA-release), the sentence in the SIR was simply explaining that SPD isn't responsible for what happens with the data that is released (the receiver of that data could further share that data in ways that SPD would not).

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

It is likely significantly more convenient to most citizens. It likely also reduces the number of officers needed.

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

1) LexisNexis Desk Officer Reporting System (DORS) aka CopLogic apparently supports a locally hosted option ("You may also choose to host the application internally; it's completely up to you!" taken from: https://secure.coplogic.com/products/dors-overview.shtml). Assuming that the locally hosted option is entirely self-contained (that is, it's not just the web form that is locally hosted, but also the backend data storage for CopLogic), then it would be better to for the City of Seattle (SPD/IT) to locally host it instead, since there would be no exposure of citizen's information to a third-party just to report simple crimes. This would improve citizen's privacy and reduce the risk if there was a LexisNexis security breach. 2) Data retention is another issue. Neither the draft SIR nor the IT/LexisNexis contract specify the data retention policy for data on the CopLogic side (not the SPD RMS). What happens to a CopLogic report after an officer submits it to the SPD RMS? How long does LexisNexis store the reports? What's the lifecycle for reports that are found inadequate/invalid by the officer? Does the officer delete them? Do reports in CopLogic "expire" and therefore get auto-deleted after some length of time? What length of time? 3) The Seattle IT/LexisNexis contract should be altered to actually place specific data handling/security/privacy requirements on LexisNexis for "personal information" entered in via CopLogic. 4) When SPD people or systems direct citizens to use online reporting, it should be made clear that they aren't required to do so (if they are unable or unwilling to report online they should still be able to report directly). This is to ensure disadvantaged populations still have a mechanism for reporting minor crimes.

Do you have any other comments?

It is unclear to the public what vendor SPD uses for their RMS; and what (if any) additional data processing and/or data analysis capabilities are available on top of that. The SPD RMS should go through similar scrutiny by the public and the council.

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

It would be helpful if once initial public release of the draft SIRs happened, that within each SIR there was a version history noting what has changed over time (so first release to the public = version 1; say a draft SIR has a contract(s) added, then the version history table says versions 2 noting the date & changes that were the added contracts in whichever Appendix).

DRAFT

ID: 10617457428

Submitted Through: Survey Monkey

Date: 3/25/2019 11:57:26 AM

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

SPD: CopLogic

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

No concerns except that we need this because we're desperately short of police officers.

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

It gives us a chance of reporting crimes in a timely fashion.

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

It saves a lot of money.

Do you have any other comments?

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

Are they planning to increase the dollar value of what you can report using this? It seems low.

ID: 11

Submitted Through: Focus Group

Date: 2/28/2019

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

SPD: CopLogic

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

The different types of communities that do not have access (whether linguistic/ rapport with police department) to the technology. Not equal playing field. The anonymous remote reporting may lead to an increase in religious profiling/targeting of criminalized identities for harmless behavior. SPD's relationship with the IDF is just one example of a poor rapport of the department with more marginalizaed communities (militarization of the police).

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?

Do you have any other comments?

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

DRAFT

ID: 8

Submitted Through: Focus Group

Date: 2/28/2019

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

SPD: CopLogic

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

targeting of people of color - who have been seen/depicted as more intimidating -- requires individual perceptions of others (ex: harassment)

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

saving time, person power, and money especially with things such as car break ins, hit and run

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

The validity of reports that are coming through. How do we ensure reports are not hurting communities of color. Crime-mapping which can happen with this technology

Do you have any other comments?

this can target locations that have been frequented by communities of color (masjid, gathering spaces, grocery stores, community centers)

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

what happens with data, how long is it kept in their systems

ID: 6

Submitted Through: Focus Group

Date: 2/27/2019

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

SPD: CopLogic

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

Not available in other languages -- not accessible form is a little confusing and long

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

saves time on the department side. Makes it easier to report on individual/community member's time

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

generally, making it more accessible to more community members

Do you have any other comments?

DRAFT

Would like to see statistics on all reports collected by this tech. What gets most reported, any follow-up upon review, by reviewing any improvements, etc.

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

ID: 5

Submitted Through: Focus Group

Date: 2/27/2019

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

SPD: CopLogic

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

My Concern: will data be safe kept.

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

convenience and effective and accountable

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

allow enough trial times - testing times- before applying

Do you have any other comments?

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

Again, how to keep data safe

ID: 2

Submitted Through: Focus Group

Date: 2/28/2019

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

SPD: CopLogic

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

People misusing/abusing the resource; can the number of reports become so excessive to the point where they can't all properly be tended to?

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

Great for accessibility for folks who can't report in person or over the phone. May be easier to convey information as opposed to talking with cops (who I've had multiple negative experiences with reporting crimes)

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

DRAFT

See number 1.

Do you have any other comments?

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

ID: 10549555511

Submitted Through: Survey Monkey

Date: 2/22/2019 3:28:12 PM

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

SPD: CopLogic

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

While there are some incidents in which this is useful, such as needing a police report for insurance to prove your car was broken into, removing human interaction from this process is concerning in its potential to embolden people to report "suspicious activity" without review, as online reports are only available for incidents in which no police follow up is needed or possible. I see the potential for city residents to act upon biases and equate race, religion, or other aspects of identity with crime or suspicious activity, and for these reports to go without verification or investigation. Consequently, I have concerns for increased police presence in neighborhoods deemed to be high-crime or suspicious, creating a vicious circle of continued mistrust between the police and community members.

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

Only for incidents with absolutely no consequence for other people, like reporting a car break in for insurance purposes.

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

I would like City Council to consider the potential consequences of this reporting tool and focus more resources toward improving community trust

Do you have any other comments?

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

ID: 10533827008

Submitted Through: Survey Monkey

Date: 2/15/2019 3:11:01 PM

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

SPD: CopLogic

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

DRAFT

This will be used to disproportionately report the homeless and people of color for existing in a place where someone feels uncomfortable

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

None whatsoever

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

Quit while you're ahead and put that money towards community welfare projects, affordable housing, and helping the homeless and addicted

Do you have any other comments?

Tax Amazon

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

DRAFT

Appendix F: Department Responses to Public Inquiries

Community Comment Responses:

FG	2/28/2019	SPD: CopLogic	What happens with data? How long is it kept in their systems?

Reports that are generated in the CopLogic system are auto-deleted from the LexisNexis servers after 120 days per the CopLogic system configuration. Reports that are rejected by SPD employees after their review are deleted immediately.

FG	2/27/2019	SPD: CopLogic	How do we keep the data safe?

The portal SPD staff use to view, approve, and import reports from CopLogic into SPD's records management system requires "Triple Lock" authentication. "Triple Lock" means that each staff member has a unique username and password, IP restricted logins (they must be authenticated on the SPD network) and use a private URL to log into the system. Only certain CJIS certified employees who have roles associated with the CopLogic online reporting process are given this access. Additionally, the LexisNexis CopLogic system is CJIS Complaint and per the contract with LexisNexis, the City requires the vendor to have the system tested for security vulnerabilities articulated in the industry standard OWASP Top-10.

FG	2/28/2019	SPD: CopLogic	How do we ensure reports are not hurting communities of color?

Because the use of this technology is an opt-in decision by its community users and crimes with known or describable suspects are not reportable through CopLogic, the risks of improper or biased usage are limited. This system does not allow for reports of crimes with known or describable suspects. All information, once reviewed by authorized SPD employees, is electronically transferred into SPD's records management system. The SPD employees tasked with this review are bound by SPD policies pertaining to electronic communications, computer and data usage, and bias-based policing. Additionally, all reports that can be made through the online reporting system can also be made utilizing other methods including by telephone.

FG	2/28/2019	SPD: CopLogic	Can the number of reports become so excessive to the point where they can't all be properly tended to?

All requests for service, no matter what the method for making that request, are responded to by SPD. The online reporting tool, CopLogic, allows for certain non-emergency requests with no known or describable suspect to be reviewed by SPD officers in an efficient manner that frees up patrol officers allowing them to respond faster to requests in a timely fashion.

FG	2/21/2019	SPD: CopLogic	What is the usefulness of the information that is not followed up on? And how does it help the people it is actually serving?

DRAFT

All reports made through the CopLogic online reporting system are reviewed by SPD officers. Often a report is made even when there is little that an SPD officer can act on, for example when a property theft happens and there is no known or describable suspect. An insurance claim may still require that a police report be filed and the CopLogic system allows community members to file this report in a convenient way. Community members wishing to speak with SPD employees to make their report may still initiate their report over the phone or in person at a precinct.

FG	2/21/2019	SPD: CopLogic	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 that already feels threaten and criminalize by communities?

Because the use of this technology is an opt-in decision by its community users and crimes with known or describable suspects are not reportable through CopLogic, the risks of improper or biased usage are limited. This system does not allow for reports of crimes with known or describable suspects. All information, once reviewed by authorized SPD employees, is electronically transferred into SPD's records management system. The SPD employees tasked with this review are bound by SPD policies pertaining bias-based policing. Additionally, all reports that can be made through the online reporting system can also be made utilizing other methods including by telephone.

FOLS FG	2/27/2019	SPD: CopLogic	Will they keep the data safe on coplogic?

The portal SPD staff use to view, approve, and import reports from CopLogic into SPD's records management system requires "Triple Lock" authentication. "Triple Lock" means that each staff member has a unique username and password, IP restricted logins (they must be authenticated on the SPD network) and use a private URL to log into the system. Only certain CJIS certified employees who have roles associated with the CopLogic online reporting process are given this access. Additionally, the LexisNexis CopLogic system is CJIS Complaint and per the contract with LexisNexis, the City requires the vendor to have the system tested for security vulnerabilities articulated in the industry standard OWASP Top-10. The Consultant Agreement limits the vendor's (LexisNexis) use and storage of all information collected by or on behalf of the City to only purposes used for providing the service in the CopLogic contact and Consultant Agreement. They are prohibited from using City data or personal information to engage or enable another party to engage in marketing or targeted advertising. Additionally, no access or information shall be provided to any employee or agent of any federal immigration agency without prior review and consent of the City.

FOLS FG	2/27/2019	SPD: CopLogic	Can the data be hacked?

DRAFT

The portal SPD staff use to view, approve, and import reports from CopLogic into SPD's records management system requires "Triple Lock" authentication. "Triple Lock" means that each staff member has a unique username and password, IP restricted logins (they must be authenticated on the SPD network) and use a private URL to log into the system. Only certain CJIS certified employees who have roles associated with the CopLogic online reporting process are given this access. Additionally, the LexisNexis CopLogic system is CJIS Complaint and per the contract with LexisNexis, the City requires the vendor to have the system tested for security vulnerabilities articulated in the industry standard OWASP Top-10.

FOLS FG	2/27/2019	SPD: CopLogic	what if you report your neighbour and your neighbor hacks the system and find out?

This system does not allow for reports of crimes with known or describable suspects, therefore you would not be able to use the CopLogic online reporting system to report a crime committed by a neighbor. Please contact 9-1-1, the SPD non-emergency number, or your local SPD precinct to file a report involving a known suspect.

FOLS FG	2/27/2019	SPD: CopLogic	What is the money amount limit for coplogic/why is there a limit for coplogic?

Theft of property valued at less than $500 may be reported using CopLogic. The online reporting tool is designed to allow community members to report certain low-level property crimes only. When the value of stolen property exceeds $500 it is more appropriate for an officer to respond in person to take the crime report.

FOLS FG	2/27/2019	SPD: CopLogic	Is there an option that someone and report a crime for someone else?

For community users who are not part of the retail users program, there is not an option to use CopLogic online reporting to report a crime for someone else. If a community member needs to make a report on behalf of another person, they will need to contact SPD either by phone or in person.

FOLS FG	2/27/2019	SPD: CopLogic	Is there resources to support these technologies? Is there translations so that it is accessible for everyone? Will this accommodate everyone?

DRAFT

With the support of Seattle IT, CopLogic benefits both the community and the Seattle Police Department by freeing resources in the 9-1-1 center, eliminating the need for patrol officers to respond in person to take some crime reports. The CopLogic online reporting tool, as with the SPD and City of Seattle websites, are not currently available in translations. Community members who need to request services need to contact SPD by phone or in person for translation services.

FOLS FG	2/27/2019	SPD: CopLogic	How will other people know of the technology if they can't come to focus group meetings? Such as flyers? Social media?

Links to the CopLogic online reporting system are prominently displayed on the Seattle Police website and is promoted on other SPD social media outlets such as Facebook, Twitter, and the Seattle Police Blotter. Additionally, callers to the non-emergency number are informed about online reporting and given the option to make their report online.

DRAFT

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

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)

ACLU
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

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.

DRAFT

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.

DRAFT

Appendix I: Supporting Policy Documentation

Management Control Agreement

Management Control Agreement Between
Seattle Police Department and
City of Seattle Information Technology Department

The City of Seattle Police Department ("SPD"), also referred to as the Criminal Justice Agency, and the City of seattle Information Technology Department (''ITD") are departments of the municipal corporation of the City of Seattle.

Pursuant to Seattle Municipal Code ("SMC") 3.23, ITD provides information technology systems, services, and support to SPD and is therefore required to support, enable, enforce, and comply with SPD policy requirements, including the FBI's Criminal Justice Information Services ("CJIS") Security Policy.

Pursuant to the CJIS Security Policy, it is agreed that with respect to the administration of computer systems, network infrastructure, devices, and services interfacing directly or indirectly with A Central Computerized Enforcement System ("ACCESS") for the exchange of criminal history/criminal justice information, the Criminal Justice Agency shall have the authority, via managed control, to set and enforce:

Priorities that guarantee the priority, integrity, and availability of service needed by the criminal justice community.

Requirements for the selection, authorization, supervision, and termination of physical and logical access to Criminal Justice Information ("CJI").

Policy governing operation of justice systems, data, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a communications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Restriction of unauthorized physical and logical access to or use of systems and equipment accessing CJI.

Compliance with all rules and regulations of the Criminal Justice Agency policies and CJIS Security Policy in the operation of, access to, or control over any CJI systems, data, or infrastructure.

The responsibility for management control of the criminal justice function remains solely with the Criminal Justice Agency. ITD will not enter into any agreements or allow any access to, possession of, or control over any SPD CJI systems, data, or infrastructure

DRAFT

without explicit authorization from at least one SPD Authorized Party. SPD Authorized Parties must be SPD employees and include:
Chief of Police
Chief Operating Officer

This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, administration, and maintenance of any Criminal Justice Agency system to include NCIC Programs that may be subsequently designed and/or implemented within the Criminal Justice Agency.

Additional agreements, such as a Memorandum of Agreements, Service Level Agreements, and/or Continuity Plans, may be established and maintained to further delineate, define, and assign roles, responsibilities, and requirements of and agreements between SPD and ITD, and other City of Seattle Departments and/or agencies.

Tracye Cantrell
Tracye Cantrell
Interim Chief Technology Officer
Seattle Information Technology Department

Date: Feb 2, 2018

Carmen Best
Carmen Best
Interim Chief of Police
Seattle Police Department

Date: 2-7-2018

Reference: CJIS Security Policy, Version 5.5, dated June 1, 2016 (CJISD-ITS-DOC-08140-5 .5)

IT Support Services for City Technology

Engineering and Operations

This division designs, implements, operates, and supports technology solutions and resources in accordance with city wide architecture and governance. Responsibilities for this division include:

- Primary communications networks that provide public safety and constituent access to and from City government; the telephone system, the data network, and Public Safety Radio System. Responsible for sustaining all three systems operating as close to 100% availability as possible 24 hours a day, seven days a week.
- Design, acquisition, installation, maintenance, repair and management of fiber optic cables on behalf of City departments and approximately 20 other local, state and federal agencies.
- Procurement requests, allocation, operation and maintenance of city wide and departmental servers, virtual enterprise computing and SAN storage environments for large scale mission critical applications in a secure, reliable, 24/7 production environment for enterprise computing.
- Allocation, operation and maintenance of enterprise level services like messaging services, web access, file sharing, user management and remote access solutions.
- Collaborate with Enterprise Architecture team to develop standards for information technology equipment and software.
- Service Desk and technical support services for City's computers, peripherals, electronic devices and mobile device management.
- Centralized IT asset management to include research, procurement request, surplus and asset transfer.
- Facility management for a reliable production computing environment to the City departments.
- Support for other enterprise services and tools.

Compute System Technologies

This team manages the operations and maintenance of computing infrastructure, including servers, storage, backup and recovery, and enterprise support systems (e.g., Active Directory, VPN, etc.). The team is also responsible for safeguarding systems and data by performing required security patches, updates, and backups to ensure systems operate at as close to 100% availability as possible 24x7. Units within this group include:

Systems Operations. The team is focused on delivering the computing environment across multiple departments. The team has technical expertise to design, integrate, and operate a secure, reliable computing environment. Key technologies include Windows, Solaris, IBM AIX, and Linux.

Enterprise Services. Enterprise Services (ES) are large scale infrastructure and application services used by the City of Seattle end user community. This includes both SaaS and NGDC hosted infrastructure and application services. The team is responsible for EA vendor management, system administration, upgrades and technical support. Key technologies includes Microsoft Active Directory (AD), Distributed File System (DFS), Exchange Online, Office 365 and SharePoint Online infrastructure.

Infrastructure Tools. The team provides a single focus for the design, planning, deployment and maintenance of standard enterprise infrastructure monitoring and management tools. This

DRAFT

includes system performance (Solarwinds, SCOM), configuration management (SCCM, WSUS), and monitoring and system management (Trend Micro, CRM, Vipre).

Virtual and Data Infrastructure. This team engineers and operates reliable, flexible, performant virtualized Windows, UNIX and Linux platforms and their related technologies in direct support of critical business applications. Key technologies include Solaris, Unix, Linux, Windows, and vmWare, and the associated virtualization Nutanix, IBM LPAR, and Solaris hardware.

The team also engineers and operates reliable, flexible, performant storage and data protection solutions to host and protect critical business data of all types, leveraging SAN, NAS, object, and cloud technologies. Key technologies include Dell Compellent, Quantum, Hitachi, NetApp, Cloud storage, Brocade fiber channel switching, and Commvault.

Network And Communications Technologies

This team is responsible for designing, installing, operating, and maintaining data, voice, radio, fiber optic, and structured cabling infrastructure that integrates with other technologies to provide access to resources used by City departments and the public we serve. Units within this group include:

Network Engineering & Operations. The Network Services team engineers, operates and maintains the City's data network, including data center core networks, the internet perimeter, the network backbone, and local area networks that support systems and users across the City. This group designs, acquires, installs, maintains, repairs, and manages an enterprise data network that aligns with City architectures and standards. This group also participates in development of those standards and provides tier 2 and 3 end user support. This team supports technologies that include routing, switching, load balancing, enterprise Wi-Fi, DNS/DHCP/NTP, and network security (including firewalls, VPN appliances, certificate infrastructure, network access control, and web filtering.)

Telecommunication Engineering & Operations. The Telecommunications Services team engineers, operates, and maintains a highly-reliable enterprise telephone and contact center infrastructure. This group supports end user move and change activity and provides tier 2 and 3 support. The Telecommunication Services team acquires, installs, maintains, and repairs telecommunications equipment and manages commercial telephony circuits. It supports technologies that include VoIP, circuit-switched telephony, voice mail, contact center services (including call routing scripts), audio conference bridges, commercial telephony services, SONET, and WDM.

Radio & Communications Infrastructure. This team delivers radio services for public safety and other government departments. It provides extremely reliable infrastructure and support for end user mobile and portable radio equipment. The group installs and maintains communications equipment inside 911 dispatch centers and City vehicles, with primary support to SPD and SFD. The team also supports regional planning, maintenance, interoperability testing, and projects (including PSERN and Washington OneNet) in partnership with other local, state, and federal agencies. This team also designs, acquires, installs, maintains, repairs, and manages in-building structured cabling systems and outside plant fiber optic and copper cable infrastructure for the City and approximately 20 external public agency partners. Technologies include trunked and conventional land mobile radio, microwave radio and other wireless communications systems (including point-to-multipoint and mesh networks,)

DRAFT

distributed antenna systems, routing/MPLS, DS3/T1/DACS, outside plant cable infrastructure (including fiber and copper,) and structured cabling infrastructure.

End User Support

This team is responsible for providing a single point of contact for IT technical support, trouble ticket and service request resolution and referral services to other IT workgroups, and for communication for all changes, patches, upgrades and standards changes. The team is also responsible for providing technical support for the City's desktop computers, peripherals, electronic devices and mobile devices. Units within this group include:

Service Desk. The Service Desk team provides a single point of contact for Seattle IT services, promptly resolving incidents and service requests when first contacted whenever possible, escalating issues accurately and efficiently, and keeping users and partners aware of service status and changes.

Device Support. This team provides direct customer support for end user computing to all departments within the City and tier 2 escalation support and management of centralized end user computing applications and hardware. requests.

Device Engineering. This team engineers and deploys software packages for end user applications, device drivers, patches, security updates and custom packages as required. This team evaluates and recommends hardware and software for end user standards. In addition, this team provides tier 3 escalation support and management of centralized end user computing applications and hardware.

Asset Management. This team is responsible tracking and inventory controls for city wide IT assets including desktops, laptops, printers, servers, switches, and miscellaneous Information Technology infrastructure. In addition to inventory control, the team will be forecasting replacement cycles for equipment based on City standards to promote a stable computing environment.

IT Operations Support

The IT Operations Support team is responsible for management of Information Technology facilities (including data centers and communications equipment rooms), and installation and cabling equipment within those facilities. This team provides the enterprise Network Operations Center (NOC) that monitors alerts, performs initial incident analysis, dispatches tier 2 and 3 technical support, and provides initial incident communication for network infrastructure and computing systems managed by Engineering and Operations. Units within this group include:

Installation Management. This team installs networking and computing equipment in data centers, communications rooms and wiring closets; installs and maintains network cabling within data centers and equipment rooms according to City standards; and supports repair and end user move and change activity (including telephone move projects).

IT Operations Center. This team manages facilities which support City computing and communications services. This includes managing access to facilities, coordinating vendors, maintaining records (including data center inventory management), and, where

DRAFT

applicable, monitoring facility systems (including CRUs, fire alarms, water detection sensors, UPS systems, and power consumption). This team also staffs the NOC that monitors alerts from network infrastructure and computing systems, performs initial problem analysis, dispatches appropriate tier 2 and 3 technical support team(s), and provides initial incident communication.

Application Services

This division designs, develops, integrates, implements, and supports application solutions in accordance with city wide architecture and governance. Its teams are organized to support business functions or service groups**.** The integration of application services will be completed gradually in 2017, with details of the organization and integration process still under development.

Applications

These teams will provide development and support for applications that include customer relationship management, billing, finance, human resources, work and asset management and records management.

Shared Platforms

These teams will provide development and support for applications that include engineering, spatial analysis, business intelligence, analytics, SharePoint Online and document management.

Cross Platform Services

These teams will provide support to application teams, including quality assurance, change control, database administration, integration services, and access management activities.

DRAFT

Data Retention

Exported report will be auto-deleted after this many days	120	(blank or 0 means exported report will not be auto-deleted)
Approved report will be auto-deleted after this many days	120	(blank or 0 means approved report will not be auto-deleted)
Pending report will be auto-rejected after this many days	30	(blank or 0 means pending report will not be auto-rejected)
Rejected report will be auto-deleted after this many days	120	

DRAFT

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

DRAFT

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

DRAFT

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • **Audio recording devices**: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • **Camera systems**: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • **Tracking devices**: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6

DRAFT

Technology	Description	Proposed Review Order
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
Remotely Operated Vehicles (ROVs)	These are SPD non-recording ROVs/robots used by Arson/Bomb Unit to safely approach suspected explosives, by Harbor Unit to detect drowning victims, vehicles, or other submerged items, and by SWAT in tactical situations to assess dangerous situations from a safe, remote location.	8
911 Logging Recorder	System providing networked access to the logged telephony and radio voice recordings of the 911 center.	9
Computer, cellphone and mobile device extraction tools	Forensics tool used with consent of phone/device owner or pursuant to a warrant to acquire, decode, and analyze data from smartphones, tablets, portable GPS device, desktop and laptop computers.	10
Video Recording Systems	These systems are to record events that take place in a Blood Alcohol Concentration (BAC) Room, holding cells, interview, lineup, and polygraph rooms recording systems.	11
Washington State Patrol (WSP) Aircraft	Provides statewide aerial enforcement, rapid response, airborne assessments of incidents, and transportation services in support of the Patrol's public safety mission. WSP Aviation currently manages seven aircraft equipped with FLIR cameras. SPD requests support as needed from WSP aircraft.	12
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14

DRAFT

Technology	Description	Proposed Review Order
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
Parking Enforcement Systems	Several applications are linked together to comprise the enforcement system and used with ALPR for issuing parking citations. This is in support of enforcing the Scofflaw Ordinance SMC 11.35.	16
Situational Awareness Cameras Without Recording	Non-recording cameras that allow officers to observe around corners or other areas during tactical operations where officers need to see the situation before entering a building, floor or room. These may be rolled, tossed, lowered or throw into an area, attached to a hand-held pole and extended around a corner or into an area. Smaller cameras may be rolled under a doorway. The cameras contain wireless transmitters that convey images to officers.	17
Crash Data Retrieval	Tool that allows a Collision Reconstructionist investigating vehicle crashes the opportunity to image data stored in the vehicle's airbag control module. This is done for a vehicle that has been in a crash and is used with consent or search warrant.	18
Maltego	An interactive data mining tool that renders graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the internet.	19

Please let me know if you have any questions.

Thank you,

Michael