2022 Surveillance Impact Report

Computer, Cellphone, & Mobile Device Extraction Tools

Seattle Police Department

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.

SPD utilizes electronic device extraction and imaging technologies to recover digital information or data from computers, cell phones, and mobile devices as part of a criminal investigations. These technologies are utilized only with the device owner's consent or pursuant to search warrant authority.

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

Extraction tools are used to pull private information from the devices of individuals. This raises concerns that individual privacy could be compromised. SPD mitigates this concern by utilizing these tools only with the device owner's consent or pursuant to search warrant authority.

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.

Extraction tools allow investigators to legally collect evidentiary information for ongoing investigations that may be used to prosecute crimes. These tools allow investigators to extract data quickly and securely from a wide variety of devices and preserve evidence from these devices in forensically sound conditions which can then be presented in court.

2.2 Provide any data or research demonstrating anticipated benefits.

Recent research shows as many as 63% of investigated cases includes some kind of digital evidence as part of the investigation. Prior to 2007, it was virtually impossible to recover forensically-sound data from mobile devices. Since the development of mobile device forensics tools, investigators are now able to preserve evidence from these devices in forensically sound conditions which can then be presented in court. One industry report found that more than half of all devices being held for analysis in police labs are passcode locked. Without proper tools to be able to access their data, these devices, which can contain crucial evidence, are often excluded from investigations because the data could not be accessed.

2.3 Describe the technology involved.

The different extraction tools SPD utilizes for mobile devices work similarly to one another – a mobile device is physically connected to a computer workstation with specialized locally installed software or to a stand-alone device with a similar software installed. The software is able to bypass/decipher/disable the device's PIN/password and extract files containing data from the mobile device. The stand-alone device can either save the files to removable physical storage (like a USB drive or similar media) or a computer workstation. These extracted data files are then accessed using the specialized installed software to parse the data. These software programs organize the data into packets of information that can then be examined.

Extracting information from computer devices involves taking a snapshot of a computer's hard drive, preserving the entirety of digital information on the hard drive at a particular point in time.

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. SPD's department priorities include the use of best practices that include officer safety guidelines and performance-based accountability to provide progressive and responsive police services to crime victims, witnesses, and all members of the community, and to structure the organization to support the SPD mission and field a well-trained sworn and non-sworn workforce that uses technology, training, equipment, and research strategically and effectively. Electronic device extraction and imaging technologies contribute to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of the investigation of criminal activity. These technologies are used only with the device owner's consent, pursuant to search warrant authority, or in certain circumstances outlined in RCW 9.73.210.

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

Extraction tools are maintained in two units within SPD: Sexual Assault and Child Abuse (SAU) Unit and the Technical and Electronic Support Unit (TESU).

SPD is the Lead Agency for the Washington Internet Crimes Against Children Task Force (WA ICAC TF), a multi-jurisdictional group of agencies dedicated to the protection of children from sexual abuse and exploitation. The WA ICAC TF is one of 61 task force groups in the national ICAC Task Force Program, which is administered by the US Department of Justice/Office of Juvenile Justice and Delinquency Prevention (OJJDP). The task force is organized to provide a multi-jurisdictional approach to the problem of Internet Crimes Against Children, by including agencies from local, state and federal law enforcement, federal and state agencies and federal and local prosecution. The SAU Unit manages extraction tools that they utilize within their unit. Within the SAU Unit, investigators must fill out a request form that includes a copy of consent or search warrant authorizing the extraction. All data extracted is stored securely on premises within SAU – not accessible to any vendor.

The Technical and Electronic Support Unit (TESU) manages extraction tools for other SPD investigations. TESU requires a written request to use extraction tools that includes evidence of consent or search warrant authority. Extraction is conducted in-house and data is provided to the requesting Officer/Detective for the investigation file. TESU then purges all extracted data. No data is stored by a vendor, as the necessary tools are maintained entirely offline and on-premises.

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 the technology, such as a notification, or check-in, check-out of equipment.

SAU: A written request accompanied by a copy of consent or a search warrant is necessary to utilize extraction tools for investigations related to internet crimes against children. One of the certified users within SAU conducts the extraction and provides copies of the data to the investigator. The technology requires training to operate the device, personal password to log onto the device, a separate password from the login to access extracted data. That same password is required to move the extracted data from the device to a portable USB. A log of device uses is kept on the SAU share drive and can be reviewed by supervisors if required. This log includes information about the specific investigation such as date, case number, detective assigned, device information and warrant parameters.

TESU: An Officer/Detective must submit a request form, accompanied by a copy of consent or search warrant to utilize extraction tools on a device. A certified user within TESU conducts the extraction and provides the entirety of the data to the requesting Officer/Detective for the investigation file and then deletes all data from the extraction tool. Each deployment is logged, and all request forms are maintained within TESU.

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

Data extraction devices are utilized only after legal standards of consent or court-issued warrant have been met.

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.

Select users in the SAU and TESU units are trained in the use of data extraction devices. These users must attend extensive training and vendor certification prior to being authorized to perform extractions and continuing training re-certification that is available through the technology provider.

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.

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.

Extraction tools of mobile devices, excluding computer imaging, collects information from electronic devices, including contact lists, call logs, Short Messaging Service (SMS) and Multi-Media Messaging Service (MMS) messages, and GPS locations. Computer imaging collects an entire image of a computer's hard drive at a specific point in time.

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

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

Use of extraction tools is constrained by consent or court order providing the legal authority. All deployments of extraction tools are documented and subject to audit by the Office of Inspector General and the federal monitor at any time.

If no data is collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the consent form and/or court order warrant (as determined by the judge), the device is purged in its entirety and no data is provided to the requesting Officer/Detective for the investigation file.

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?

Officers/Detectives provide written consent and/or a court approved warrant for all uses of extraction tools. Unit supervisors are responsible for screening all technology deployments to ensure that the appropriate authorities are in place before approving deployment of tracking technology. Specific individuals within each appropriate unit (see 3.1 above) are certified and trained to conduct extraction and/or imaging.

4.4 How often will the technology be in operation?

Extraction tools are used, as appropriate, when supported by consent or a search warrant, in conjunction with an active investigation.

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

Temporary.

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?

Extraction tools are not necessarily visible to the public. Owners are aware of their use with consent. They are often aware of their use with a search warrant.

Extraction tools are most often used within SPD, in a unit's lab or workstation. On occasion, extraction may be utilized in the field. The tools themselves contain no markings.

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

Only authorized SPD users can access the device or the extracted/imaged data while it resides in the extraction/imaging software. Access to the software is limited to Detectives via password-protected login information.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel. Access to data extracted by SAU, such as depictions of minors engaged in acts of sexually explicit conduct, is controlled by Federal and State law. SAU data is stored on a separate secured server with access limited to authorized SPD SAU users.

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

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

No entity, other than SPD personnel, utilize the technology.

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

In order to deploy and utilize extraction tools, TESU and SAU require that Officers/Detectives submit a request form that requires proof of consent or search warrant, and active investigation. Extracted data is provided to Officers/Detectives to include with their investigation files.

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.)?

SAU: Only authorized users within SAU have access to the extraction tools. Request forms are collected that include copies of consent or search warrant. Extracted data is provided to the requesting Officer/Detective for the investigation file.

TESU: Requesting Officers/Detectives collect request forms that include copies of consent or search warrant to utilize extraction tools. Data is extracted per the request and provided to the requesting Officer/Detective. TESU then destroys all extracted data, maintaining nothing.

Logs of collected information are available for audit.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

Once the data has been extracted and provided to the investigating detective for inclusion in the investigation file, all data is purged from the extraction devices. Evidence data is stored per the requirements established within SPD Manual Title 7 – Evidence and Property.

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

Each unit with extraction tools collects request forms and/or copies of consent or search warrant. The Office of Inspector General and the federal monitor can access all data and audit for compliance at any time.

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

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense (GO) Report.

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

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

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

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD.

SPD’s Intelligence and Analysis Section reviews the audit logs and ensures compliance with all regulations and requirements.

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.

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, has direct access to the data extraction devices or the data while it resides in the device.

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 these data extraction devices 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 devices.

6.2 Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission of contributing to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigation, and to comply with legal requirements.

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

Yes ☒ No ☐

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

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

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

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

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

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or manner in which the extraction tool systems may be used.

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

Generally, extraction tool systems do not check for accuracy; however, with the exception of computer imaging, the technologies generate a hash value for every extraction that compares the data at two points in time to ensure data integrity. Additionally, users can manually confirm that the information in a report generated from an extraction matches what it is in the manual logs.

Computer imaging is a direct snapshot of a computer's hard drive.

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

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

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?

Each application and utilization of extraction tools is authorized by consent, pursuant to search warrant authority, or in certain circumstances outlined in RCW 9.73.210.

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

SPD Policy 12.050 mandates that all employees, including those utilizing extraction tools, receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training.

Additionally, specific to extraction tools, all users have undergone certification by the requisite vendors.

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.

Extracted data is collected for individuals involved in criminal investigations wherein legal authority exists to apply the technology. Privacy risks imposed by the collection of personal information from private devices, such as the concern that data may be accessed out of scope, are mitigated by the consent/warrant requirement, supervisory approval requirement, and authority to audit access and use of the technologies by the Office of the Inspector General and the federal monitor.

Additionally, all SPD personnel receive Security Awareness Training (Level 2) and City Privacy Training.

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?

Extraction tools have the capacity to access large amounts of very private and personal information of individuals. Without the appropriate safeguards, these tools could seem to be unreasonable intrusions of privacy.

As it relates to extraction tools themselves, use is authorized, and constrained, only by consent or search warrant.

As it relates to sharing of information collected from extraction tools, SPD does share some information obtained with non-City entities in the context of particular cases (i.e., investigative records are shared with the defense in criminal prosecution); however, SPD does not share access to the technology.

8.0 Monitoring and Enforcement

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

Each owning unit maintains logs of deployment. These logs are available for audit, both internally and externally.

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

Any requests for public disclosure are logged by SPD's Public Disclosure Unit. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained 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.

No formal audits exist for extraction tool requests or deployments; however, requests to utilize extraction tools, as well as logs of deployments, are kept within each unit, and are subject to audit by the unit supervisors, Office of the Inspector General, and the federal monitor at any time.

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
Prior to 2011	-	-	-	-	-

Notes:

Initial acquisition occurred prior to 2011.

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
Approximately $200,000 for annual licensing across platforms for both TESU and SAU Units combined	-	-	None- No IT Support	GRANT FUNDED - 2018-MC-FX-K054/ USSS Task Force/ ICAC state allocation

Notes:

GRANT FUNDED - 2018-MC-FX-K054/ USSS Task Force/ ICAC state allocation

1.3 Cost savings potential through use of the technology

Data extraction devices are used with consent and/or search warrant to resolve investigations. They provide invaluable evidence that could not be calculated in work hours.

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

GRANT FUNDED - 2018-MC-FX-K054/ USSS Task Force/ ICAC state allocation

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
N/A	N/A	N/A

2.0 Academics, Consultants, and Other Experts

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

Agency, municipality, etc.	Primary contact	Description of current use
N/A	N/A	N/A

3.0 White Papers or Other Documents

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

Title	Publication	Link
N/A	N/A	N/A

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?

Without appropriate policies, extraction tools could be used to surveil individuals without reasonable suspicion of having committed a crime. This concern is mitigated by the requirement that these technologies be applied only after obtaining appropriate legal authority or consent.

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. To mitigate the risks for racial or ethnicity-based bias in the use of these data extraction tools, these devices are utilized only with consent and/or court-ordered warrant, having established probable cause.

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

☒ all Seattle neighborhoods

☐ Ballard
☐ Belltown
☐ Beacon Hill
☐ Capitol Hill
☐ Central District
☐ Columbia City
☐ Delridge
☐ First Hill
☐ Georgetown
☐ Greenwood / Phinney
☐ International District
☐ Interbay
☐ North
☐ Northeast

☐ Northwest
☐ Madison Park / Madison Valley
☐ Magnolia
☐ Rainier Beach
☐ Ravenna / Laurelhurst
☐ South Lake Union / Eastlake
☐ Southeast
☐ Southwest
☐ South Park
☐ Wallingford / Fremont
☐ West Seattle
☐ King county (outside Seattle)
☐ Outside King County.

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

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

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

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

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?

Data extraction tools are used exclusively during the investigation of crimes and only with consent and/or court-ordered warrant, having established probable cause. There is no distinction in the levels of service SPD provides to the various and diverse neighborhoods, communities, or individuals within the city.

All use of the data extraction tools must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

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. Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process.

In an effort to mitigate the possibility of disparate impact on historically targeted communities, 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.

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. The information obtained by the data extraction tools is related only to criminal investigations 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 / have you taken to ensure these consequences do not occur.

The most important unintended possible consequence related to the continued utilization of the data extraction tools is the possibility that the civil rights of individuals may be compromised by unlawful surveillance. SPD mitigates this risk by requiring consent and/or a court-ordered warrant, having established probable cause, prior to the utilization of these technologies.

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.	2.	3.

2.1 Scheduled public meeting(s).

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

Location	
Time	
Capacity	
Link to URL Invite	

2.2 Scheduled focus Group Meeting(s)

Meeting 1

Community Engaged	
Date	

Meeting 2

Community Engaged	
Date	

3.0 Public Comment Analysis

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

3.1 Summary of Response Volume

Dashboard of respondent demographics.

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

Dashboard of respondent demographics.

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

Dashboard of respondent demographics.

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

Dashboard of respondent demographics.

3.5 Question Four: General response to the technology.

Dashboard of respondent demographics.

3.5 General Surveillance Comments

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

Dashboard of respondent demographics.

4.0 Response to Public Comments

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

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

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

5.0 Equity Annual Reporting

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

Respond here.

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.

Submitting Department Response

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.

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.

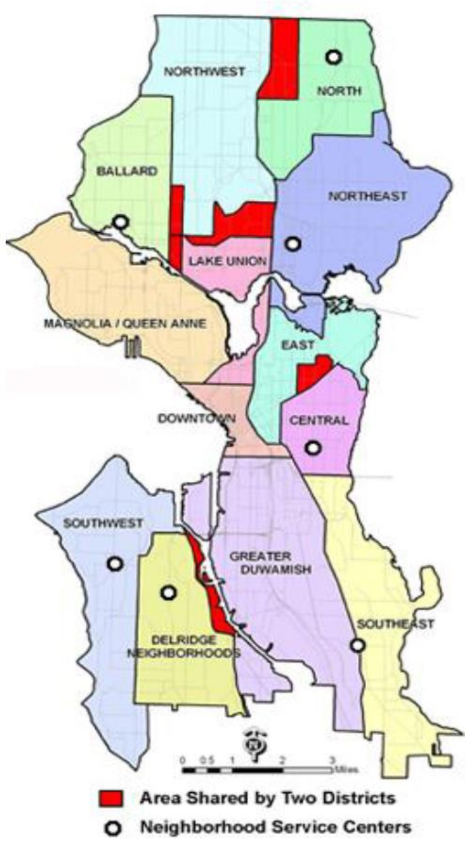
RET: “racial equity toolkit”

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: Public Comment Analysis

Appendix C: Public Comment Demographics

Appendix D: Comment Analysis Methodology

Appendix E: Questions and Department Responses

Appendix F: Public Outreach Overview

Appendix G: Meeting Notice(s)

Appendix H: Meeting Sign-in Sheet(s)

Appendix I: All Comments Received from Members of the Public

Appendix J: Letters from Organizations or Commissions

Appendix K: Supporting Policy Documentation

Appendix L: CTO Notification of Surveillance Technology