

2019 Surveillance Impact Report

Computer-Aided Dispatch (CAD)

Seattle Police Department

Table of Contents

Submitting Department Memo	3
Surveillance Impact Report (“SIR”) overview	4
Privacy Impact Assessment	5
Financial Information.....	25
Expertise and References.....	27
Racial Equity Toolkit (“RET”) and Engagement for Public Comment Worksheet	28
Privacy and Civil Liberties Assessment	40
CTO Response to Privacy and Civil Liberties Assessment	41
Appendix A: Glossary	43
Appendix B: Meeting Notice(s) (PDF)	45
Appendix C: Meeting Sign-in Sheet(s) (PDF)	46
Appendix D: Department of Neighborhood Focus Group Notes	47
Appendix E: All Comments Received from Members of the Public	79
Appendix F: Department Responses to Public Inquiries(PDF)	84
Appendix G: Letters from Organizations or Commissions(PDF)	85
Appendix H: Comment Analysis Methodology	86
Appendix I: Supporting Policy Documentation	89
Appendix J: CTO Notification of Surveillance Technology.....	108

Submitting Department Memo

Description

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

Purpose

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

Benefits to the Public

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

Privacy and Civil Liberties Considerations

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

Summary

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

Surveillance Impact Report (“SIR”) overview

About the Surveillance Ordinance

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

How this Document is Completed

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

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

Surveillance Ordinance Review Process

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

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

Privacy Impact Assessment

Purpose

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

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

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

1.0 Abstract

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

The Seattle Police Department's 9-1-1 Center is the primary Public Safety Answering Point (PSAP) for emergency 9-1-1 calls placed within the City of Seattle. Computer Aided Dispatch (CAD) is a software package utilized by the Seattle Police Department's 9-1-1 Center. It assists 9-1-1 Center call takers and dispatchers with receiving requests for police services, collecting information from 9-1-1 callers, and providing dispatchers with real-time patrol unit availability so dispatchers may dispatch appropriate patrol resources to requests for police service. CAD software also enables real-time documentation of the Seattle Police Department's response to calls for service, including relevant information obtained by responding officers.

The Seattle Police 9-1-1 Center, staffed 24 hours per day, 365 days per year, receives approximately 900,000 calls resulting in the creation of approximately 250,000 CAD events per year. Approximately 135,000 additional CAD events are initiated by police officers during their normal patrol activities.

Calls requiring a fire or medical response that do not also require a police response are transferred to the Seattle Fire Alarm Center for appropriate resource deployment and are not entered into SPD's CAD system.

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

The CAD system automatically receives the telephone number, name (if available), and location of the caller (if available) from the West VIPER telephone system for calls placed to 9-1-1. Non-emergency calls, and associated phone numbers, are not automatically entered into CAD. If the call is determined to be a request for police services, call takers and dispatchers then manually enter additional information into CAD, such as the nature of the emergency, and create a CAD event to facilitate a police response. Call takers and dispatchers may add supplemental information into CAD regarding scene safety, descriptions of individuals, vehicles, and premises. Much of the privacy-sensitive information entered into CAD is provided by 9-1-1 or non-emergency callers or by officers or dispatchers who input information into the CAD system when responding to a call.

All of the information and data that is entered into CAD is viewable and retrievable. Some information from one call may be used for subsequent calls at the same location or involving the same individuals.

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.

CAD is the system used by SPD to coordinate and document, in real-time, requests for police service and SPD's response to those requests. The technology is used by 9-1-1- call takers to document information reported by a 9-1-1 caller and then assists 9-1-1 dispatchers with prioritizing emergency calls and assigning appropriate police resources to incidents. CAD is also used to document patrol officers' proactive policing ("on-views"), such as initiating a traffic stop. About 250,000 CAD events are created from the approximately 900,000 calls received by the 9-1-1 center annually, and approximately 135,000 CAD events are created annually from patrol officers' on-viewing an incident such as a traffic violation.

Developed in the 1960s, CAD systems are used by virtually all modern police departments. Computer aided dispatch allows for increased efficiencies in dispatching responses to emergencies. CAD also provides information that allows SPD to allocate patrol resources effectively while reducing response times. CAD is the real-time record-keeping system for officers' response to calls for service, thereby documenting SPD's actions related to each of those requests in an organized and reportable method.

2.2 Provide any data or research demonstrating anticipated benefits.

McEwan, Tom. et al. "Computer Aided Dispatch in Support of Community Policing, Final Report." National Institute of Justice. Feb 2004.

This 2004 research project studied the effects CAD systems have in the support of community policing objectives at several police departments throughout the United States. The benefits provided by CAD outlined in this article include; reporting access to recorded data, location of resource data, data on call types received, better crime analysis, department problem solving information, and resource allocation measures. The article also provided suggestions for enhancements, such as better integration with other data systems and more robust remote access for real-time CAD data by officers in the field, which have largely been implemented by CAD system developers in the years since.

"Versadex PoliceCAD" *Law and Order: The Magazine for Police Management*. Volume:56 Issue:7. July 2008 Pages:38-40,42,43

The *Versadex PoliceCAD* article details the history of the development of the Computer Aided Dispatch system created by Versadex. The style of CAD they developed was more streamlined and easier to integrate with other law enforcement data systems including records management systems. Effective CAD systems should "improve delivery (of services) and boost the speed and accuracy of the caller's critical information to the emergency responder."

A study by the Illinois Department of Transportation on the impact of CAD systems:
<https://utc.uic.edu/wp-content/uploads/Strategic-Project-Plan-Computer-Assisted-Scheduleing-and-Dispatch1.pdf>

This study by the Urban Transportation Center at the University of Illinois at Chicago, looks at the impact of CAD systems on the operation and coordination of paratransit services in the state of Illinois. Though this research was not specifically relevant to the dispatch of law enforcement services, the study provides insight into cost-savings and service improvements which are provided by the implementation of CAD systems.

2.3 Describe the technology involved.

CAD (Computer Aided Dispatch) software, made by Versaterm, consists of a set of servers and software deployed on dedicated terminals in the 9-1-1 center, on SPD computers, and as an application on patrol vehicles' mobile data computers (MDCs) and on some officers' smart phones.

When a request for police service is initiated by a 9-1-1 call or an officer on-viewing an incident, a CAD event is created by the 9-1-1 Center staff, and a unique CAD event ID number is automatically generated. Information related to that CAD event is entered into the CAD system. A call taker assigns the CAD event a specific type code and priority associated with the type of police service requested. The location of the event is entered and CAD validates the address, locates the address electronically, and then plots it on a map. Based on this information, the call taker routes the CAD call to the appropriate dispatcher. The dispatcher then assigns patrol officers to the service request and records this information in the CAD event. Each of the assigned patrol officers then log their activities related to that request for service into CAD using established codes. When the request for service is completed, the primary officer assigned closes the CAD call. Based upon the codes used to close the CAD call, the system then automatically routes the information recorded into SPD's Records Management System (RMS) where additional information, such as police reports and supplementary material, is stored.

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

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. CAD is a technology that supports this mission by ensuring that police resources are efficiently and appropriately dispatched to address emergencies and by documenting the police response to those emergencies.

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

SPD's authorized users of CAD include all sworn personnel, 9-1-1 Center staff, and other civilian staff whose business needs require access to this data.

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.

All authorized users of CAD are Criminal Justice Information Services (CJIS) certified and maintain Washington State ACCESS (A Central Computerized Enforcement Service System) certification. More information on CJIS compliance may be found at the CJIS Security Policy [website](#). Additional information about ACCESS may be found on the Washington State Patrol's [website](#).

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.

Access for personnel into the system is predicated on state and federal law governing access to Criminal Justice Information Services (CJIS). This includes pre-access background information, appropriate role-based permissions as governed by the CJIS security policy found in Appendix M, and audit of access and transaction logs within the system. All users of CAD must be CJIS certified and maintain Washington State ACCESS certification.

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

This technology is used each time the 9-1-1 Center receives a request for police service or when a police officer assigns themselves to an incident which was self-initiated (an “on-view”) such as a traffic stop. About 250,000 CAD events are created from the approximately 900,000 calls received by the 9-1-1 center annually, and approximately 135,000 CAD events are created annually from patrol officers’ on-viewing an incident such as a traffic violation.

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.

Supervisors and commanding officers are responsible for ensuring compliance with policies.

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](#).

All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification. [SPD Policy 12.050](#) defines the proper use of criminal justice information systems.

Outside of SPD, Seattle Information Technology Department (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, including the FBI's Criminal Justice Information Services, (CJIS) Security Policy.”

The MCA document may be found in Appendix K.

Additionally, per the CJIS security policy, records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained. Details of the compliance program in Appendix M.

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.

When an individual places a call to 9-1-1, the telephone number they are calling from, the location they are calling from, the name associated with the phone number (if available from the phone company), and the type of telephone service (landline, cell phone, VOIP phone) are provided by the West VIPER telephone system and automatically entered into CAD when a CAD call is initiated by the call taker.

Additionally, private information may be entered into a CAD call by SPD officers requesting information, such as a warrant check, while responding to a request for service.

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

A CAD call is initiated when someone requests police services. All users of the CAD system are trained in its use to ensure the data collected is entered appropriately. Authorized users of the CAD system are required to be CJIS certified and adhere to the CJIS security policy, found in the appendices of this document.

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?

The Seattle Police 9-1-1 Center is the primary Public Safety Answering Point (PSAP) for emergency 9-1-1 calls placed within the City of Seattle. CAD is in continual use by police communications dispatchers. When a call is entered into CAD, a radio dispatcher communicates to police resources in the field, maintaining contact with those resources and coordinating responses.

4.4 How often will the technology be in operation?

The CAD system is in continuous use 24 hours a day, 365 days a year.

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

CAD software is permanently installed.

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?

The CAD software has no physical or visual indicator that it is in use. The software itself runs 24 hours a day, 7 days a week, 365 days a year.

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

Within SPD, only authorized users can access the system, technology, or the data. Access to the application requires SPD personnel to log in with password-protected login credentials which are granted to employees with business needs to access CAD. These employees are ACCESS and CJIS certified.

Data is entered into CAD from both the West VIPER telephone system and from information manually entered by SPD personnel. It is accessed and used on SPD's password-protected network with access limited to authorized personnel as described in 2.5, above.

According to the CJIS security policy, "The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services."

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.

Data with regards to response times, response locations, crime trends, and general statistics is managed by the Data Driven Policing unit within SPD.

Additionally, 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; applicable CJIS compliance policies are found in Appendix M.

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 FBI's Criminal Justice Information Services, (CJIS) Security Policy."

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.

CAD is operated and used primarily by SPD personnel. Seattle IT Department personnel have administrative access to the system for support services as outlined in 4.7.

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

Authorized SPD users, as described in 2.5, may have access to the system to document, review, or report on police activity pursuant to law and policy, to extract information for use in court or administrative proceedings as required by law, to respond to appropriate requests for information, to make aggregate information available to the public, and to provide information to oversight bodies on issues such as stop and detention rates, for example.

Incidental access may occur from ITD 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 FBI's Criminal Justice Information Services, (CJIS) Security Policy.”

This MCA document between Seattle IT and SPD may be found in Appendix K.

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.)?

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. All activity within CAD (including timeline of commands issued) generates a log that is auditable.

Data is securely input and used on SPD's password-protected network with access limited to authorized users.

The entire system is located on the SPD network that is protect by industry standard firewalls. ITD performs routine monitoring of the SPD network.

The CAD system is CJIS compliant. More information on CJIS compliance may be found at the CJIS Security Policy [website](#).

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'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 audit for compliance at any time.

ITD client services interaction with SPD systems is governed by the terms of the 2017 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 FBI's Criminal Justice Information Services, (CJIS) Security Policy."

The MCA document may be found in Appendix K.

Additionally, policy requires the following safeguards to be in place:

- The agency shall establish identifier and authenticator processes.
- Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. 08/16/2018 CJISD-ITS-DOC-08140-5.7 37 password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).
- Unsuccessful login attempts - the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJIS or systems with access to CJIS). The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.

- When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128-bit strength to protect CJI.
- When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256-bit strength.
- Intrusion Detection Tools/Techniques such as monitor inbound and outbound communications for unusual or unauthorized activities, send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort, employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
- Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
- The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.
- A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

Publicly accessible computers shall not be used to access, process, store or transmit CJI.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

All of the data in CAD are held in SPD/ITD servers, located on City premises on SPD networks. Access to these networks is as specified in 4.1. All data that goes to mobile clients are encrypted to FIP 140-2 standards and is therefore CJIS compliant.

Per the CJIS Security Policy (see Appendix M):

“Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history 08/16/2018 CJISD-ITS-DOC-08140-5.7 D-3 records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

Network Diagrams - Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.”

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

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

The 2017 Technical Security Audit for CJIS Compliance for SPD can be found in Appendix K

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](#).

Per the CJIS Security Policy:

“5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.”

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.

The CJIS security policy in Appendix M of this SIR includes applicable data retention requirements associated with the CAD system. The MCA between SPD and ITD (see Appendix K) is the inter-departmental agreement that ensures compliance with the CJIS Security Policy.

6.0 Data Sharing and Accuracy

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

No person, outside of SPD and Seattle IT, has direct access to the application or the data.

As Seattle IT supports the CAD 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 CAD system through inter-departmental partnership. The MCA can be found in the appendices of this SIR.

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

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 data collected by CAD 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.

6.2 Why is data sharing necessary?

Data sharing is not an automatic component of the CAD system. Instead, discrete pieces of data may be shared with outside agencies and individuals only within the context of the situations outlined in 6.1. Data sharing may be necessary for SPD to provide coordinated, rapid responses to 911 incidents, particularly reducing the amount of time needed to contact individuals, thereby improving outcomes.

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 CAD system documents information provided by the participants and witnesses in the event being reported, as input by SPD personnel. The system itself does not check for accuracy of the information that is provided by personnel. Instead, the Department may later determine that the information provided was not accurate and can provide updated information.

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

SPD cannot delete any information in CAD. Updates to information may be added to individual CAD events by SPD personnel with access to CAD.

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.

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?

CAD data is not legally constrained at the local, state, or federal level. Instead, retention of data is restricted. SPD retains CAD data that is not case specific (i.e. not related to an investigation) for 90 days.

Case specific data is maintained for the retention period applicable to the specific case type.

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

SPD Dispatchers undergo training on the use of CAD, which includes privacy training.

All authorized users of CAD must be CJIS certified and must maintain Washington State ACCESS certification.

[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](#).

The CJIS training requirements can be found in the appendices of this document, as well as in question 3.3, above.

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.

The nature of the Department's mission will inevitably lead it to collect and maintain information many may believe to be private and potentially embarrassing. Minimizing privacy risks revolve around disclosure of personally identifiable information.

[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.

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 (i.e., activity logs) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of CAD.

The largest privacy risk is the un-authorized release of personally identifiable 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.

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.

The latest CJIS technical security audit from 2017 can be found in Appendix K of this SIR.

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
N/A	N/A	N/A	N/A	N/A	General Obligation Bonds, King County Voter-Approved Levy, Capitol Project Fund, and IT Operating Funds.

Notes:

The existing CAD system has been in place for more than 10 years. The documents related to this legacy technology project were purged after six years, per the City's retention schedule, so we are unable to find specific information related to the initial cost of acquiring CAD. The City appropriated \$3,228,000 in 2004 for the acquisition of the existing CAD system.

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
\$333,757	N/A	N/A	N/A	N/A

Notes:

This is funded through the City's General Fund. The King County E 9-1-1 Program Office reimburses the City up to 50% of the initial purchase and maintenance costs for CAD, up to 100% of 9-1-1 call taking modules, and up to 25% of data storage costs are reimbursable.

1.3 Cost savings potential through use of the technology

These are not quantified; however, the use of CAD systems is standard practice in emergency response in the United States and has been for decades. Prior to the development of this type of system, 9-1-1 Center call takers wrote the specifics of emergency calls on paper notecards which were delivered to dispatchers on a conveyer belt. The cost savings provided using CAD technology is measured by its impact on efficiencies.

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

The King County E 9-1-1 Program Office reimburses the City up to 50% of the initial purchase and maintenance costs for CAD, up to 100% of 9-1-1 call taking modules, and up to 25% of data storage costs are reimbursable.

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
Numerous other agencies use Versaterm, including the Anaheim Police Department, the Austin Police Department, the Bellingham Police Department, the Minneapolis Police Department, the San Jose Police Department, and the Salt Lake City Police Department.	No available	Not available

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
Versaterm	480-663-7739 infoUSA@versaterm.com	Technical support for SPD’s use of Versaterm

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
Standard Functional Specifications for Law Enforcement Computer Aided Dispatch (CAD) Systems	Law Enforcement Information Technology Standards Council (LEITSC)	https://it.ojp.gov/documents/LEITSC_Law_Enforcement_CAD_Systems.pdf

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?

Some personally identifiable information (PII) gathered during emergency responses could be used to identify individuals, such as their name, home address or contact information. Victims of criminal activity may also be identified during incident responses, whose identities should be protected in accordance with [RCW 42.56.240](#) and [RCW 70.02](#).

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.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional and dependable police services. While race and ethnicity information of individuals is recorded in the CAD system, there are no means within the system through which and ethnic bias may emerge. CAD is the real-time record-keeping system for officers' response to calls for police service and its users are subject to SPD's existing policies prohibiting bias-based policing. 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.

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

☒ all Seattle neighborhoods

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

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?

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific 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%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

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?

The CAD system is used to assist in the dispatch of police resources and document SPDs response to requests for service throughout the city of Seattle. There is no distinction in the levels of service this system provides to the various and diverse neighborhoods, communities, or individuals within the city.

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.

Data entered into CAD 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. CAD is the real-time record-keeping system for officers' response to calls for police service and its users are subject to SPD's existing policies prohibiting bias-based policing. 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.

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 most important unintended possible consequence related to the continued utilization of the CAD system by SPD is the unintentional release of privacy data. The policies in place requiring ACCESS and CJIS certification by all CAD users and the data security processes in place mitigate the likelihood of this occurring.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

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

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

2.2 Additional Outreach Efforts

Department	Outreach Area	Description
SPD	Meeting: South Seattle Crime Prevention Council	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	Meeting: Fabulous Forum	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	Meeting: East African Advisory Council	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	Meeting	East African Community Senior Lunch
SPD	Meeting: East Precinct Advisory Council at Seattle University	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.
ITD	Social Media Outreach Plan: Twitter	Directed Tweets and Posts related to Open Public Comment Period for Group 2 Technologies, as well as the BKL event.
SPD, SFD, OPCD, OCR, SPL, SDOT, SPR, SDCI, SCL, OLS, Seattle City Council	Social Media Outreach Plan: Twitter	Tweets and Retweets regarding Group 2 comment period and/or BKL event.
ITD	Press Release	Press release sent to several Seattle media outlets.
ITD	Ethnic Media Press Release	Press Release sent to specific ethnic media publications.

ITD	Social Media Outreach Plan: Facebook Event Post	Seattle IT paid for boosted Facebook posts for their BKL event.
ITD	CTAB	Presented and utilized the Community Technology Advisory Board (CTAB) network and listserv for engaging with interested members of the public
ITD	Blog	Wrote and published a Tech Talk blog post for Group 2 technologies, noting the open public comment period, BKL event, and links to the online survey/comment form.
ITD	Technology Videos	Seattle IT worked with the Seattle Channel to produce several short informational/high level introductory videos on group 2 technologies, which were posted on seattle.gov/privacy . And used at a number of Department of Neighborhoods-led focus groups.

2.3 Scheduled public meeting(s).

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

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

2.4 Scheduled focus Group Meeting(s)

Meeting 1

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

Meeting 2

Community Engaged	Entre Hermanos
Date	Thursday, February 28, 2019

Meeting 3

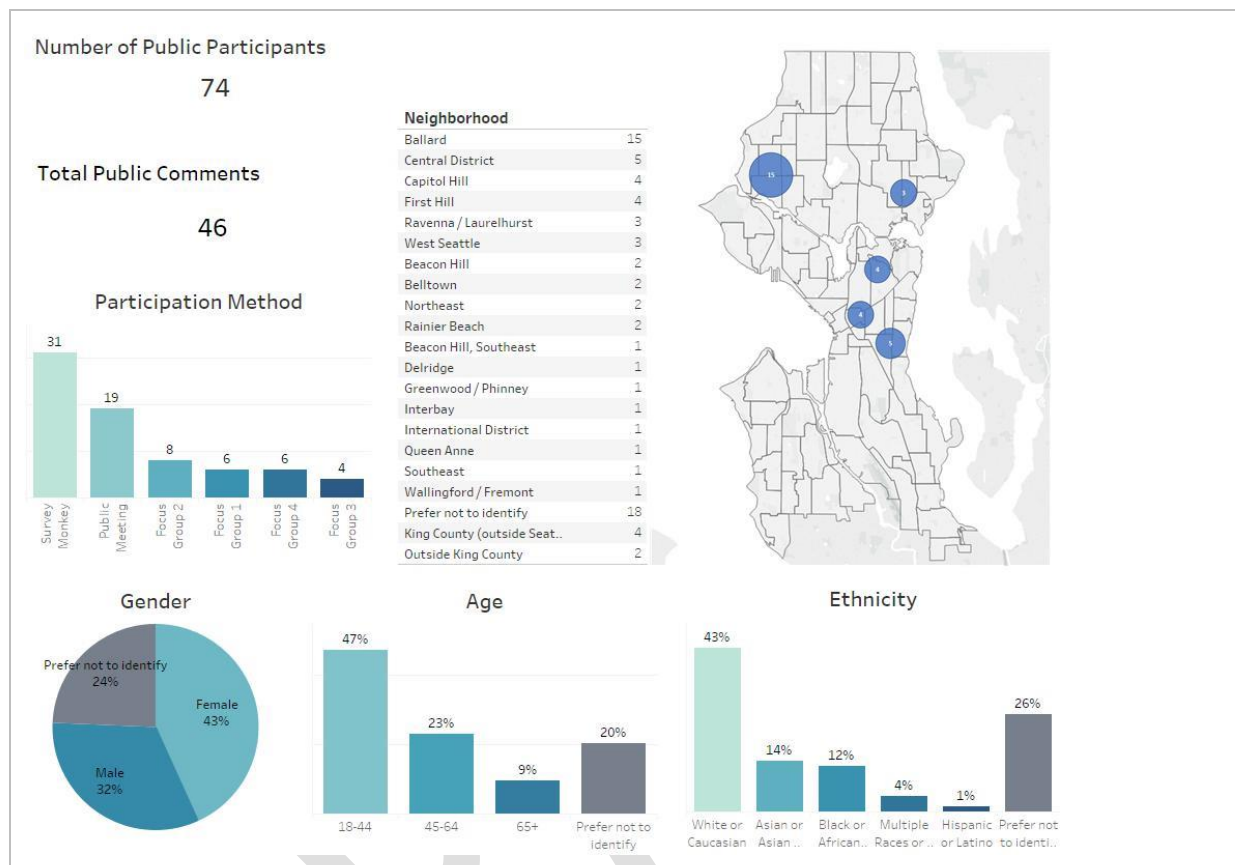
Community Engaged	Byrd Barr Place
Date	Thursday, February 28, 2019

Meeting 4

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

3.0 Public Comment Analysis

3.1 Summary of Response Volume



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

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see [Appendix E](#) for all comments received from the public about this technology.

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

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see [Appendix E](#) for all comments received from the public about this technology.

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

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see [Appendix E](#) for all comments received from the public about this technology.

3.5 Question Four: Do you have any other comments?

Due to the low volume of responses received about this technology, a comment analysis was not able to be completed. Please see [Appendix E](#) for all comments received from the public about this technology.

DRAFT

4.0 Equity Annual Reporting

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

Respond here.

DRAFT

Privacy and Civil Liberties Assessment

Purpose

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

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

Working Group Privacy and Civil Liberties Assessment

Respond here.

CTO Response to Privacy and Civil Liberties Assessment

Respond here.

DRAFT

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.

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

RET: "racial equity toolkit"

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

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

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

Surveillance ordinance: Seattle City Council passed ordinance [125376](#), also referred to as the "surveillance ordinance."

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

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



Appendix B: Meeting Notice(s) (PDF)

DRAFT

Appendix C: Meeting Sign-in Sheet(s) (PDF)

DRAFT

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 department is having all these technologies being used but not letting the public aware of it
- Coplogic is not clear and is confusing to use (what you can report and what you can't report)
- If coplogic is known by the community would they use it ? (Community members agreed that no one would use coplogic because it's not in Vietnamese. Not even people who speak english fluently even use it.
- Many community members don't trust the system)

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

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

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

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

Other comments:

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

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

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

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

Friends of Little Saigon (FOLS)

Please select which technology you wish to comment on:

- | | | | |
|---|---|--|--|
| ☐ SCL: Binoculars | ☐ SCL: Sensorlink
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.

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

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: CopLogic

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

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

- What is the logic behind this overall, because it seems like it presents more cons than pros, and what is the 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 I'm 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 out 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 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 that can lower the property value. And if the police isn't following up then how is it being used
 - Its definitely possible for people to report inaccurate information
4. What recommendations would you give policy makers at the City about this technology?
- a. But my concern is reporting someone that can really target people of color. And that happens much more threatening to people. So the concept of an upset black women is more intimidating than an upset women that is another race and how many times will behavior like that be reported. Or how many times will a black man be reported against because it seems scary. So I think it lowers the bar when you don't have to talk to an individual when you don't have to talk to a police
 - b. My questions are, how accessible are cop logic to people who don't read or speak English. How is SPD going to do what they can to make sure that this doesn't negatively impact communities they are already having issues with like the Sea Tac community that already feels threaten and criminalized by communities.
5. Can you imagine another way to solve the problem this technology solves?
- So the SPD is very data driven these days and the one thing we repeat is report report report, call 911 and report online whatever you thinking is happening because all of that goes into their data base and is used for them to use resources and put police based off of where there is more crime. The report report report mentality assumes there are good relationships between the community and police, so even if someone doesn't do something bad, I don't know that they would feel comfortable reporting, even if online
 - From the community I have come from I am almost certain that they haven't even used online reporting so how do we make sure that we are giving everyone access to use online reporting. And there are certain crimes that are so common in areas that they don't even report it because they think the police should already know about it
 - I think the department should solely rely on the technology only as a way of collecting info they should still use in personal resources to actively participant in local community and make connections you can't rely only on this technology alone to do this
6. Other comments
- a. Also in this day in age we need to consider that immigration is a issue, and this administrative has blended the different agencies so people have a hard time knowing where SPD starts and ICE starts and those lines have been blurred and that is a real concern for many families

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Binoculars/Spotting Scope

1. Do you have concerns about this specific technology or how it's used?
 - . People in our community don't have the access to say or be apart of these conversation. A lot of these people are literate, and might not have the same cultural values. For Muslim women there are a type of consent that you have when you walk outside and are covered in a certain away versus when you are in the privacy of your own home. And people might not have that cultural and religious awareness
 - a. I had one quick concerns, as far as the data that is collected using these binoculars, who has access to it
 - Seattle City Light: Information goes into the billing system, which customers can access if they have the automated reader but do not have access to under the current system
 - I know the focus is on binoculars but my mind is on new technologies and when people who are consumers and feel like I am overcharged how do I follow up and get those issues resolved. For systems that are completed based off of technologies how will I know if that data is being altered.
 - b.
2. What value do you think this brings to our city?
 - . I would just add this is more my general comments I think its good that Seattle city lights is providing notifications to people when this is happening. Are they wearing something visible that show people they are from Seattle city lights? And is there a way for people to complain?
 - Yes they are wearing vests that are very visible. Yes we have a couple different avenues the easiest is to call the customer service line and to submit a complaint there
3. What worries you about how this is used?
 - . My primary concerns on my end is if someone is looking into my home with binoculars its a privacy concern. Most Muslim women wear hijab and I don't feel comfortable if someone is using binoculars looking from the outside when we are not wearing the hijab. My concern is that it is a huge invasion of privacy
 - a. I have a question as the women expressed the feeling of people reading the meters with binoculars, if the meter has abnormal behavior or is in a different place of the house. Have there been situations where someone sees the person looking at someone house with binoculars, and they might not have gotten notified. Or the meter might be on the opposite side of where they are looking. Are they getting background checks? Or are complaints being followed up

- Seattle City Light: Yes all city employees have background checks, and if a complaint gets called in they will go through disciplinary actions
 - What are the average times for disciplinary actions. How long is the process for a full investigation
 - Seattle City Light: It's a multiple step process in terms of different levels. There are warnings, and if there was undo actions. Timeline really depends, I'm not sure
 - Cause I think that people who go through the different nuances of how privacy can be breach that is just the end all be all of how privacy can breach so I think there needs to be policy put in place so that people don't have their privacy breach and they are being monitored by a pedophile
4. What recommendations would you give policy makers at the City about this technology?
- When I look at the Seattle city of light they do a lot of estimated guesses and as a consumer they might give you a \$500 fee based off of the estimated guesses so I think it is important to have some sort of device that better clearly shows how much you use
5. Can you imagine another way to solve the problem this technology solves?
- My other question is if its actually not efficient why do you get the option to opt out (of the new automated system). If there is an old school way of doing it that involves a breach of privacy because these are human beings using the binoculars, so If this other option is better why are people having the ability to opt out.
6. Other comments: (Many comments were discussed over Seattle City Light's upcoming change from binocular use to automated meter readers)
- Who opted out was it home owners?
 - a. When we go to a place with 12 tenements do all 12 of them have the ability to opt out or in, or just the owners of the building?
 - b. Each home owner has a schedule provided to them and it is a 3 day period which they can come in and look at the system
 - c. Is there a cost to them to have the new meter.
 - Seattle City Light: There is no cost with getting the new meter, but there is still a cost If we have to send someone out there to read it
 - What I don't understand is why the new practice is not to just use the new system since that is more accurate and it is doesn't require binoculars
 - What is the cost of opting out
 - Seattle City Light: There is a flat rate
 - I was gonna reiterate when we talk about equity and equitable practices. You can opt out (of the automated system) but there is a fee. And it makes me think

how much of It is a choose if one of these you have to pay for and the other one is free. So that sounds a little problematic when looking at choices of equity. I think choices are great, but also people need to be well informed. Like people within the community need to have more clear information to make the best decision for themselves

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

Council on Islamic Relations, Washington (CAIR-WA)

Focus Group with Council on American-Islamic Relations, Washington

Thursday, Feb. 21, 2019

Technology Discussed: Acyclica

1. Do you have concerns about this specific technology or how it's used?
 - Where does this data go? Does it go to SDOT? Google maps?
 - My other question is, it said whatever is being transferred is encrypted. All encrypted means to me is getting data from one device to another will be transferred without it being intercepted. What I don't know is, how much information are people getting
 - My concern is related to data, yeah we like to use gps. But what is the perimeter, what is the breach of access. Where is the data being used, and what can that turn into. we might be okay if the data is only being used for traffic related updates, but they might use it for more
 - I also would like to see how acyclica actually does what they do. They are using a lot of words that normally don't know. So I want to know how exactly they are hashing and salting. So for them to be clear about how they doing it. like when whatsapp encrypted they didn't give us the exact code but told us how they are doing it
 - Asking for a greater transparency for how they are doing this
 - I think the purpose of it is really important but the biggest concern is collecting all of this information without consent of passersby.
 - So the specific identifier that acyclica uses it mac addresses? You could potentially use that number to track that phone for the lifetime of the phone, for as long as that phone is on and being used. And that is very concerning.
 - Also I want to understand more where is this data going, and I want to know if this data is going to be used for future projects.
 - I want to ask is this something people opt into
 - People don't even know this is being used
2. What value do you think this brings to our city?
 - I like getting places and I like getting traffic information.
3. What worries you about how this is used?
 - What I don't like is you using my phone to get that information. I want whatever is in my cellphone to be protected. And I wanna know what you can access
 - I think based on Seattle and Seatac's higher up wanting to monitor and map out Muslims and where they are, and I don't like people being able to use our phone to track our location or actions they might think is violent. So based off of Seattle's track record and law enforcement agencies I don't like it
 - People who live outside of Seattle are also being impacted by it anytime they drive in Seattle
 - Could someone "opt out" by having wifi disabled on their device? I don't know if this covers cell towers. Because if it covers cell towers the only thing you could is having your phone on airplane mode

4. What recommendations would you give policy makers at the City about this technology?
 - I think the big question is why aren't we using other vendors, like I mentioned google maps, or waze, in fact komo 4 uses waze. Where other options we're looked at, and what were the trade off there's. And I want to see some transparency between the decision-making processes
 - I don't think this data should be shared with other private agencies, or other interagency programs
 - If all you're looking at is traffic flow, why are you not using the sensors in the road to give traffic flow updates.
 -
5. Can you imagine another way to solve the problem this technology solves?
 - I don't know if this already exists but something that makes it that data can't be used from one technology and use it for a different purposes
 - I think speaking from an industry perspective that is really important to have a processes for. Because all of this data is being used regardless of if you live in Seattle, or people live in different countries even who are visiting. That data is being collected. My understanding is that SDOT doesn't get the data directly. So my concern is how long can acyclica keep this data, use this data. Why wasn't a different option used, one in which some sort of consent can be used, so something like waze, google maps where people can opt in can get that information.
 - Road sensors or ways to count cars
 - I think its better to count cars than phones, because there is some expectation that your car will be monitored.
 - Using vehicle level granularity

Entre Hermanos

Please select which technology you wish to comment on:

- | | | | |
|---|---|--|---|
| ☐ SCL: Binoculars | ☐ SCL: Sensorlink
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?

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 necesidad de puntos estratégicos y calles con más necesidad de ayuda por causa del tráfico.

What do you think about this technology in particular ?

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

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

Si es solo para ver el tráfico está bien.

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

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

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

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

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

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

Alternatives to this technology

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

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?

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

Al grupo le incomoda el uso de binoculares

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

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

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

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

Ahorro de energía

Record y datos mas precisos

Oportunidad de trabajo a quien utiliza los binoculares

Estabiliza los precios de la electricidad

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

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

What do you think about this technology in particular ?

Sensorlink Si

Binoculares son invasivos

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

La confianza en estos medidores serán confiables? Serán efectivos?

El uso de binoculares se puede acompañar de una cámara añadida

Alternatives to this technology

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

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.

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 transcurencia alarmante/peligrosa el uso de será implementado o limitado solo a instantes inmediatos de peligro.

Para reportar algo que ya sucedió o que son recurrentes.

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

Los reportes no son anónimos.

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

Alternatives to this technology

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

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.

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 individuos 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 benéfico?

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

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

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

El video de Seattle Department of Transportation de Acyclica fue mostrado

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

Seattle Metering Tool fue mostrada

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

Video de Fire Department's Computer Aided Dispatch fue mostrado

El 9-1-1 logging recorder video fue mostrado

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

Video de Coplogic fue mostrado

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

El video de Seattle Police Computer Aided Dispatch fue mostrado

Esta tecnología es similar a la de los bomberos.

Se preguntó cuál video era de interés para analizar

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

Las Preguntas que sea harán serán las siguientes:

- ¿Qué piensan de este sistema de tecnología en específico y el motivo de usarla?
- ¿Cuál creen que sea el aporte de esta tecnología a la ciudad?
- ¿Qué preocupación les causa el uso que se le dará a este sistema?
- ¿Qué recomendarían a el grupo de políticos de la ciudad 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?

- Sería algo bueno el aporte por la agilidad del tráfico solo si la tecnología está sincronizada con los semáforos, de otra manera no es útil si no aporta para el mejoramiento del tráfico.
- Participante dice que hay alternativas para esquivar el tráfico.
- Participante opina que la tecnología es interesante ya que usa google maps y está de acuerdo con el mejoramiento del tráfico.
- Si el objetivo es de mejorar el tráfico está de acuerdo. Pero también quiere saber en qué lugar(es) estarán los aparatos, si algunas personas serán beneficiadas más que otras.

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

- Le preocupa el uso de wifi en Acyclica porque pueden obtener toda la información de los teléfonos.
- Si el potencial puede ser aplicada a la inversión.

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

- El tráfico sigue igual.
- Quien usa o almacena la información.
- La preocupación es la colección de data.

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

- Participante no está de acuerdo. No es la colección de data lo alarmante sino los recursos (dinero utilizado) ya que o la tecnología no están funcionando porque el tráfico

sigue igual. No hay cambio con la nueva tecnología, esos gastos no son válidos ya que no hay resultados. Esos gastos pudieran ser utilizados para la comunidad.

- También tienen que ver si la tecnología emite radiación o alguna otra cosa dañina; perjudicial a la salud.
- El gobierno tiene todos los datos.
- Opinión de otro participante: No necesitan esta tecnología para tener los datos porque ya existen métodos para eso, incluso aplicaciones o alguna otra cosa.

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

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

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

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

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

- Participante no cree que allí se ocupan.

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

Presentador: Crees que Acrylica es como el router de google?

- La tecnología no es un router, sino colección de data para planeaciones urbanas.
- Participante: “quiero creer” “convencerme” que los sensores están allí para ayudar con el tráfico.
- No se sabe cuándo las instalaron, los resultados deberían de ser públicos. Si la tecnología es para aliviar el flujo de tráfico entonces por qué no extienden el programa? O por qué no hay mejoramiento del tráfico?

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

Alternativas:

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

Tecnología #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 ciudad/ciudadanos/comunidad?

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

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

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

Tecnología #3 Coplogic

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

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

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

Pregunta: En que ayuda a la comunidad?

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

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

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

Pregunta: Alguna inquietud sobre el uso de esta tecnología?

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

Pregunta: En qué situación usarán esta tecnología?

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

Pregunta: Para qué sirve el reporte de la computadora?

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

Pregunta: Qué les recomendarían a los políticos?

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

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

- Si es usada de manera adecuada y como han dicho está bien.
- El uso de la tecnología es bueno para dar respuesta para todas las cosas y personas.

Consejo:

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

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

Byrd Barr Place

2/28/2019 Surveillance Technology Focus Group

Thursday, February 28, 2019

1:42 PM

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

Videos:

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

Tom: Read definition of surveillance

Craig: invasion of privacy?

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

Community Member: used to be in the tech industry for thirty years. Writing a book about surveillance and technology

Wanda: I like the online police report. If someone is experiencing a crisis or trauma, you can go ahead and report it.

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

Mercy: security is a great safety issue

Craig: there are some parts of the neighborhood/city that need to be watched, and some that need to be left alone

Wanda: as long as it's even

Craig: Sometimes it's not even

Both: There are hot spots though

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

IG: The Computer Aided Dispatch

Talking about the International District:

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

"Some neighborhoods need to be watched"

- Gangs; drug use

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

- Craig: there are concerns, but who is allowed to see it, how is it stored? That's a concern
 - Is it used for BOLOs? Is it everyone who is in the area, all of the police officers? Or is there some discretion as to which police officers would be given the information?
- Wanda: plenty of people are arrested who "fit a description"
 - Discussion about the racial discrimination: how people who think that "all [insert race here] look alike".
 - Individuals may think like that, but police officers have the capability to ruin someone's life.
- Marjorie: just recently got a smart phone, and it's new to me that someone could know where I'm going and I wouldn't be aware of it
 - Without my consent.
- Mercy: grew up with the idea that big brother is watching you
 - Tracking how many times I go to the library seems like a waste of money
 - People who are not law abiding citizens, they are the ones to be worried
- Craig: What about selling weed, coke, etc. Should they be worried?
 - Mercy: well at least in Seattle, it's ok to sell
- Mercy: big brother is watching. We already know that, it's just more obvious now
- There is a lot of technology that we are not made aware of

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

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

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

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

- Location privacy: you can tell a lot about a person based on where they go, and tracking that can build a pretty extensive profile of who you are
- IG: now that I know they are tracking, I will turn it off.

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

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

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

SCL binoculars:

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

Regarding being watched in public:

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

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

- Craig: how about just making it even? Police have an image to people of color; they are afraid of why they are going to be there. We can police ourselves
- Wanda: I disagree. There are some who think there should be less, but there are also a lot of people who worry about walking down the street
 - As a woman and DV survivor, I appreciate the police and appreciate living in a country where I can call a number for help.

- I have a big problem with the shooting of unarmed black men, but as an individual I still appreciate the police.
- But I have a problem being tracked, and I have a problem being watched in my home.
- General comment: The number of police being on the corner is a touchy situation
 - Knowing the police that are on your corner makes a difference. They can police the community better if there is more of a relationship between the two.
- Craig: it has to be both, even. You can't trade off the technology for the police.
- Mr. Surveillance: The trend is they want to go to more technology and less police.

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

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

CopLogic: making police reports online

- Craig: I think it's stupid.
 - Would use that technology for stupid crimes
- Mercy: you could report your neighbor for silly things
 - Anonymous reporting of crimes that could target people for things they might not call 911 for
- Wanda: there were some lines of traffic where I saw cars lined up with their windows smashed in; nothing taken, but glass all over the place.
 - Police response when called: maybe you should get a cheaper type of car
 - Would he have said that to us if we were a different skin color, or lived in a different neighborhood?
- IG: I think it's a bad thing: someone could make up a story and the officer didn't have to check it.
- Marjorie: I think the online reporting could be abused

Appendix E: All Comments Received from Members of the Public

ID: 10617659831

Submitted Through: Survey Monkey

Date: 3/25/2019 1:18:11 PM

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

SPD: Computer-Aided Dispatch (CAD)

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

Concerns: 1) 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. 2) No 2-step-verification/2-factor-authentication (2SV/2FA) for login to Versaterm vCAD; however, an individual would need to first logon to an SPD workstation and then login to vCAD. That being said, page 14 of the SIR implies that 2FA is in place.

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

It meets a functional need that likely is more accurate and efficient than a paper-based workflow.

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

The draft SIR did not specify what (if any) other vendors SPD/IT considered before deploying Versaterm vCAD. Is this the optimal CAD solution for the City of Seattle? Is there perhaps another CAD software provider that is more competitive and perhaps has better security/privacy/audit features?

Do you have any other comments?

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

ID: 10617346709

Submitted Through: Survey Monkey

Date: 3/25/2019 11:16:33 AM

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

SPD: Computer-Aided Dispatch (CAD)

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

None at all

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

Gets help where it's most needed faster.

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

Allow it.

Do you have any other comments?

I can't believe this is even an issue.

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

Don't you have better things to do with your time and our money?

ID: 4

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: CAD

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

Dispatching softwares should have "detail options" on language callers speak that may be different than English

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: 3

Submitted Through: Focus Group

Date: 2/27/2019

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

SCL: Binoculars, SCL: CheckMeter, SCL: AmpFork, SFD: CAD, SPD: CAD, SPD: 911 Logging Recorder

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

That would be good with advanced technology

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

Yes, around the city.

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

Need good train to people who use new technologies

Do you have any other comments?

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

ID: 10529127076

Submitted Through: Survey Monkey

Date: 2/13/2019

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

SPD: CAD

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

Why isn't Geotime and Maltego on this list? This is what I have the most concern about.

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

Geotime and Maltego - I want to know where it get it's data and how it's collected.

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

Geotime should NOT exist

Do you have any other comments?

Why don't you have Maltego and Geotime. I think the public should know more about this technology and how it's used. Disregard question 1

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

Maltego and Geotime. -- Disregard question 1

Appendix F: Department Responses to Public Inquiries(PDF)

DRAFT

Appendix G: Letters from Organizations or Commissions(PDF)

Please see the following pages for formal letters regarding Group 2 surveillance technologies from various community organizations, commissions, and boards.

DRAFT

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 documented and defined in the codebook.
 - IV. Apply the framework to code the remainder of the comments received.
 - V. Interpret the data by identifying differences and map relationships between codes and themes, using R and Tableau.

Step Three: Conduct Quantitative Analysis

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

themes.

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

Step Four: Summarization

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

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 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

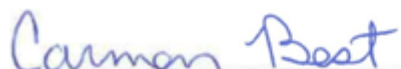
This agreement covers the overall supervision of all Criminal Justice Agency systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, administration, and maintenance of any Criminal Justice Agency system to include NCIC 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.



Tracy Cantrell
Interim Chief Technology Officer
Seattle Information Technology Department

Date Feb 2, 2018



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 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,) 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 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

Remote Access Policy

June 1st, 2018



City of Seattle

CJIS Remote Access Policy

Overview

The CJIS Remote Access Policy defines the necessary controls for remote access to Criminal Justice Information Services (CJIS) in scope systems.

Purpose

This policy ensures proper measures are taken when granting remote access to any employee, contractor, or vendor, to Criminal Justice Information (CJI) in-scope systems.

Definition

CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, decimation, storage, and destruction of CJI.

Scope and Applicability

This policy applies to personnel at City of Seattle, including those affiliated with third parties who remotely access City of Seattle systems to include CJI data. The policy applies to all systems owned by and/or administered by City of Seattle, including network to network VPN tunnels.

Policy

This policy applies to City of Seattle employees, City of Seattle Police Department employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the City of Seattle network or Public network, are required to utilize two factor authentication & VPN tunnel on City of Seattle workstation OR through a jump-box protected by two-factor Advanced Authentication (AA). Contractors, Vendors and City employees accessing in-scope systems from non-city computers are required to utilize the jump-box AA solution.

All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

- CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access to CJI.

- **Verify Identification:** a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
- All requests for access shall be made as specified by the CSO (CJIS Systems Officer). The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.
- VPN access must be approved by the requesting department prior to activation.
- Users must not:
 - Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.
 - Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).
- Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.
- Vendors must:
 - Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.
 - Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Applicability of other Policies

January 17, 2016 1 The City of Seattle has an existing Remote Access Policy that must be adhered to and can be found [here](#).

Enforcement

Enforcement of this policy will be led by the Chief Technology Officer (CTO). Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment or vendor contract termination. Where illegal activities or loss of City of Seattle assets are known or suspected, the City of Seattle must report activities to the appropriate authorities, City of Seattle is obliged to adhere to breach reporting by statutory limitation and must notify the Terminal Agency Coordinator (TAC) of any potential violations. All potential violations that involve CJI must be report to the Washington State Patrol ACCESS Section.

Implementation

This Policy is implemented by the ITD Security, Risk, and Compliance Director and applies to the City of Seattle access to CJI.

Document Control

Version	Content	Contributors	Approval Date
1.0	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson Approvers: CISO Andrew Whitaker CTO	
1.1	Initial Draft	Reviews: Denise Mendoza; Pepper Bojang-Jackson	
1.2	Initial Draft	Reviews: Denise Mendoza Bruce Hills Pepper Bojang-Jackson	
1.3	Review	Andrew Whitaker	6/5/18
1.4	Approved	Tracye Cantrell	6/12/18

Technical Security Audit



Technical Security Audit

Agency Information: Seattle PD - (WASPD0000)

Submitted By: Pepper Bojang-Jackson - On: March 22, 2017 Compliance Report with Agency Responses

Compliance Report

NCIC compliance standards must be improved and a response submitted to the WSP ACCESS Section.

Item:	1
Section Name:	Personnel Security
Question:	Are you maintaining a record of all your agency and/or county/city IT personnel that must receive a state of residency fingerprint background check within 30 days of employment? (<i>CJIS Security Policy, Version 5.5, Section 5.12.1.1</i>) Yes Please provide the SID numbers for all the IT personnel.
Agency Response:	List emailed 05/16/17

Item:	2
Section Name:	Personnel Security
Question:	Have all your agency and/or county/city IT personnel viewed the technical security awareness training (Level 4) in CJIS Online? (<i>CJIS Security Policy, Version 5.5, Section 5.2</i>) Yes All technical staff must view the technical security training - level 4 once every two years. Please provide a list of names of who viewed the training. The training is available at the following address: https://www.cjisonline.com/
Agency Response:	Sent email 05/16/17

Item:	3
-------	---

Section Name: Personnel Security

Question: Does your agency use an IT vendor for any IT needs?

Sub Question(s)

Item: 3.1

Section Name: Personnel Security

Question: Have all IT vendors had a Washington State fingerprint background check completed? (*CJIS Security Policy, Version 5.5, Section 5.12.1.1 and 5.12.1.2*)

User Answer: Yes

Compliance Response: All IT vendors must have a Washington State fingerprint background check completed.

Agency Response: List emailed 05/16/17

Sub Question(s)

Item: 3.2

Section Name: Personnel Security

Question: Please send a copy of the security addendum signed by each employee of the vendor company to CJISAudits@wsp.wa.gov

User Answer: I have read and will comply.

Compliance Response: Please provide a copy of the signed security addendum for each employee of the vendor company. I am missing security addendums for the following vendors:

1. 4quarters
2. Advantage Factory
3. Dorsey Consulting
4. Gartner
5. Genetec Corp
6. Sabey
7. Sysorex Consulting
8. TASER
9. TEKsystems
10. Versaterm - only a few

Agency Response: 1. 4quarters - Emailed 05/08/17
2. Advantage Factory - All Advantage Factory accounts are inactive

3. Dorsey Consulting - DOJ Monitoring Team - Should be CJIS Level 2, not 4 (deactivated all accounts)
4. Emailed 05/22/17
5. Genetec Corp - All accounts are inactive.
6. Adashi - Adashi employees are working in an environment that does not currently have CJIS data. Future plans do include CJIS data so they are in the process of completing the Security Addendums.
7. Sysorex Consulting - All accounts are inactive
8. TASER - Emailed 05/18/17
9. TEKsystems - Contractor is now City IT w/updated information.
10. Versaterm - Emailed 05/08/17

Item: 4

Section Name: System and Communications Protection and Information Integrity

Question: Does your agency email CJ? (*CJIS Security Policy, Version 5.5, Section 5.10.1.2*)

Sub Question(s)

Item: 4.1

Section Name: System and Communications Protection and Information Integrity

Question: Is the email that contains CJ encrypted? (*CJIS Security Policy, Version 5.5 Section 5.10.1.2*)

User Answer: No

Compliance Response: CJ that is emailed is required to be encrypted. Please advise when you will have this in place.

Agency Response: Seattle is utilizing Office 365 for email and email is encrypted

Is the email encrypted in transit? <https://products.office.com/en-us/business/office-365-trust-center-security>

Outlook client to O365 - SSL/TLS connection is established between Outlook client and O365

O365 to OME server - SSL / TLS connection between EXO Transport servers and OME server. "Office 365 uses Transport Layer Security (TLS) to encrypt the connection, or session, between two servers." <https://support.office.com/en-us/article/Email-encryption-in-Office-365-c0d87cbe-6d65-4c03-88ad-5216ea5564e8>

Is the email encrypted at rest when it sits on the server? <https://support.office.com/en-us/article/Email-encryption-in-Office-365-c0d87cbe-6d65-4c03-88ad-5216ea5564e8>

What about encryption for data at rest?

"Data at rest" refers to data that isn't actively in transit. In Office 365, email data at rest is encrypted using BitLocker Drive Encryption.

BitLocker encrypts the hard drives in Office 365 datacenters to provide enhanced protection against unauthorized access. To learn more, see [BitLocker Overview](#).

What level of encryption does OME use? - Microsoft attests that they meet and/or exceed FBI CJIS requirements

The CJIS Security Policy defines 13 areas that private contractors such as cloud service providers must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for the Federal Risk and Authorization Management Program (FedRAMP), a program under which Microsoft has been certified for its Government Cloud offerings

Item:	5
Section Name:	Event Logging
Question:	Does your agency have an established audit trail capable of monitoring the following: - Successful and unsuccessful log on attempts - Successful and unsuccessful password changes - Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources - Successful and unsuccessful actions by privileged accounts - Successful and unsuccessful attempts for users to access, modify, or destroy audit log files (CJIS Security Policy, Version 5.5, Section 5.4.1.1)
User Answer:	No
Compliance Response:	Please advise when your agency will have an established audit trail capable of monitoring the following: - Successful and unsuccessful log on attempts - Successful and unsuccessful password changes - Successful and unsuccessful attempts to access, create, write, delete or

change permissions on a user account, file, directory or other system resources

- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

Agency Response:

Seattle PD has established an audit trail capable of monitoring the following:

- Successful and unsuccessful log on attempts
- Successful and unsuccessful password changes
- Successful and unsuccessful attempts to access, create, write, delete or change permissions on a user account, file, directory or other system resources
- Successful and unsuccessful actions by privileged accounts
- Successful and unsuccessful attempts for users to access, modify, or destroy audit log files

Item: 6

Section Name: Identification and Authentication

Question: Does your agency and/or county/city IT department employee perform remote assistance from a non-secure location? Example employees home or coffee shop etc. (CJIS Security Policy, Version 5.5, Section 5.6.2.2)

User Answer: Yes

Compliance Response: IT has the ability to remote in the system from a non-secure location. Please advise once Advanced Authentication will be in place or when a remote session will be virtually escorted at all times.

Agency Response:

Full policy emailed to ACCESS on 04/23/18:

This policy applies to employees, contractors, or vendors who have a need to remotely access the CJI (Criminal Justice Information) in-scope systems for maintenance and operations. All access both remote and within the Seattle network (except for the SPD network) is through bastion hosts protected by two-factor Advanced Authentication (AA).

*All non-law enforcement personnel who perform criminal justice functions or have access to Criminal justice data shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS

Security Addendum. Seattle Information Technology employees are not required to sign the Security Addendum provided there is a CJIS Management Control Agreement (MCA) between Seattle Information Technology and Seattle Police/Fire.

*CJIS Security Awareness Training shall be required upon initial assignment, and biennially thereafter, for all personnel who have access toCJI.

Verify Identification: a state of residency and national fingerprint-based record checks shall be conducted (prior to) assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.

*All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All designees shall be from an authorized criminal justice agency.

*VPN access must be approved by the requesting department prior to activation.

*Users must not:

Type remote access passwords while someone is watching. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. (CJIS Security Policy Section 5.5.5) A session lock is not a substitute for logging out of the information system or from disconnecting a remote session.

Be connected to other network connections during remote access sessions into CJI data in-scope (e.g., no split tunnels are allowed).

*Users must maintain current virus protection and a host firewall on remote systems to protect from viruses and other remote attacks.

*Vendors must:

Be provided with the minimum access required to perform the necessary duties while the VPN session is active. Other access and privileges will be limited to the specific function performed by each vendor or service provider.

Be monitored by a City of Seattle CDE administrator during an assisted remote control session using Skype for Business or other current City of Seattle Enterprise standard for remote control sessions. The CDE administrator must have the ability to end the session at any time and the session must be terminated as soon as their work has finished.

Item: 6.1
Section Name: Identification and Authentication
Question: Describe the type of Advanced Authentication (AA) that is being used while the remote session is in process or advise if the session is being virtually escorted at all times. Virtually escorting is permitted when the following conditions are met:

- The session shall be monitored at all times by an authorized escort.
- The escort shall be familiar with the system/area in which the work is being performed.
- The escort shall have the ability to end the session at anytime.
- The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
- The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

(CJIS Security Policy, Version 5.5, Section 5.5.6)

User Answer: Certificate on the workstation. RSA is being implemented for network equipment.

Rarely workstations are remotely accessed. If they are, an SPD computer would be used to do the support work.

Compliance Response: Please advise when AA will be in place for IT staff that conducts remote assistance on applications or networks that access CJI or when all personnel will be virtually escorted or a policy prohibiting remote access from an unsecure location is established.

Agency Response: See #6

Item: 7

Section Name: Cloud Computing

Question: Does the agency utilize a cloud provider to host or store CJI related systems, applications or data? (*CJIS Security Policy, Version 5.5, Section 5.10.1.5*)

 Sub Question(s)

Item: 7.1

Section Name: Cloud Computing

Question: Is the CJI encrypted prior to entering the cloud?

User Answer: No

Compliance Response: Please advise when the CJI that goes to the cloud will be encrypted.

Agency Response: Seattle is utilizing Office 365 and CJI is encrypted

Report Summary:

The Federal Bureau of Investigation (FBI) assigned the Washington State Patrol (WSP) as the Criminal Justice Information Services (CJIS) Systems Agency (CSA) for the state of Washington. The CSA is responsible for establishing and administering an information technology security program throughout the CSA user community, to include the local levels. All standards set forth in the audit questionnaire originate from the CJIS Security Policy which provides Criminal Justice Agencies (CJA) with a minimum set of security requirements for access to FBI CJIS Division systems and information to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

CJIS Security Policy

[Add here]

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

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

Technology	Description	Proposed Review Order
Undercover/ Technologies	The following groups of technologies are used to conduct sensitive investigations and should be reviewed together. • Audio recording devices: A hidden microphone to audio record individuals without their knowledge. The microphone is either not visible to the subject being recorded or is disguised as another object. Used with search warrant or signed Authorization to Intercept (RCW 9A.73.200). • Camera systems: A hidden camera used to record people without their knowledge. The camera is either not visible to the subject being filmed or is disguised as another object. Used with consent, a search warrant (when the area captured by the camera is not in plain view of the public), or with specific and articulable facts that a person has or is about to be engaged in a criminal activity and the camera captures only areas in plain view of the public. • Tracking devices: A hidden tracking device carried by a moving vehicle or person that uses the Global Positioning System to determine and track the precise location. U.S. Supreme Court v. Jones mandated that these must have consent or a search warrant to be used.	4
Computer-Aided Dispatch (CAD)	CAD is used to initiate public safety calls for service, dispatch, and to maintain the status of responding resources in the field. It is used by 911 dispatchers as well as by officers using mobile data terminals (MDTs) in the field.	5

Technology	Description	Proposed Review Order
CopLogic	System allowing individuals to submit police reports on-line for certain low-level crimes in non-emergency situations where there are no known suspects or information about the crime that can be followed up on. Use is opt-in, but individuals may enter personally-identifying information about third-parties without providing notice to those individuals.	6
Hostage Negotiation Throw Phone	A set of recording and tracking technologies contained in a phone that is used in hostage negotiation situations to facilitate communications.	7
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

Technology	Description	Proposed Review Order
Washington State Patrol (WSP) Drones	WSP has begun using drones for surveying traffic collision sites to expedite incident investigation and facilitate a return to normal traffic flow. SPD may then request assistance documenting crash sites from WSP.	13
Callyo	This software may be installed on an officer's cell phone to allow them to record the audio from phone communications between law enforcement and suspects. Callyo may be used with consent or search warrant.	14
I2 iBase	The I2 iBase crime analysis tool allows for configuring, capturing, controlling, analyzing and displaying complex information and relationships in link and entity data. iBase is both a database application, as well as a modeling and analysis tool. It uses data pulled from SPD's existing systems for modeling and analysis.	15
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

Technology	Description	Proposed Review Order
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