City of Seattle

## 2022 Surveillance Impact Report

# Computer, Cellphone, & Mobile Device Extraction Tools

## Seattle Police Department

City of Seattle

# 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 | City Council will decide on the use of the surveillance technology, by full Council vote. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | SIR and submitted to Council. | |

City of Seattle

# 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.

City of Seattle

# 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 |

City of Seattle

# 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 Scheduled public meeting(s).**

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

| **Location** | **Virtual (Webex)** |
|---|---|
| **Time** | Wednesday, Apr 27, 2022 3:00 pm |

| **Location** | **Virtual (Webex)** |
|---|---|
| **Time** | Wednesday, May 18, 2022 3:00 pm |

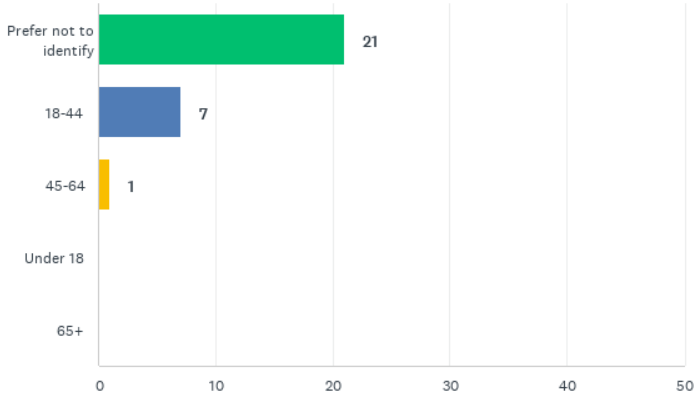
## 3.0 Public Comment Analysis

Note: 10 comments were received via email. Demographics and analysis was not conducted on these comments but are included in the Appendix containing all public comments.

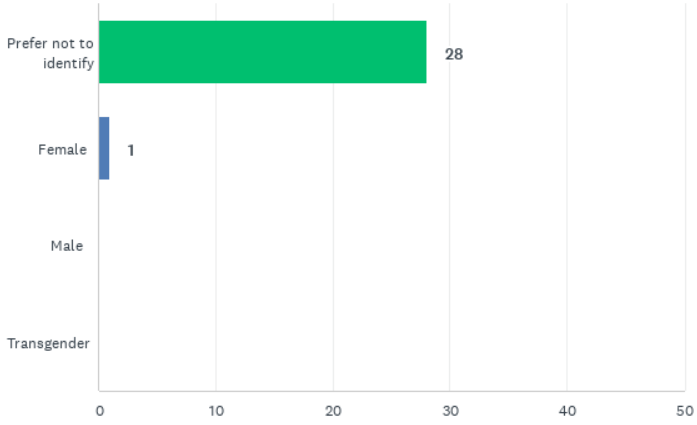
Due to low comment volume on individual technologies, analysis of comments was conducted across the group of technologies.

### 3.1 Summary of Response Volume

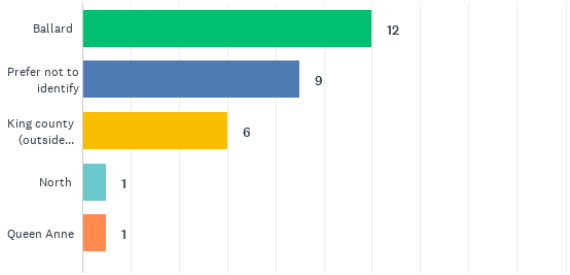
Q7 Which age range are you are currently in?

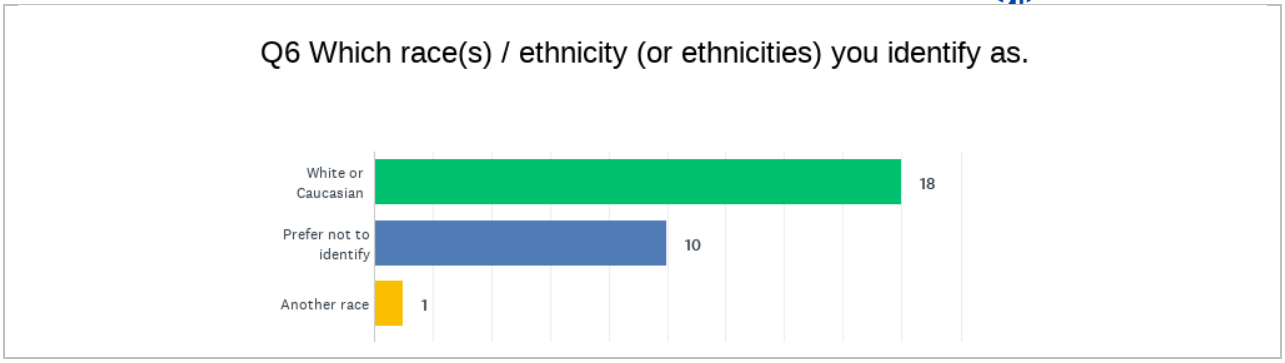



Q8 What gender do you identify as?

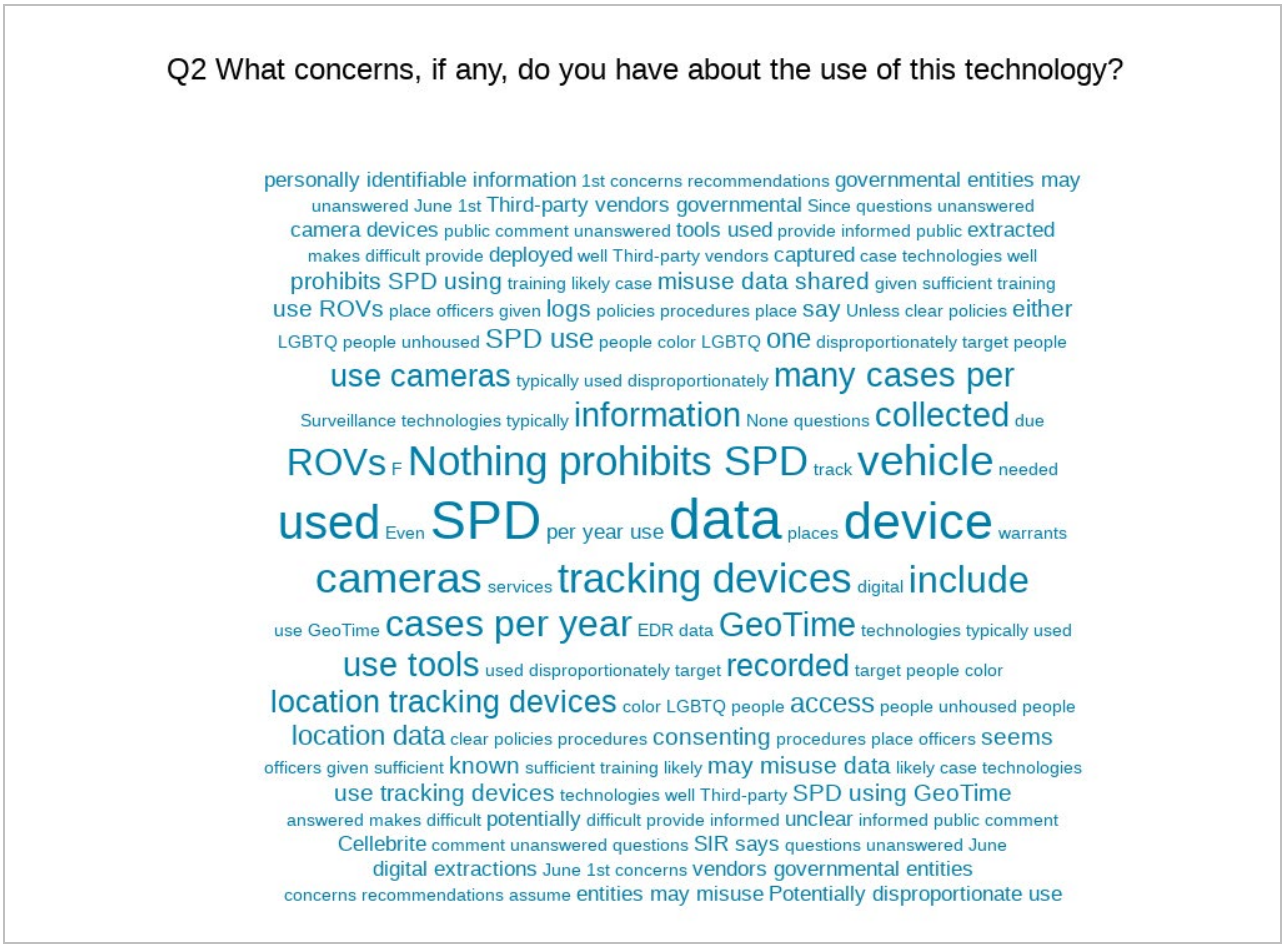



Q9 Which neighborhood do you currently reside in?



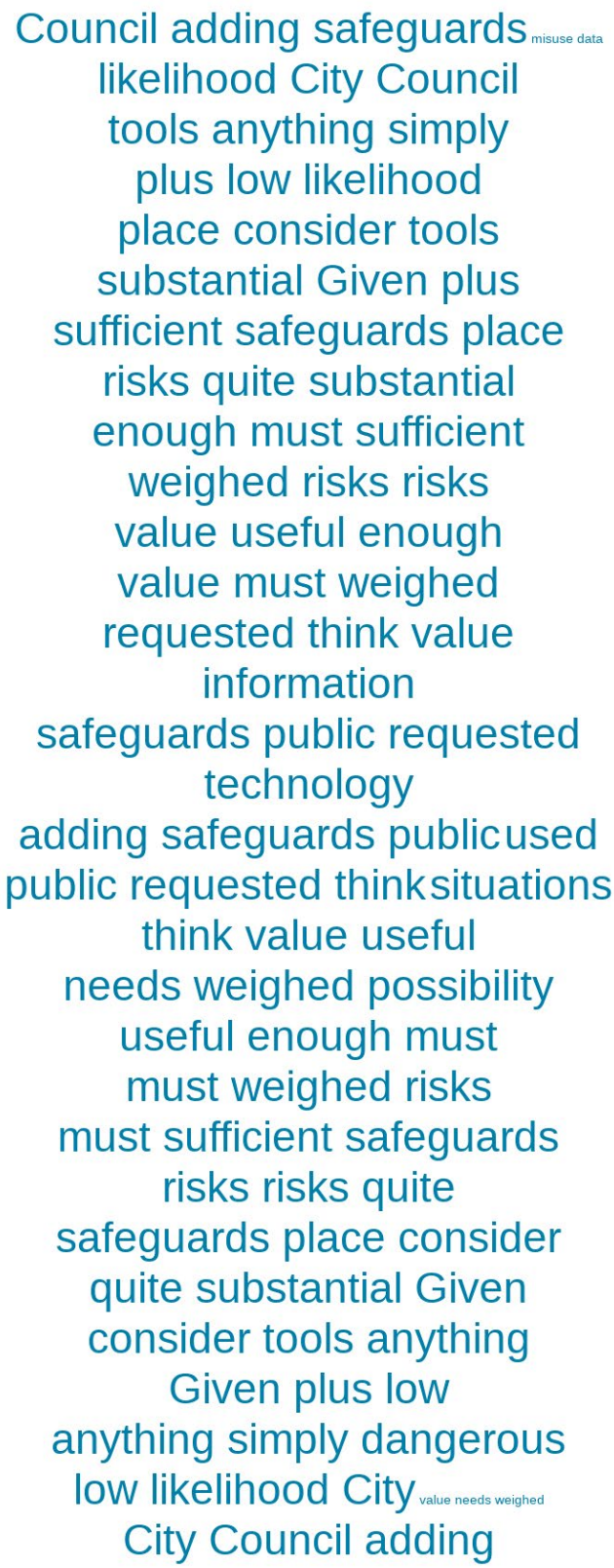



### 3.2 Question One: What concerns, if any, do you have about the use of this technology?




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

Q3 What value, if any, do you see in the use of this technology?



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


### 3.5 Question Four: General response to the technology.


## 4.0 Response to Public Comments

### 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.

City of Seattle

# 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."

City of Seattle

## Working Group Privacy and Civil Liberties Assessment

From: Seattle Community Surveillance Working Group (CSWG)

To: Seattle City Council

Date: August 4, 2022

Re: Privacy and Civil Liberties Impact Assessment for Computer, Cell Phone, and Mobile Device Extraction Tools

**Executive Summary**

The CSWG has completed its review of the Surveillance Impact Reports (SIRs) for the six surveillance technologies included in Group 4b of the Seattle Surveillance Ordinance technology review process. These technologies are GeoTime; Computer, Cell Phone, and Mobile Device Extraction Tools; Camera Systems; Remotely Operated Vehicles; Crash Data Retrieval; and Tracking Devices. This document is the CSWG's Privacy and Civil Liberties Impact Assessment for Computer, Cell Phone, and Mobile Device Extraction Tools used by Seattle Police Department (SPD) as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

This document first provides our recommendations to Council, then provides background information, key concerns, and outstanding questions regarding Computer, Cell Phone, and Mobile Device Extraction Tools (Mobile Device Forensic Tools – MDFTs).

Our assessment of Computer, Cell Phone, and Mobile Device Extraction Tools as used by Seattle Police Department (SPD) focuses on the following major issues.

1. No prohibition on inherently coercive "consent searches".
2. No transparency on MDFT vendor names and model numbers.
3. Inadequate policies defining purpose limitations for MDFT use.
4. No transparency and inadequate policies on data storage, safeguards, and retention.

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

1. There must be a prohibition on the use of consent searches of computer, cell phone, and mobile devices.
2. The purpose and allowable uses of MDFTs must be clearly defined, and any SPD use of MDFTs must be limited to that specific purpose and those allowable uses. The specific incident types for which MDFTs may be used must be specified. For example, the use of MDFTs should be restricted to only cases involving an event type flagged in the system as a violent and/or serious offense involving a non-property crime.
3. The MDFT vendor names, model numbers, purchase orders, and contracts must be publicly disclosed.
4. SPD must be prohibited from signing a non-disclosure agreement with any manufacturer, vendor, or reseller of MDFTs.
5. Each use of a MDFT must be registered with the city and compiled into a publicly available transparency report on at least a monthly basis. This report must include at a minimum:
    a. How many phones were searched in a given time period;
    b. When the search occurred and if it is ongoing;

   c. Whether those searches were by consent (though consent searches should be banned) or through a warrant;
   d. Warrant numbers associated with searches, when applicable;
   e. How many individuals and devices searched;
   f. The types of offenses being investigated;
   g. How often MDFTs resulted in an arrest or conviction;
   h. Whether the extracted data were shared with or uploaded to any other software program, entity, company, agency, or person, and their names;
   i. Explanations for any failed extractions;
   j. Whether the use of the MDFT was associated with a political protest, demonstration, or other public assembly, and whether the extraction data has been shared with or uploaded to any other software program, entity, company, agency or person, and their names.
6. Any information obtained through the execution of a warrant that is unrelated to the objective of the warrant must be destroyed within thirty days after the information is seized and be not subject to further review, use, or disclosure.
7. MDFTs used by SPD must have clear recordkeeping functions, specifically detailed audit logs and automatic screen recording.
8. All MDFT data must be promptly deleted if charges are dismissed or do not result in a conviction.
9. There must be strong access controls in place for licensed workstations as well as for access to extracted data on whatever medium they exist, including removeable physical storage such as a portable USB device.
10. There must be adequate training for all personnel who use MDFTs and the training must include a privacy component specific to the risks inherent to using MDFTs as an investigative tool.

**Key Concerns**

1. **No Transparency on MDFT Vendor Names, Product Names, and the number of Licenses SPD owns**. The SIR does not disclose vendor names, product names, or the number of licenses. Without this information it is challenging to comprehensively assess the impacts of SPD's use of MDFTs on privacy rights and civil liberties, as well as SPD's need for this technology.

2. **Lack of Policy on Purpose of Use and Usage Limits.** The SIR does not fully explain use cases for MDFTs and does not include policies placing limits on its uses.

   a. **No Limits on Scope of Data Collection.** The SIR does not specify how SPD creates limitation on data collection if the detective is given the entire contents of a device. There are no measures that constrain or minimize inadvertent or improper data collection.
   b. **No Limits on Type of Offense or Investigation.** The SIR does not specify limitations on which offenses or investigations for which MDFTs may be used (e.g., First Amendment demonstrations or petty crimes).
   c. **No Limits on Tools MDFTs May Interface with.** The SIR does not specify any limitations on technologies that MDFTs may interface with.

3. **Lack of Clarity and Transparency on What Other Technologies MDFTs Interface with.** The SIR does not specify which other technologies, if any, SPD uses in conjunction with MDFTs. The GeoTime SIR states that its data sources include cell phone extraction devices, but MDFT use with GeoTime is made clear in the MDFT SIR. MDFTs are capable of interfacing with a host of other technologies. Without this information, it is difficult to adequately assess the privacy risks posed by SPD's use of MDFTs.

4. **Lack of Legitimacy of "Consent-Based" Use of MDFTs and Lack of Clarity on How Consent Is Obtained.** "Consent searches" are inherently coercive given the power and information

asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law enforcement, and individuals may fear that refusing to give their consent to police will lead to deadly consequences. Many states ban consent searches at traffic stops, and California and New jersey have banned consent searches for minors, recognizing this racialized power imbalance. A recent study designed "specifically to examine the psychology of consent searches" found that when participants were brought into a laboratory and presented with a "highly invasive request" to allow an experimenter unsupervised access to their unlocked smartphone, more than 97% of participants handed over their phone to be searched, even though only 14.1% of a separate group of observers said that a "reasonable person" would hand over their phone in such a situation." Additionally, when individuals give consent to police to see their text messages or another specific category of data with the assumption that police will look at the phone manually, many individuals may not understand that the police will actually perform full extractions using MDFTs and retain that data indefinitely.

5. **No Transparency on How Many and Which Personnel Have Access to MDFTs and Any Extracted Data.** The SIR does not specify who qualifies as an "authorized user or detective.

6. **Low Threshold for MDFT Deployment.** The SIR states: "As it relates to extraction tools themselves, use is authorized, and constrained, only by consent or search warrant." There is no indication there are any criteria for determining whether use of MDFTs is warranted or appropriate in the first place, despite the invasiveness of the technology and the lack of limitations on the scope of data collection via these tools.

7. **Lack of Transparency and Inadequate Policies on Data Storage, Safeguards, and Retention.** The SIR provides only a vague description of how extracted data are stored, safeguarded, and for how long they are retained. It states that "once the data has been extracted and provided to the investigating detective for inclusion in the investigative file, all data is purged from the extraction devices." This leaves out critical details about what access control mechanisms are in place.

8. **Inadequate Policies to Mitigate Inadvertent or Unauthorized Data Collection.** No access controls are specified for TESU extraction requests or data extracted by TESU. Once data has been extracted, the MDFT can "either save files to removable physical storage or a computer workstation. These extracted data files are then accessed using the specialized installed software, which enable the user to examine and search the data. However, the SIR does not specify what access control mechanisms are in place for accessing this software and the data on it, including whether data are encrypted. This is concerning as it puts private data at risk of being improperly accessed and searched.

9. **Inadequate Data Sharing Policies.** The SIR states that SPD may share extracted data "with other agencies, entities, and individuals" outside of SPD, which presumably includes agencies from outside the state. However, it does not specify under what circumstances data would be shared or the policies and practices in place that govern data storage, retention, and transfer to protect the data. It also does not indicate whether and how these disclosures are documented.

10. **Lack of Clarity and Transparency on How Often MDFTs are Deployed.** The SIR does not specify how often MDFTs are deployed. Without this information, it is difficult to adequately assess the impacts on privacy rights and civil liberties, as well as SPD's need for this technology.

11. **SPD uses MDFTs to Extract Data from Devices of Minors.** The Upturn report on MDFTs provides evidence via public records that SPD uses MDFTs to extract data from the device of minors. However, the SIR does not mention this fact. When asked at the 5/18/22 public engagement meeting about what percentage of devices SPD extracts belong to minors, the SPD representative claimed they do not have that data, which suggests SPD does not collect data on the demographics of the people whose phones they search. The use of MDFTs to search the phones of minors is very concerning, given that minors are a vulnerable population and are entitled under law to extra protections to safeguard their rights. Moreover, the lack of data collection on MDFT use makes it challenging, if not impossible to detect whether there is bias in SPD's use of MDFTs.

12. **Inadequate Oversight and Auditing Policies.** It is unclear if there have been any audits at all, and if so, if they are publicly available. It is unclear what percentage of deployments have been audited by the Office of the Inspector General and SPD's Intelligence and Analysis Section. It is unclear if any audits have specifically assessed discriminatory uses. Without detailed auditing capabilities, or regular auditing, it is not possible to have sufficient oversight of SPD's use of MDFTs.

**Outstanding Questions**

1. Which vendor(s) provide SPD the extraction tools they use?
2. Which extraction tools and how many does SPD currently own?
3. How many licenses does SPD have for each MDFT product?
4. What is the cost to obtain and maintain each? What funding source(s) does SPD use to cover these costs/expenditures?
5. With what frequency/how often does SPD use extraction tools?
    a. How many times a week/for how many investigations a week is it used?
6. Besides child sexual assault and child abuse investigations, what kinds of investigations are extraction tools used for? Describe the range of investigations and what kinds of investigations they are mostly used for.
7. How often are extraction tools used in the field vs. at a unit work station? Under what circumstances are they used in the field vs. at a unit work station?
8. What does the training and certification for these extraction devices entail?
    a. How many hours of training do they receive? What does the training cover?
    b. Do they receive periodic updated training?
    c. Is there a privacy component to the training that is specific to the privacy risks of this tech? (response to 7.2 indicates no.)
9. What does the process of obtaining consent from the phone owner look like?
    a. In what context does an officer/detective typically ask a person for consent to access their phone?
    b. At the 5/18/22 public engagement meeting, the SPD representative indicated that a person can consult a lawyer before signing the form. Is that something the person is explicitly informed of?
    c. Is there a script that officers/detectives follow when obtaining consent? If so, what does that script say?
    d. What information is the phone owner provided about how their data will be extracted and what data? Is the person informed both verbally and in writing that the extraction tool will extract a full copy of data from their device—all emails, texts, photos, location, app data and more—which can then be programmatically searched?

   e. Does policy require that non-English speakers be taken through the consent process in their native language?
   f. Does policy permit SPD to seek consent from minors to search their device with MDFTs? If so, how does that process differ, if at all, from the process used for non-minors?
10. When an officer/detective makes a request to a supervisor to use a data extraction tool, are they required by policy to articulate something they are specifically looking for?
11. What policies and practices and/or procedures limit the scope of data SPD extracts with MDFTs?
12. How does SPD safeguard the data of people on the device who are not under investigation (i.e., smart phones usually contain the private data of other people, such as location data from photos or social media pages)?
13. What policies and practices and/or procedures minimize improper or inadvertent data collection?
14. Question 4.10 of the SIR asks about safeguards in place for protecting data from unauthorized access and to provide an audit trail. SPDS's response is not very detailed or satisfactory. What safeguards are in place for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (view logging, modification logging, etc.)?
15. How are device data safeguarded when the device is sent to the vendor for extraction? How does SPD ensure that vendors providing "Advanced Services" don't receive improper/unauthorized access to device data?
16. How often is a deployment audit performed? How often is a request audit performed? When was the last time an audit was performed for each?
17. The SIR states: "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." How much time is data typically stored on an extraction device before it is downloaded to the investigation file? Is it immediate? Is deletion of data on the extraction device also immediate? Is that reflected in the training?
18. What other technologies, if any, do MDFTs interface with? What policies, if any, limit the technologies that MDFTs interface with?
19. Is any information extracted with MDFTs shard with Fusion Centers?
20. Who has access to the data on the extraction device? What constitutes an "authorized user"? How many "authorized users" within SPD have access to the data?
21. Who within SPD has access to the data once it has been downloaded out of the extraction tool? How many people have access?
22. Which agencies, entities and individuals outside of SPD can SPD share extracted data with? Are these disclosures documented? If so, where and how?
23. What data storage, retention and transfer/sharing safeguards in place to protect the data?
24. Are data obtained via extraction tools subject to the PRA?

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

City of Seattle

# Memo

**To:** Seattle City Council

**From:** Jim Loter, Interim Chief Technology Officer

**Subject:** CTO Response to the Surveillance Working Group Computer, Cellphone, & Mobile Device Extraction Tools SIR Review

---

## Purpose

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department's Computer, Cellphone, & Mobile Device Extraction Tools.

## Background

The Information Technology Department (ITD) is dedicated to the Privacy Principles and Surveillance Ordinance objectives to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. IT and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

## Technology Purpose

The Seattle Police Department (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.

## Working Group Concerns

In their review, the Working Group has raised concerns about these devices being used in a privacy impacting way, including data collection, sharing, retention, deletion, storage, and protection.
We believe that policy, training and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this operational technology.

*Note: The Working Group refers to Computer, cellphone and mobile device extraction tools as "Mobile Device Forensic Tools" or MDFTs.*

## Recommended Next Steps

I look forward to working together with Council and City departments to ensure continued transparency about the use of these technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about this technology are addressed in the attached document.

City of Seattle

# Response to Specific Concerns: Computer, Cellphone, & Mobile Device Extraction Tools

## Concern: No Transparency on MDFT Vendor Names, Product Names, and the number of Licenses SPD owns

**CTO Assessment:** The policies in place in the SIR and SPD manual operate regardless of the manufacturer or model of the devices. The conditions under which the devices are used are clearly outlined in the SIR and are further regulated by RCW 9.73.

**SIR Response:**
Section 2.3
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.

## Concern: Lack of Policy on Purpose of Use and Usage Limits

- **Scope of Data Collection**
- **Limits on Type of Offense or Investigation**
- **Limits on Tools Extraction Tools May Interface With**

**CTO Assessment:** The policies in place in the SIR and SPD manual govern the use of data collected by Computer, Cellphone, & Mobile Device Extraction Tools and the circumstances under which they will be used, including in prosecutions. The conditions under which the devices are used are clearly outlined in the SIR and are further regulated by RCW 9.73. These technologies are operated under the authorization of a warrant from a court. Warrant and consent procedures are governed by state and federal law.

**SIR Response:**
Section 4.3
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.

Section 4.9

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.

Section 7.1
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.

## Concern: Lack of Clarity and Transparency on What Other Technologies MDFTs Interface with

**CTO Assessment:** The SIR covers the technologies used to extract information from electronic devices. Once the information is collected off of the device, it is handled according to SPD digital evidence management policies.

**SIR Response:**
Section 4.1
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."

## Concern: Lack of Legitimacy of "Consent-Based" Use of MDFTs and Lack of Clarity on How Consent Is Obtained

**CTO Assessment:** The SIR contains discrete sections relating to each of the concerns in addition to additional policies governing the use in the SPD manual and state law (RCW 9.73). As the data collected from these systems are primarily intended in use for criminal prosecution, there are other superseding policies and procedures that must be followed (circumstances around sharing or retention for example).

**SIR Response:**
Section 4.6
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.

## Concern: No Transparency on How Many and Which Personnel Have Access to MDFTs and Any Extracted Data.

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

**SIR Response:**
Section 4.3
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.

Section 4.7
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.

Section 4.10
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.

## Concern: Low Threshold for MDFT Deployment

**CTO Assessment:** Data extraction devices are utilized only after legal standards of consent or court-issued warrant have been met. These technologies are deployed within the Sexual Assault and Child

Abuse Unit which is the lead agency for the Washington Internet Crimes Against Children Task Force. The other unit, the Technical and Electronic Support Unit, only provides assistance with extraction tools after evidence of consent or search warrant authorization.

**SIR Response:**
Section 4.3
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.

Section 4.9
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.

Section 7.1
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.

## Concern: Lack of Transparency and Inadequate Policies on Data Storage, Safeguards, and Retention

**CTO Assessment:** Data collected from extraction tools are treated as evidence, which is stored securely in line with SPD policy, CJIS Security Policy, and other state and federal regulations relating to handling of law enforcement data.

**SIR Response:**
Section 4.10
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.

Section 5.1
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.

Section 5.2

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.

Section 5.4
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.

## Concern: Inadequate Policies to Mitigate Inadvertent or Unauthorized Data Collection

**CTO Assessment:** Specifically with computer imaging, the entire image of a hard drive is captured at that point in time. For mobile devices, information may include contact lists, call logs, text messages, and location data. As stated in the SIR, if no data collected is within scope of the consent form or warrant, the data is purged and not provided for any investigative purposes.

**SIR Response:**
Section 4.2
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.

Section 5.3
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.

## Concern: Inadequate Data Sharing Policies

**CTO Assessment:** No entities outside of SPD have direct access to the data or the device. Only evidence related to the investigation would be shared with identified partners in the SIR. Data sharing is a legal requirement for assisting with criminal prosecutions or complying with legal requirements with other law enforcement agencies.

**SIR Response:**

Section 6.1

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.

Section 6.2

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.

## Concern: Lack of Clarity and Transparency on How Often MDFTs are Deployed

**CTO Assessment:** Data extraction devices are utilized only after legal standards of consent or court-issued warrant have been met. These technologies are deployed within the Sexual Assault and Child Abuse Unit which is the lead agency for the Washington Internet Crimes Against Children Task Force. The other unit, the Technical and Electronic Support Unit only provides assistance with extraction tools after evidence of consent or search warrant authorization.

**SIR Response:**
Section 4.3
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 are certified and trained to conduct extraction and/or imaging.
Section 4.4
Extraction tools are used, as appropriate, when supported by consent or a search warrant, in conjunction with an active investigation.

## Concern: SPD uses MDFTs to Extract Data from Devices of Minors

**CTO Assessment:** The threshold of use or specific populations of cases of which an Extraction Tool is used is not a question represented in the SIR but may be part of the OIG's audit through the surveillance process.

**SIR Response: N/A**

## Concern: Inadequate Oversight and Auditing Policies

**CTO Assessment:** SPD has existing audit functionality with the Office of Inspector General, unit supervisors, or the federal monitor. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, the Surveillance Ordinance does mandate yearly auditing of these technologies by the Office of Inspector General and the IT department in some circumstances.

**SIR Response:**
Section 8.1
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.

Section 8.2

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.

# 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.

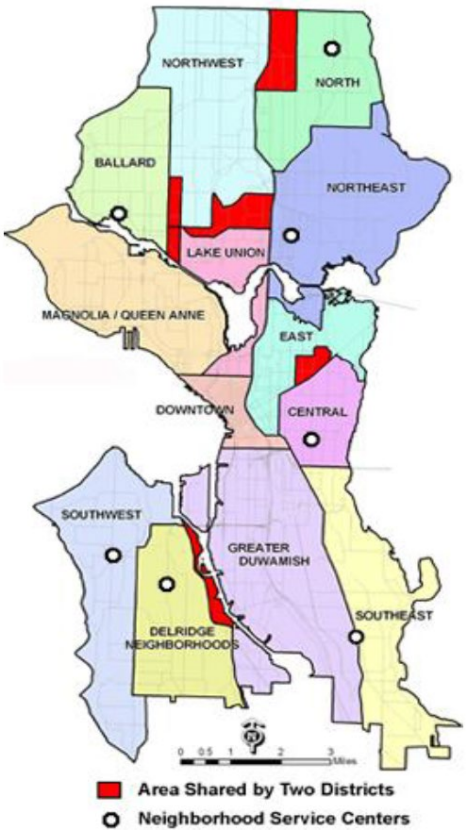
**RET**: "racial equity toolkit"

**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)

Seattle

## Tech Talk

Seattle Information Technology

Home / Privacy

<< Previous Next >>

## City's Surveillance Ordinance Virtual Event Wednesday, April 27, 3-4:30 p.m.

by Seattle IT on April 25, 2022

The City will host the first of two virtual presentations related to the City's Surveillance Ordinance this Wednesday, April 27 at 3 p.m. The virtual event facilitates the public comment period and will allow attendees to engage with the technology experts and hear from City leadership. These virtual events will take place using Webex and participants can join via online or by phone. Links and times for the event dates below can be found on the events calendar on the City's Surveillance Technologies website.
For more information on the public comment period read last week's blog post on *TechTalk*.

The next public virtual event will be on May 18. More information on these technologies, as well as the City of Seattle's Privacy program, can be found online at the City of Seattle's Privacy website.

Filed Under: Privacy
Tagged With: Surveillance, Surveillance technology

Share Tweet Pin Share Share Share

<< Previous Next >>

City of Seattle

# Public Comment Period Opening for Technologies Subject to the City's Surveillance Ordinance

by Seattle IT on April 18, 2022

The City of Seattle has published the fifth set of draft Surveillance Impact Reports (SIRs) for six of the 26 currently existing surveillance technologies, per the Surveillance Ordinance.

The City of Seattle is looking for the public's input on the SIRs to provide the City Council with community perspective and ensure the City's policies responsibly govern the use of these technologies.

The public comment period is currently open and runs through May 20, 2022. There are three ways for residents to provide input and share their concerns:

1. Residents can submit their surveillance comments on each technology online at: City of Seattle Privacy website.

2. Seattle residents can also mail comments to Attn: Surveillance & Privacy Program, Seattle IT, PO Box 94709, Seattle, WA 98124

3. City Surveillance Technology Events: The City will hold virtual events to allow attendees to engage with the technology experts and hear from City leadership. These virtual events will take place using Webex and participants can join via online or by phone. Links and times for the event dates below can be found on the events calendar on the City's Surveillance Technologies website. Scheduled event dates are:
Date and time:
Wednesday, Apr 27, 2022 3:00 pm
**Wednesday, May 18, 2022 3:00 pm**

Webinar topic:
Group 4b Surveillance Public Meeting

Next Date and time: **Wednesday, May 18, 2022 3:00 pm**

Join link: https://seattle.webex.com/seattle/j.php?MTID=m549182a7ee153d68cc332b28fe94e311

Webinar number:
2497 635 9688

Webinar password:
D6JhTcf5KU7 (36548235 from phones)

Join by phone
+1-206-207-1700 United States Toll (Seattle)
+1-408-418-9388 United States Toll
Access code: 248 062 39194

# Appendix D: Letters from Organizations or Commissions

City of Seattle

June 2, 2022

Seattle Information Technology
700 5th Ave, Suite 2700
Seattle, WA 98104

RE: ACLU of Washington Comments on Group 4b Surveillance Technologies

ACLU
AMERICAN CIVIL LIBERTIES UNION
Washington

P.O. Box 2728
Seattle, WA 98111-2728
(206) 624-2184
aclu-wa.org

Michele Storms
*Executive Director*

On behalf of the ACLU of Washington, we write to offer our comments on the surveillance technologies included in Group 4b of the Seattle Surveillance Ordinance implementation process.

The six Seattle Police Department (SPD) technologies in Group 4b are covered in the following order:

1. GeoTime
2. Mobile Device Extraction Tools
3. Camera Systems
4. Remotely Operated Vehicles
5. Crash Data Retrieval Tool
6. Tracking Devices

These comments should be considered preliminary, given that the Surveillance Impact Reports (SIR) for each technology leave a number of important questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology. Answers to these questions should be included in the updated SIRs provided to the Community Surveillance Working Group and to the City Council prior to their review of the technologies.

## GeoTime

### I. *Background*

GeoTime is a geospatial analysis software that visually maps data over space and time. It raises serious privacy and civil liberties concerns. These concerns are three-fold. First, GeoTime's data aggregation and analysis features are incredibly invasive. They enable law enforcement to gather and

create correlations between large amounts[1] of personal data from numerous sources at a time, including call detail records, mobile forensic data, GPS, location-tracking data, and social media data, creating very detailed, personalized maps of people's lives.[2]

Secondly, GeoTime's capabilities are excessively broad and intrusive. It creates links between people and reveals "patterns of behavior and relationships between seemingly unconnected events and entities,"[3] producing a dragnet that potentially captures the private data of those not involved in the crime or event being investigated. It may therefore implicate innocent individuals in a crime.

Lastly, and relatedly, GeoTime may be used to surveil and ultimately chill constitutionally protected activities concerning religion, expression, and assembly. For example, GeoTime advertises a "Trip Counter" feature, which enables users to "find new locations of interest [e.g. a mosque, an abortion clinic, or the site of an anti-police violence rally] and get quick answers. Who visited? How many times? When was each visit?"[4]

SPD has access to a potentially wide variety of undisclosed GeoTime products with various surveillance functionalities. GeoTime is owned by UnCharted Software, which sells a number of GeoTime products with various surveillance functionalities. The SIR does not disclose which GeoTime products SPD owns. At the 5/18/22 public engagement meeting with SPD, following up from a question asked at the first public engagement meeting on 4/18/22, the SPD representative stated that SPD owns two GeoTime Desktop licenses on computers secured in the Intel Unit and seven GeoTime Glimpse licenses that allow web access to the portal.[5] According to the SPD representative, three detectives have access to GeoTime and there is one detective who accesses it regularly.[6]

Though the SIR does not disclose GeoTime Desktop's functionalities or how they work,[7] there is evidence that SPD can use GeoTime to analyze

---

[1] On its website, GeoTime advertises that its "Enterprise" product can "handle millions of records at once." "GeoTime Enterprise," *GeoTime,* Accessed May 12, 2022, http://www.geotime.com/enterprise.

[2] The GeoTime website advertises that its "Desktop" product can "layer datasets to provide a comprehensive picture of activity." See "GeoTime Enterprise."

[3] "GeoTime for Analysis of Behavior in Time and Geography," *Oculus Info Inc.,* 2011, Accessed May 12, 2022, https://www.uncharted.software/assets/GeoTime_Overview.pdf.

[4] "GeoTime Desktop," *GeoTime*, Accessed May 12, 2022, https://www.geotime.com/desktop.

[5] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2," Accessed June 1, 2022, https://www.seattle.gov/event-calendar?trumbaEmbed=view%3Devent%26eventid%3D159435131

[6] Ibid.

[7] Seattle Police Department, "2022 Surveillance Impact Report: GeoTime," Accessed May 12, 2022,

social media data. At the 5/18/2022 public engagement meeting, the SPD representative, following up from a question at the first public engagement meeting, stated that SPD does not use the social media analysis functionality of GeoTime.[8] However, it remains unclear which of the remaining functionalities SPD does use. It should be noted that although SPD states they do not use the social media analysis functionality, it is unclear whether they can still input social media data into GeoTime in order to gain insights via the other functionalities such as the mobile device forensic analysis functionality. This functionality ostensibly analyzes data extracted from people's phones, which SPD has the capability to do with their mobile device extraction tools.[9] This strongly suggests that even without the social media analysis functionality, analysis of social media data is nevertheless something SPD can capably do with GeoTime, given that 99% of people access their social media from their mobile phone.[10] It is noteworthy that GeoTime Desktop can import data from Cellebrite,[11] one of the mobile device extraction tools that public records show SPD owns or has owned in the past.[12]

In general, SPD provides a very general and vague explanation of GeoTime's capabilities in the SIR that does not meaningfully convey the vast number of sources of personal and private data that SPD can aggregate and analyze within GeoTime, and the kinds of outputs it generates. The GPS analysis functionality alone, for example, can use the following data sources: automated license plate readers, transit pass, automated toll pass, crime incident data, witness/informant statements, in-vehicle GPS system, Google location history, Uber/Lyft location reports, and on-board vehicle data (e.g., odometer, speed, location logs, saved locations/routes, connected devices/media, call logs), among others.[13]

Despite how powerful this tool is, the SIR does not indicate use cases for GeoTime, or define limitations on the kinds of data sources that SPD can input. There is also a lack of clarity on the oversight measures in place, such as whether GeoTime has audit logs and what data those logs might collect. When asked at the 5/18/22 public engagement meeting about the last time

---

https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20%20Geotime.pdf.

[8] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

[9] Seattle Police Department, "2022 Surveillance Impact Report: Computer, Cellphone, & Mobile Device Extraction Tool," Accessed June 1, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Computer%2C%20Cellphone%2C%20%26%20Mobile%20Device%20Extraction%20Tools.pdf.

[10] Dean, Brian, *BackLinko*, "Social Network Usage & Growth Statistics: How Many People Use Social Media in 2022?, 2021, https://backlinko.com/social-media-users.

[11] "GeoTime Desktop."

[12] On file with the author.

[13] Khamisa, Adeel, "GeoTime: GPS Data Analysis – Tips and Best Practices," *GeoTimeInfo*, October 10, 2021, https://www.youtube.com/watch?v=oOUKjwDKCVo.

an audit was conducted, the SPD representative referred the question-asker to the Office of Inspector General (OIG), which strongly suggests that no audit has been done by OIG, and certainly no audit conducted by SPD's Audit, Policy, and Research Section (APRS—SPD's auditing body) or the federal monitor.[14] Moreover, the SIR does not indicate there are any validation measures for the data inputs, or outputs such as images, animated videos, or PowerPoint files of mapped data. When asked at the 5/18/22 public engagement meeting whether there are measures in place to verify the accuracy of GeoTime data and analyses, the SPD representative stated that this verification is part of the normal investigative process, and an SPD officer will validate GeoTime data and analyses.[15] This is troubling, given that GeoTime enables SPD to annotate maps/graphics & edit visualizations used as the output. It is also concerning because one of the supported file formats for imported data is an Excel file format, which can be edited.[16] This means SPD can modify or fabricate records that GeoTime analyzes. Without a way to track SPD's movements inside the application, it is hard to know whether data or the output has been tampered with or manipulated. This has high costs given that outputs are shared in court presentations, used as evidence, etc.

Another concern is the lack of clarity regarding how SPD obtains the data that GeoTime analyzes. For example, the SIR states that the data are obtained by investigators "under the execution of court ordered warrants, including data from cellular providers and from data extracted from mobile devices," and it cites to the Mobile Device Extraction Tools SIR.[17] However, this contradicts what is actually written in the Mobile Device Extraction Tools SIR, which is that mobile device forensic data can also be obtained via consent agreement with the mobile device owner.[18] Clarity is needed as to whether data can be obtained based on consent alone, what data can be obtained under consent agreement as opposed to search warrant, and under what circumstances. Moreover, there must be policies in place

Finally, there is a lack of clarity about who at SPD has access to GeoTime data inputs and outputs, with which entities outside SPD those data are shared (including law enforcement agencies outside the state), and how those data are shared. When asked about this at the 5/18/22 public engagement meeting, the SPD representative stated that SPD does share case info with other law enforcement agencies as it relates to

[14] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[15] Ibid.
[16] "Frequently Asked Questions," *GeoTime*, Accessed May 12, 2022, https://www.geotime.com/frequently-asked-questions.
[17] SPD, "GeoTime," 6.
[18] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 3.

investigations.[19] This is a particularly pressing issue given recent indications that the US Supreme Court is poised to overturn *Roe v. Wade*, and that states are ready to pass legislation criminalizing abortion.[20] Our state recognizes the individual right to abortion care and it is anticipated that Washington will see an influx of people from neighboring states seeking abortion services here.[21] GeoTime may be used to surveil these people and it is critical that there be restrictions on the ability of SPD to share these data and analysis with law enforcement and other agencies outside the state. Moreover, for any data that are shared, there should be stringent data storage, retention and transfer/sharing safeguards in place to protect the data.

Given the lack of adequate policies described by the SIR and the number of unanswered questions that remain, we have concerns that SPD's use of GeoTime may infringe upon people's civil rights and civil liberties.

## II. *Specific Concerns*

a. **Lack of Clarity on How Often GeoTime is Deployed and Who Determines Whether Deployment Will Occur.** According to the SIR, "GeoTime is utilized frequently by investigators during the investigation of crimes." Conversely, at the public engagement meeting on 4/27/22, SPD representative stated that SPD "rarely" used GeoTime. At the public engagement meeting on 5/18/22, the SPD representative stated that it is used 1-2 times a week by one detective.[22] It remains unclear how often GeoTime is deployed (e.g., how many times a week? For how many cases?). In addition, the SIR provides no information about who determines in which cases/when to use GeoTime.

b. **Lack of Clarity on What Data SPD Inputs Into GeoTime.** Regarding data that SPD manually inputs into GeoTime to produce visualizations, the SIR refers variously to "geodata, such as latitude

[19] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[20] Almanza, Emily Galvin, "The Criminalization of Abortion: What to Expect in a Post-Roe United States," May 6, 2022, https://www.teenvogue.com/story/criminalization-of-abortion-laws-roe.
[21] Ahmed, Tasnim, "As States Move to Restrict Abortion Access, Neighboring States Prepare for Surges in Demand, *CNN*, April 13, 2022, https://www.cnn.com/2022/04/13/health/neighboring-states-abortion-bans/index.html.
[22] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

and longitude" (4) and "location information," (4) "cell records," "cell site locations," (4) "criminal information," "data from cellular providers and from data extracted from mobile devices" (6), and "Personally Identifiable Information" (14). It does not provide a comprehensive list of data sources that GeoTime aggregates and analyzes.

c. **Lack of Clarity on How SPD Obtains the Data it Inputs into GeoTime.** The SIR states: "The data analyzed using GeoTime is obtained by investigators under execution of court ordered warrants, including data from cellular providers and from data extracted from mobile device."[23] This contradicts the Computer, Cellphone, & Mobile Device Extraction Tools SIR, which states that extraction tools are "used only with the device owner's consent, pursuant to search warrant authority or in certain circumstances outlined in RCW 9.73.210."[24] The implication is that search warrants are not the only means through which data are obtained. Relatedly, when asked at the 5/18/22 public engagement meeting about whether any private information without a warrant or any public data are ever added to GeoTime, the SPD representative stated that SPD does input public data.[25] He did not respond to the part of the question asking whether any private information without a warrant is added to GeoTime.

d. **Lack of Clarity on How SPD Accesses GeoTime and What Access Controls are in Place for GeoTime.** The SIR states that GeoTime can be accessed via licensed workstations and through an online internet portal.[26] It later states that "access to the application is limited to SPD personnel via password-protected login credentials. Data is securely input and used on SPD's password-protected network with access limited to authorized users."[27] It's unclear from this explanation: (1) what software-level security controls (authentication, authorization, logging, etc.) are in place for *both* the GeoTime workstations and for the portal; (2) whether they are the same access control mechanisms for both the portal and the workstations; and (3) where the internet accessible portal can be accessed from (e.g. can it be accessed from a cell phone?). Without

[23] SPD, "GeoTime," 6.
[24] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 5.
[25] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[26] Ibid., 5.
[27] Ibid., 9.

this information, it is difficult to assess the privacy risks and suggest measures to mitigate them.

e. **Lack of Clarity on Which SPD Personnel/Units and How Many Have Access to GeoTime.** In one part of the SIR, it states, "Only trained, backgrounded, and CJIS certified SPD detectives have access to GeoTime."[28] In a different part, it states that log-in credentials "are granted to employees with business needs to access GeoTime" without any elaboration on which employees and the definition of "business needs" (8). At the 5/18/22 public engagement meeting, an SPD representative stated that three detectives have access to GeoTime, and one of those three uses it regularly.[29] However, it remains unclear whether these are the only individuals in SPD who have access to GeoTime via both the licensed workstations and the internet portal. There is a large discrepancy between the number of licenses for the internet portal (7 GeoTime Glimpse licenses) and the number of people who purportedly have access (3).

f. **Lack of Clarity on Which SPD Personnel Have Access to Data Output Generated from GeoTime.** The SIR states that GeoTime is "used to aggregate and analyze data manually input by investigators and exports complex geospatial maps which users save into locally stored investigation files."[30] However, the SIR does not state which SPD employees has access to those exported files created by GeoTime and how many SPD employees have access to them.

g. **Lack of Clarity About Data Storage, Safeguards, and Retention.** In response to data storage and retention questions, the SIR states that GeoTime "does not collect information or data…No information is saved inside the GeoTime tool."[31] While it may be the case that technically GeoTime does not "collect" data, SPD manually inputs data into GeoTime to generate maps and other visualizations and that data must be hosted/stored somewhere. However, that location is not provided in the SIR. At the 4/27/22 public engagement meeting, the SPD representative stated the internet accessible portal is hosted by GeoTime (i.e., UnCharted Software) but the data that GeoTime uses are not

[28] Ibid., 5.
[29] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[30] SPD, "GeoTime," 7.
[31] Ibid.

hosted there and that he would have to check on where the data are stored.[32] The SIR also does not indicate for how long the data are stored/hosted in that location, what safeguards are in place to protect it, who has access to the data, including whether UnCharted Software stores or has access, and when that data must be deleted.

h. **Lack of adequate policy and practices for validating the accuracy of the data and the analysis that GeoTime provides.** In the SIR, SPD evades the question of how GeoTime checks the accuracy of the information collected by stating: "GeoTime does not collect information or data. It is a tool used to aggregate and analyze data manually input by investigators an exports complex geospatial maps…"[33] This response does not address what measures SPD takes to ensure that the data it inputs into GeoTime is accurate. It also does not address what steps it takes to validate the accuracy of the GeoTime data output/analysis. GeoTime is a powerful tech that purports to help investigators, among other things, "dispute an alibi or demonstrate criminal intent."[34] Without validation of its analyses, it could have deleterious impacts on the lives of the people whose data is inputted, including implicating the wrong person in a crime.

i. **Inadequate Oversight Policies.** In response to the question about safeguards in place for protecting data and to provide an audit trail, the SIR states the entities authorized to conduct audits but it does not address whether there are self-audits, third-party audits, or review. It also does not address whether GeoTime has an audit log or not, what that log contains if they in fact have one, and whether that log is sufficient to conduct an audit investigation. At the 4/27/22 public engagement meeting, the SPD representative expressed uncertainty about whether there is a direct audit log about what actions each user takes inside the application.[35] At the 5/18/22 public engagement meeting, when asked about the last time an audit was conducted on SPD's use of GeoTime, the SPD representative referred the questioner to OIG, which strongly suggests no audit has been conducted by OIG or any other entity, including APRS and the federal monitor.[36] Without detailed auditing capabilities, or regular auditing, it is not possible to have sufficient

[32] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[33] Ibid., 13.
[34] "Frequently Asked Questions."
[35] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #1," Accessed June 1, 2022, https://www.seattle.gov/event-calendar?trumbaEmbed=view%3Devent%26eventid%3D159435112.
[36] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

oversight into how SPD uses GeoTime and whether they are complying with policy.

j. **Lack of Clarity and Transparency on What Other Tech GeoTime Interfaces With.** The SIR does not specify which other tech, if any, GeoTime interfaces with. SPD stated at the 4/27/22 public engagement session that it doesn't interface with PredPol, Crime View or other predictive policing utility, yet when a member of the public asked if SPD would include that in the SIR, SPD's response was that it was "not a tenable option" for SPD to list all the tech that GeoTime does not interface with.[37] Without this information, it is difficult to adequately assess the privacy risks that GeoTime poses.

k. **Lack of Policy on Purpose of Use and Usage Limits.** The SIR does not fully explain use cases for GeoTime and does not include policies placing limits on its uses.
   i. **Visualization vs. Predictive Policing.** Without clearer usage limits, analyses provided by GeoTime might be used for predictive policing.
   ii. **Data.** There are ostensibly no policies governing limits on the kinds of data sources that can be manually input into GeoTime.
   iii. **Type of crime.** In response to the question of "what are acceptable reasons for access to the equipment and/or data collected?" the SIR states: "Data is only accessed as part of ongoing criminal investigations or under the City of Seattle Intelligence Ordinance."[38] It is not specified if there are limits to the type of events (e.g. First Amendment protected demonstrations) or crimes that SPD will investigate via GeoTime (e.g. petty crimes like graffiti and trespassing). At the 4/27/22 public engagement meeting, the SPD representative indicated there is no policy governing the incident types for which SPD may use GeoTime but claimed that "SPD doesn't have time to apply" GeoTime to "lower-level offenses."[39] The implication is that with more time and resources, there is nothing stopping SPD from using GeoTime to investigate more offenses, even minor ones.

[37] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #1."
[38] SPD, "GeoTime," 8.
[39] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #1."

l. **No Policies Restricting Use of GeoTime's Additional Surveillance Features.** The SIR does not provide sufficient information about what components of GeoTime SPD uses and doesn't use. For example, during the 4/27/22 public engagement meeting, when asked about SPD's use of GeoTime's Social Media Analysis functionality, the SPD representative stated SPD does not use this feature of GeoTime.[40] He claimed this fact was in the SIR, which it is not.[41] There also don't appear to be any policies restricting SPD's use of Social Media Functionality. Without a full accounting of the features of GeoTime that SPD uses, it is impossible to assess all the potential privacy risks. With regard to the Social Media Analysis Functionality in particular, social media data will include the private information of non-targeted people so if SPD is using it, measures are necessary to ensure those data are protected and not misused in the GeoTime analysis.

m. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share GeoTime data and analyses with outside entities[42] but does not address whether SPD maintains a record of those disclosures. It only addresses recording of public disclosure requests made pursuant to the Public Records Act and the City of Seattle Intelligence Ordinance. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

n. **Inadequate Data Sharing Policies.** The SIR offers only an extremely general description of who might receive GeoTime data and analyses and how such data would be shared. Neither security protocols for transferring data nor for ensuring that shared data are properly deleted are explicated in the SIR. Indefinite retention of data and insecure sharing processes could lead to exposure of sensitive data, with manifold consequences for those whose data is inputted into GeoTime.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

[40] Ibid.
[41] SPD, "GeoTime."
[42] Ibid., 11.

a. Which GeoTime functionalities does SPD use?
b. Which SPD units have access to GeoTime? How many SPD employees have direct access to GeoTime, both via GeoTime Glimpse (internet portal) and GeoTime Desktop (workstations)?
c. Which SPD units have access to the files (e.g. maps and other visuals) generated by GeoTime? How many SPD personnel have access to those files? What other agencies or groups outside of SPD that have access to GeoTime files?
d. What other technology does GeoTime interface with?
e. What are all the data sources that SPD inputs into GeoTime?
f. Can data manually input into GeoTime be obtained without a warrant and based on two-party consent alone? If so, under what circumstances may the data be obtained without a warrant and what rules set the parameters for GeoTime's use?
g. How often is GeoTime deployed? How many times/for how many investigations a week is it deployed?
h. Who determines whether GeoTime should be deployed?
i. What is the criteria for deployment? Can any detective determine based on their own discretion that deployment of GeoTime is necessary for their investigation? Is supervisor approval required?
j. What software-level security controls are in place for both the GeoTime workstations and for the internet accessible portal? Are they the same access control mechanisms? Where can the internet accessible portal be accessed from (i.e., a mobile device)?
k. Where does SPD store/host the data it manually inputs into GeoTime? Is there a difference in where the data are hosted or stored when GeoTime is accessed via the portal vs. via a workstation?
l. How long are the data stored there? When are the data deleted?
m. What safeguards are in place to protect the data that is inputted into GeoTime (is the data encrypted? What are the access control mechanisms?)
n. How does SPD validate the accuracy of the data it manually inputs into GeoTime, as well as GeoTime data outputs/analyses?
o. Which SPD personnel have access to the data output/files generated from GeoTime? How many SPD personnel have access to the GeoTime data outputs?

p. What is the nature of the training that SPD personnel receive on GeoTime? How many hours of training do they receive? What does the training cover? Do they receive periodic updated training? Are they provided privacy training specific to the privacy risks associated with GeoTime?
q. Does GeoTime have an audit log? If so, what does it contain/what information does it collect? Does it log what actions each user takes inside the application?
r. How often is SPD's GeoTime subject to an audit? When was the last audit of SPD's GeoTime conducted and by which entity (APRS, OIG, or the federal monitor)? Where are the audit reports located?
s. Does SPD maintain a record of all disclosures of GeoTime data and analyses/output, including those to outside entities?

## IV. *Recommendations for Regulation*

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

- There is a specific and restricted purpose of use. There must be a policy defining clear limits on GeoTime's uses, including narrow parameters for: (1) using data that were obtained via consent agreement as opposed to a search warrant; (2) using GeoTime in conjunction with other technology; (3) the use of all of GeoTime's surveillance features; and (4) the event type or crime type that GeoTime is used for.
- The use of GeoTime's social media analysis functionality must be prohibited.
- The use of GeoTime for predictive policing must be prohibited.
- People whose data is obtained via consent agreement must be informed, as part of the consent process, that their data will be inputted into GeoTime.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for both the GeoTime licensed workstations and for the internet accessible portals, as well as for access to GeoTime outputs and analyses.
- Any data inputs or outputs must be securely shared with third parties and properly deleted.

- SPD must disclose/log to whom and under what circumstances GeoTime data inputs and outputs are shared.
- There must be adequate training for all personnel who use GeoTime and the training must include a privacy component specific to the risks inherent to using GeoTime as an investigative tool.
- There must be a detailed direct audit log of user actions within GeoTime, and SPD must produce a publicly available annual audit report about its use of the technology.
- Any data inputs hosted by UnCharted Software or data outputs created via GeoTime are not owned by, used by, or retained by UnCharted Software, and any data inputs and data outputs are properly secured.
- There must be measures in place to validate the accuracy of GeoTime data inputs and outputs/analyses.

## Computer, Cell Phone, and Mobile Device Extraction Tools

### I. *Background*

A computer, cell phone, and mobile device extraction tool, also known as mobile device forensic tool (MDFT),[43] is a powerful software technology that allows police to circumvent most security features on a person's device to easily extract all the data on the device—including call logs, contacts, text messages, emails, social media posts, photographs, location information, search history, and financial transactions—and systematically search and analyze it. As such, this tool "represent[s] a dangerous expansion in law enforcement's investigatory powers."[44] Its use by SPD raises serious privacy concerns, given the sheer amount of personal, sensitive information stored on people's smartphones. Eighty-five percent of U.S. adults own a smartphone,[45] and they generally keep it on their person wherever they go. The implication is that the vast majority of people are vulnerable to having their phones invasively searched by law enforcement. This risk is particularlyacute and the privacy infringement is particularly egregious for

[43] National Institute of Standards and Technology, "Mobile Security and Forensics," Accessed May 17, 2022, https://csrc.nist.gov/Projects/Mobile-Security-and-Forensics/Mobile-Forensics.
[44] Koepke, Logan, et al. "Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones," *UpTurn*, October 20, 2020, https://www.upturn.org/work/mass-extraction/.
[45] Pew Research Center, "Demographics of Mobile Device Ownership and Adoption in the United States," April 7. 2021, https://www.pewresearch.org/internet/fact-sheet/mobile/?menuItem=d40cde3f-c455-4f0e-9be0-0aefcdaeee00.

the many low-income people who rely exclusively on their smartphone to access the internet.[46]

The use of MDFTs by SPD also raises serious civil liberties concerns. This technology enables police to conduct an excessively broad and intrusive search. It provides access that "can be disproportionately invasive compared to the scope of evidence being sought and poses an alarming challenge to existing Fourth Amendment protections."[47] Without limitations on use cases and narrowly defined parameters around, for example, what data can be extracted and for what purpose, the use of this tech is rife for misuse. In particular, the ACLU-WA is concerned about the use of MDFTs by SPD to surveil and ultimately chill constitutionally protected First Amendment activities concerning religion, expression, and assembly. Furthermore, use of MDFTs by SPD likely tracks with disparities in SPD policing practices[48] and statewide criminal legal system outcomes.[49] Therefore, it likely disproportionately impacts marginalized groups, including Black people, people of color, and people experiencing poverty or houselessness.

SPD does not disclose in the SIR which vendor provides its MDFT tools, which products it uses, and how many licenses it has for each product. When asked about its MDFT vendors at the 5/18/22 public engagement meeting, the SPD representative stated that SPD will not disclose what vendors they use because this information "could hinder investigative efforts."[50] In particular, the representative cited concerns that having this information would help people create so-called "counter-measures."[51] Without vendor information though, it is challenging to assess the privacy and civil liberties impacts of the technology. It is also antithetical to the

---

[46] "As of early 2021, 27% of adults living in households earning less than $30,000 a year are smartphone-only internet users—meaning they own a smartphone but do not have broadband internet at home." Vogels, Emily A., "Digital Divide Persists Even As Americans with Lower Incomes Make Gains in Tech Adoption," June 22, 2021, https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption.

[47] Koepke, et al., "Mass Extraction."

[48] See, e.g., Kasakove, Sophie, "Seattle Bike Helmet Rule is Dropped Amid Racial Justice Concerns," *New York Times*, February 18, 2022, https://www.nytimes.com/2022/02/18/us/seattle-bicycle-helmet.html; "Report Finds Racial Disparities in Stops, Arrests, Use-of-Force by Seattle Police Officers," *KOMO News*, July 15, 2021, https://komonews.com/news/local/report-finds-racial-disparities-in-stops-arrests-use-of-force-by-seattle-police-officers.

[49] "Race and Washington's Criminal Justice System: 2021 Report to the Washington Supreme Court," *Fred Korematsu Center for Law and Inequality, Seattle University School of Law* https://law.seattleu.edu/media/school-of-law/documents/centers-and-institutes/korematsu-center/initiatives-and-projects/race-and-criminal-justice-task-force/task-force-20/2021-race-and-washingtons-criminal-justice-system-report.pdf.

[50] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

[51] Ibid.

spirit and purpose of the Seattle Surveillance Ordinance process, which was established in part to create transparency about Seattle agencies' use of new and old technology.

Via Public Records Act disclosures, the ACLU-WA is aware that SPD uses or has used a variety of device extraction tools, including but not limited to: Cellebrite[52] (and Cellebrite's Advanced Investigative Services, or CAIS); Black Bag Forensic Software; GrayShift GrayKey; Octoplus; Medusa Pro; MSAB Incorporated aka Micro Systemation, and XRY Office Version.[53] It's noteworthy that law enforcement often purchase tools from multiple vendors in order to maximize the types of devices they can extract data from (e.g., iPhone, Android, etc.).[54]

***Concerns with Data Extraction and Analysis***

MDFTs can reliably access and extract some, if not all, data from most phones, with very few exceptions.[55] According to the SIR, there are very few hurdles to SPD officers or detectives using this technology, despite how easily it provides full access to device data. The SIR states that in order to use MDFTs, investigators must fill out a request form that includes a copy of consent or search warrant authorizing the extraction.[56] The SIR further states that "unit supervisors are responsible for screening all technology deployments to ensure that the appropriate authorities are in place before approving deployment of tracking technology."[57] However, the SIR does not specify any criteria for determining whether MDFTs should be deployed in the first place—i.e., what constitutes a case where the deployment of MDFTs is considered necessary?

The SIR does not adequately convey this invasiveness and the implications for privacy rights and civil liberties. It describes the data extraction process in the following way: "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."[58] This description does not explicitly communicate the wide range of data sources and the sheer amount of data that MDFTs can extract and analyze, which is troublingly vast. On the most basic level, MDFTs can extract photographs taken from smartphones along with the metadata from

[52] Hvistendahl, Mara and Sam Biddle, "Use of Controversial Phone-Cracking Tool is Spreading Across Federal Government," *The Intercept*, February 8, 2022, https://theintercept.com/2022/02/08/cellebrite-phone-hacking-government-agencies/.
[53] On file with the author.
[54] Koepke et al., "Mass Extraction."
[55] Ibid.
[56] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 6.
[57] Ibid., 8.
[58] Ibid., 5, DRAFT SIR - Computer, Cellphone, & Mobile Device Extraction Tools.pdf (seattle.gov)

those photos, such as the GPS coordinates of where a photo was taken and the time and date it was taken, thereby providing a "geographic record of the person's movements," as well as the movements of anyone else in those photos.[59] MDFTs can also extract app data and access location information, in-app communications, and in-app photos from those apps.[60] Cellebrite software tools, for example, can extract and interpret data from at least 181 apps on Android's operating system and at least 148 apps on Apple iPhones.[61] These can include everything from social media apps like Instagram, Facebook, Snapchat, and Twitter; navigation apps like Google Maps; web browsers like Chrome and Firefox; and dating apps like Tindr, Grindr, and OkCupid.[62] They can even extract data from encrypted messenger apps like Signal and Telegram.[63] MDFTs are also frequently updated by the vendor in order to be able to extract data from an ever growing number of apps.[64]

Many apps are account-based, i.e., data are stored on the cloud as opposed to directly on the device, and can be accessed remotely. MDFTs, including Cellebrite, often have specific features or products that provide law enforcement access to those data as well.[65] Google's Location History is an example of a particularly rich cloud-based data source that MDFT's enable access to. Any user with their location history turned on in their Google account will have years' worth of precise location records stored online in their Google Account, which can be extracted with MDFT's.[66]

In addition to app data, MDFT's can access "deleted" data from phones, as well as phone meta data, i.e., data about how people use their phone (e.g., when certain applications were installed and deleted, how often an application was used, when a device was locked or unlocked, when a message was viewed, etc.).[67]

MDFT's commonly extract all these user data by circumventing the device's security features using various tactics that exploit the device's security flaws or built-in diagnostic or development tools. For example, since March 2016, Cellebrite has added lock-bypass support for about 1500 devices, which exploits device vulnerability to force the phone to skip the passcode-checking step when it turns on.[68] Moreover, to get around encryption, MDFT's can repeatedly guess the decryption key, which is usually based on

[59] Koepke et al., "Mass Extraction."
[60] Ibid.
[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Ibid.

the phone's log-in password, to identify the correct one, thereby enabling the MDFT to decrypt the phone's contents.[69] It's been estimated by John Hopkins professor and security technologist Matthew Green that this password-guessing process would take at most 13 minutes for a 4-digit passcode (average 6.5 minutes), 22 hours for 6 digits (average 11.1 hours), and 92 days for 8 digits (average 46 days).[70] iPhones (which are the device used by 45% of smartphone users) default to a six digit passcode. With GrayKey or Cellebrite Premium (both of which SPD has owned or owned in the past), law enforcement can decrypt the data on an iPhone in less than a day, and on, average less than half a day.[71]

Even without an encryption key though, MDFTs can still extract plenty of phone data because phones don't encrypt all data on a device.[72] There are also many phones that don't encrypt user data, or that have encryption schemes that can be dismantled. If all else fails, law enforcement can install on the device a spyware tool, such as the one provided by Grayshift (a vendor SPD uses), which enables phone access by recording future password entries[73]

If law enforcement is unable to access and extract data from a device in house, they can send it to the vendor for "Advanced Services." At the 5/18/22 public engagement meeting, SPD stated they use "white glove" services which entails sending the phone to the vendor and having them extract the data.[74] Public records confirm SPD utilizes these services. They show, for example, that in 2018, SPD purchased 20 "vouchers for service that unlocks, extracts, and decrypts data from cellular phones" for over $33,000."[75] Emails from Cellebrite's Advanced Services Team to an SPD detective show Cellebrite unlocked iPhones within days or weeks.[76]

In addition to data extraction capabilities, MDFTs also provide powerful analysis tools that allow law enforcement to quickly sort, search, examine, and ultimately make meaning out of the vast trove of data they now have at their fingertips. These details are also omitted from the SIR. Data analysis tools include data visualization functionalities that can, for example, show

---

[69] Ibid.
[70] Green, Matthew [matthew_d_green], "Guide to iOS estimated passcode cracking times (assumes random decimal passcode + an exploit that breaks SEP throttling): 4 digits: ~13min worst (~6.5avg) 6 digits: ~22.2hrs worst (~11.1avg) 8 digits: ~92.5days worst (~46avg) 10 digits: ~9259days worst (~4629avg)," *Twitter*, April 16, 2018, https://twitter.com/matthew_d_green/status/985885001542782978.
[71] Koepke et al., "Mass Extraction."
[72] Ibid.
[73] Ibid.
[74] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[75] Koepke et al., "Mass Extraction."
[76] Ibid.

full text conversations as a chat instead of as individual messages or create a network map using contact data in order to reveal connections and relationships.[77] Moreover, they include data searching functions like basic keyword search but also more advanced options like Cellebrite's "search by face" function that enables law enforcement to compare an image of a person's face to all the other images of faces found on the phone.[78] With Cellebrite, law enforcement can also input their own images into the software and search for similar images on the device.[79] These visualization functionalities can be applied to data from multiple phones to discern connections between people, through, for example, shared contacts, call or text correspondence, or account information.[80]

Despite the power MDFTs give SPD to broadly access people's most sensitive data, it is not clear from the SIR how often MDFTs are utilized and for what kinds of cases. The SIR cites that SPD uses these tools to investigate internet crimes against children, via their Sexual Assault and Child Abuse (SAU) Unit).[81] It further states that the Technical and Electronic Support Unit (TESU) "manages extraction tools for other SPD investigations"[82] but it is unclear what those "other" SPD investigations. An extensive report written by UpTurn on the use of MDFTs by law enforcement agencies across the country, including SPD, found that MDFTs are used as "an all-purpose investigation tool for a broad array of offenses."[83] In other words, the use of MDFTs by law enforcement is routinely used for a variety of different kinds of investigations. During their investigation, UpTurn received "hundreds of cellphone extraction request forms" as part of a public records request to SPD. ACLU-WA's analysis of SPD's logs of extractions records found that between September 19, 2016 and March 20, 2017, a six-month period, SPD attempted at least 194 extractions, 67 which were failures and 127 that were successful. This is a conservative estimate, given that these records are likely incomplete and ostensibly don't include any extractions sent to the vendor for "Advanced Services."

***Concerns with Consent Searches***

[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Ibid.
[81] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 6.
[82] Ibid.
[83] Koepke et al., "Mass Extraction."

Relatedly, there are inadequate policies that govern and ultimately limit SPD's use of this technology. According to the SIR, MDFTs are "utilized only with the device owner's consent or pursuant to search warrant authority"[84] and these measures mitigate privacy risks, such as "concerns that data may be accessed out of scope."[85] However, there are several reasons to believe that the consent requirement is not rights protective and will not sufficiently limit the misuse of MDFTs.

Firstly, there is an inherent power imbalance between police officers and members of the public,[86] given that police are armed and act with state authority. That imbalance is arguably greater when the interaction is between police and Black people or people of color, who are disproportionately the targets of violent police practices and may feel pressure to "consent" to a phone search because of fear of being harmed by police if they do not consent.[87] In this context, "consent" is obtained under duress and is arguably coerced, not voluntary.

In addition to the power imbalance, the notion of a consent agreement is problematic because of the significant information asymmetry between police officers and members of the public about MDFTs. It is reasonable to assume that the vast majority of people have very little if any knowledge of MDFTs and their capabilities, or much if any understanding of how much of their personal, private and often sensitive data are stored on their phones and can be easily and quickly accessed via this technology. Any consent process is unlikely to adequately convey these things and fix the information deficit, especially in the absence of legal counsel. Arguably, no one can really know what they are consenting to, so truly informed, meaningful consent is not possible.

This is especially the case in situations where the device owner is a juvenile or a non-English speaker. At the 5/18/22 public engagement meeting, when asked how the consent process is different for non-English speaking people, the SPD representative stated SPD would "try to have an interpreter on site or use a language line to make sure we have informed consent."[88] This statement is troubling because it implies that it is not standard practice to provide non-English speakers a translator and a consent form in their language during the consent process. Any consent obtained without interpretation would be constitutionally invalid.

---

[84] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 3.
[85] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 15.
[86] Nadler, Janice, "No Need to Shout: Bus Sweeps and the Psychology of Coercion," *The Supreme Court Review*, vol. 2002, 2002, pp. 153-222.
[87] Strauss, "Reconstructing Consent."
[88] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

Lastly, even if consent processes provide for interpretation, consent searches are problematic because consent agreements generally do not define adequate parameters limiting the phone search, so police have huge amounts of discretion about what data they extract with MDFTs, the scope of the data they extract, and what they do with those data. For all these reasons, SPD's reliance on consent agreement to conduct phones searches with MDFTs is extremely problematic and concerning. This concern is exacerbated by SPD's heavy reliance on consent agreement to deploy MDFTs; according to UpTurn's report, "approximately one third of the phones the Seattle Police Department sought to extract data from were consent searches."[89]

Finally, it is unclear who within SPD and which entities outside SPD have access to extracted data and how those data are protected. The SIR states: "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."[90] Further down, the SIR states "All data extracted is stored securely within SAU—not accessible to any vendor."[91] However, this contradicts evidence, cited earlier, that SPD relies on the vendor to unlock phones they can't unlock themselves on premises. Moreover, during the 5/18/22 public engagement meeting, the SPD representative stated that has it sent devices to the King County Sheriff's Office in the past for "Chip-Off" extraction.[92] The implication then is that extraction is not always conducted in house, that extraction may be conducted by the vendor or another law enforcement agency, and therefore that vendor and the law enforcement agency have access to the data. However, the SIR does not specify the policies or practices that govern how the data extracted by the vendor are safeguarded while it is in the possession of the vendor.

***Concerns with Data Sharing***

Moreover, the SIR states that "data obtained from the system may be shared outside SPD with other agencies, entities, or individuals within legal guidelines or as required by law."[93] The sharing of data extracted via MDFTs with law enforcement agencies outside Washington state is particularly troubling given that many states have signaled they are ready to criminalize abortions in the wake of a US Supreme Court draft leak which indicates the high court is ready to overturn Roe v. Wade. Our state remains a safe haven for people to exercise their reproductive rights and it

[89] Koepke et al., "Mass Extraction."
[90] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 6
[91] Ibid.
[92] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[93] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 12.

is anticipated that Washington will see an influx of people from neighboring states seeking abortion services here.[94] MDFTs may be used to surveil these people and it is critical that there be restrictions on the ability of SPD to share these data with law enforcement and other agencies outside the state. Moreover, for any data that are shared, there should be stringent data storage, retention and transfer/sharing safeguards in place to protect the data.

Given the lack of adequate policies described by the SIR and the number of unanswered questions that remain, we have concerns that SPD's use of MDFTs may infringe upon people's civil rights and civil liberties.

## II. *Specific Concerns*

a. **Lack of clarity about MDFT vendor names, product names, and the number of licenses SPD owns.** The SIR does not disclose vendor names, product names or the number of licenses. At the 5/18/22 public engagement meeting, the SPD representative stated that SPD would not share information about vendor names because this information "could hinder investigative efforts."[95] Without this information, it is challenging to comprehensively assess the impacts of MDFTs on privacy rights and civil liberties, as well as SPD's need for this technology.

b. **Lack of Clarity and Transparency on What Other Tech MDFTs Interface With.** The SIR does not specify which other tech, if any, SPD uses in conjunction with MDFTs. MDFTs are capable of interfacing with a host of other technologies, including ones owned by SPD such as GeoTime. GeoTime states on their website that that their technology can import data from Cellebrite software tools, which public records show SPD owns or has otherwise owned in the past. Without this information, it is difficult to adequately assess the privacy risks that MDFTs pose.

c. **Lack of Clarity on Which SPD Personnel and How Many Have Access to MDFTs and How Often They are Deployed.** The SIR does not specify how many SPD personnel

[94] Ahmed, "States Move to Restrict Abortion Access."
[95] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

are trained and certified in the use of MDFTs and/or otherwise have access to MDFTs. It also does not indicate how often MDFTs are deployed. Without this information, it is difficult to adequately assess the impacts on privacy rights and civil liberties, as well as SPD's need for this technology.

d. **Lack of Clarity on Which SPD Personnel and How Many Have Access to Extracted Data.** The SIR states: "Only authorized SPD users can access the device or the extracted/imaged data while it resides in the extraction/imaging software" and that when the data are moved to an investigative file, access to it there is again "limited to authorized detectives and identified supervisory personnel." However, it does not specify who qualifies as an "authorized" user or detective. Therefore, it remains unclear which SPD personnel and how many have access to data that has been extracted via MDFTs.

e. **Lack of Clarity on How SPD Mitigates Potential for Inadvertent or Unauthorized Data Collection**. In response to the question of how SPD minimizes improper data collection, the SIR states, in part, that "[u]se of extraction tools is constrained by consent or court order providing the legal authority."[96] This is a vague statement that does not describe the measures SPD takes to ensure that the data extracted via MDFTs is narrowly tailored to the needs of the investigation.

f. **Legitimacy of Consent-Based Use of MDFTs and Lack of Clarity on How Consent is Obtained.** It is unlikely that consent-based use of MDFTs is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law enforcement, and individuals may fear that refusing to give their consent to police will lead to deadly consequences. Additionally, the SIR does not describe the process by which officers obtain consent from witnesses or confidential informants. It is unclear if this process is standardized.

g. **Lack of Clarity on Vendor Access to Data.** According to the SPD representative at the 5/18/22 public engagement meeting,

[96] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 8.

SPD relies on vendors to extract data from devices that it cannot do itself in-house with off-the-shelf MDFT tools.[97] This is corroborated by UpTurn's extensive report on MDFTs, which examined public records from SPD. This contradicts the SIR, which states that all extraction is done in-house and that vendors do not have access to data. The implication is that vendors do have access to device data. This is extremely concerning because it increases the risk of those data being exposed or otherwise misused.

h. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share extracted data "with other agencies, entities, and individuals" outside of SPD, which presumably includes agencies from outside the state. However, it does not specify under what circumstances data would be shared or the policies and practices in place that govern data storage, retention and transfer/sharing to protect the data. It also does not indicate whether these disclosures are documented, and how.

i. **Low Threshold for MDFT Deployment.** The SIR states: "As it relates to extraction tools themselves, use is authorized, and constrained, only by consent or search warrant."[98] There is no indication there are any criteria for determining whether use of MDFTs is warranted or appropriate in the first place, despite the invasiveness of the technology and the lack of limitations on the scope of data collection via these tools. This suggests the barrier to using extraction tools is very low, even though the privacy infringement is incredibly egregious.

j. **Lack of Clarity on Safeguards in Place to Protect MDFTs and Extracted Data From Unauthorized Access.** The SIR states, regarding SAU extraction requests, that a personal password is needed to log onto the device.[99] A separate password is required to access extracted data and that same password is required to move the extracted data from the device to a portable USB.[100] No access controls are specified for TESU extraction requests or data extracted by TESU. Once data has been extracted, the MDFT can "either save the files to

[97] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."
[98] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 15.
[99] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 7
[100] Ibid.

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," which enable the user to examine and search the data.[101] However, the SIR does not specify what access control mechanisms are in place for accessing this software and the data on it, including whether data are encrypted. This is extremely concerning as it puts private data at risk of being improperly accessed and searched.

k. **Lack of Clarity About Data Storage, Safeguards, and Retention.** The SIR provides only a vague description of how extracted data are stored, safeguarded, and for how long they are retained. It states that "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." This leaves out critical details about what access control mechanisms are in place to safeguard the data and how long data there are retained. The SIR also states that the data are sometimes saved to "removal physical storage (like a USB drive or similar media) or a computer workstation"[102] but it does not specify what policies and practices govern data storage, safeguards and retention on those mediums.

l. **Inadequate Data Sharing Policies.** The SIR offers only an extremely general description of who might receive device data extracted with MDFTs and how such data would be shared. Neither security protocols for transferring data nor for ensuring that shared data are properly deleted are explicated in the SIR. Indefinite retention of data and insecure sharing processes could lead to exposure of sensitive data, with manifold consequences for those whose data is collected.

m. **Lack of Clarity on Use of MDFTs to Search the Phones of Minors.** The UpTurn report on MDFTs provides evidence via public records that SPD uses MDFTs to extract data from the device of minors.[103] However, the SIR does not mention this fact. When asked at the 5/18/22 public engagement meeting

[101] Ibid., 5.
[102] Ibid.
[103] Citing to a King County Search Warrant, the report states that SPD "[o]fficers were looking for a juvenile who allegedly violated the terms of his electronic home monitoring. Officers eventually located the individual, and, after a 'short foot pursuit…he threw several items to the ground,' including a phone. Officers located the phone and sought to search it for evidence of escape in the second degree." Koepke et al., "Mass Extraction."

about what percentage of devices SPD extracts belong to minors, SPD claimed they don't have that data, which suggests SPD does not collect data on the demographics of the people whose phones they search. The use of MDFTs to search the phones of minors is very concerning, given that minors are a vulnerable population and are entitled under law to extra protections to safeguard their rights. Moreover, the lack of data collection on MDFT use makes it challenging, if not impossible, to detect whether there is bias in SPD practices.

n. **Lack of Policy on Purpose of Use and Usage Limits.** The SIR does not fully explain use cases for MDFTs and does not include policies placing limits on its uses.
   i. **Scope of data collection**. The SIR states that "[a] certified user within TESU conducts the extraction and provides the entirety of the data to the requesting Officer/Detective for the investigation file."[104] The SIR also states that improper data collection is limited through the consent agreement or a search warrant[105] but does not specify how these create limitations on data collection if in fact the detective is given the entire contents of a device. Arguably there are no measures that constrain or minimize inadvertent or improper data collection since virtually everything is collected.
   ii. **Type of offense or investigation**. According to the SIR, SPD's SAU uses MDFTs to investigate internet crimes against children[106] and the TESU "manages extraction tools for other SPD investigations"[107] without elaboration on what those "other investigations" are. Furthermore, the SIR does not specify if there are limits to the type of events (e.g. First Amendment demonstrations) or offenses that SPD will investigate (e.g. petty crimes like graffiti and trespassing).
   iii. **Tools MDFTs interface with.** The SIR does not specify any limitations on the technology that MDFTs can interface with.

[104] SPD, "Computer, Cellphone, & Mobile Device Extraction Tool," 7.
[105] Ibid., 8
[106] Ibid., 6.
[107] Ibid.

o. **Lack of clarity about oversight.** The SIR states that both TESU and SAU "maintain logs of deployment,"[108] "all deployments of extraction tools are documented,[109], and "logs of collected information are available for audit,"[110] but it does not specify what information is collected exactly. When asked at the 5/18/22 about the last time an audit was conducted, SPD did not have a response and referred participants to OIG for an answer, strongly suggesting there has is no history of auditing. Without detailed auditing capabilities, or regular auditing, it is not possible to have sufficient oversight into how SPD uses MDFTs and whether they are complying with policy.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

a. Which vendor(s) provide SPD the extraction tools they use?
b. Which extraction tools and how many does SPD currently own?
c. How many licenses does SPD have for each MDFT product?
d. What is the cost to obtain and maintain each? What funding source(s) does SPD use to cover these costs/expenditures?
e. With what frequency/how often does SPD use extraction tools?
    a. How many times a week/for how many investigations a week is it used?
f. Besides child sexual assault and child abuse investigations, what kinds of investigations are extraction tools used for? Describe the range of investigations and what kinds of investigations they are mostly used for.
g. How often are extraction tools used in the field vs. at a unit work station? Under what circumstances are they used in the field vs. at a unit work station?
h. What does the training and certification for these extraction devices entail?
    a. How many hours of training do they receive? What does the training cover?
    b. Do they receive periodic updated training?
    c. Is there a privacy component to the training that is specific to the privacy risks of this tech? (response to 7.2 indicates no.)

[108] Ibid., 16
[109] Ibid., 8
[110] Ibid., 10

i. What does the process of obtaining consent from the phone owner look like?
    i. In what context does an officer/detective typically ask a person for consent to access their phone?
    ii. At the 5/18/22 public engagement meeting, the SPD representative indicated that a person can consult a lawyer before signing the form. Is that something the person is explicitly informed of?
    iii. Is there a script that officers/detectives follow when obtaining consent? If so, what does that script say?
    iv. What information is the phone owner provided about how their data will be extracted and what data? Is the person informed both verbally and in writing that the extraction tool will extract a full copy of data from their device—all emails, texts, photos, location, app data and more—which can then be programmatically searched?
    v. Does policy require that non-English speakers be taken through the consent process in their native language?
    vi. Does policy permit SPD to seek consent from minors to search their device with MDFTs? If so, how does that process differ, if at all, from the process used for non-minors?
j. When an officer/detective makes a request to a supervisor to use a data extraction tool, are they required by policy to articulate something they are specifically looking for?
k. What policies and practices and/or procedures limit the scope of data SPD extracts with MDFTs?
l. How does SPD safeguard the data of people on the device who are not under investigation (i.e., smart phones usually contain the private data of other people, such as location data from photos or social media pages)?
m. What policies and practices and/or procedures minimize improper or inadvertent data collection?
n. Question 4.10 of the SIR asks about safeguards in place for protecting data from unauthorized access and to provide an audit trail. SPDS's response is not very detailed or satisfactory. What safeguards are in place for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (view logging, modification logging, etc.)?
o. How are device data safeguarded when the device is sent to the vendor for extraction? How does SPD ensure that vendors

providing "Advanced Services" don't receive improper/unauthorized access to device data?

p. How often is a deployment audit performed? How often is a request audit performed? When was the last time an audit was performed for each?
q. The SIR states: "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." How much time is data typically stored on an extraction device before it is downloaded to the investigation file? Is it immediate? Is deletion of data on the extraction device also immediate? Is that reflected in the training?
r. What other technologies, if any, do MDFTs interface with? What policies, if any, limit the technologies that MDFTs interface with?
s. Who has access to the data on the extraction device? What constitutes an "authorized user"? How many "authorized users" within SPD have access to the data?
t. Who within SPD has access to the data once it has been downloaded out of the extraction tool? How many people have access?
u. Which agencies, entities and individuals outside of SPD can SPD share extracted data with? Are these disclosures documented? If so, where and how?
v. What data storage, retention and transfer/sharing safeguards in place to protect the data?
w. Are data obtained via extraction tools subject to the PRA?

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of Computer, Cell Phone, and Mobile Device Extraction Tools. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The use of consent searches of mobile devices must be prohibited.
- The plain view exception for digital searches must be abolished.
- There is a specific and restricted purpose of use. There should be policy defining clear limits on the use of MDFTs, including narrow parameters for: (1) data collection (2) using MDFTs in conjunction with other technology; (3) the event type or offense type that MDFTs are used for.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for licensed workstations as well as for access

to extracted data on whatever medium they exist, including removable physical storage like a portable USB drive.
- Any device data extractions must be securely shared with third parties and properly deleted.
- SPD must create and abide by robust data deletion and sealing policies.
- SPD should disclose/record to whom and under what circumstances extracted device data are shared.
- There is adequate training for all personnel who use MDFT's and that the training includes a privacy component specific to the risks inherent to using MDFT's as an investigative tool.
- There must be a detailed and direct public audit log of user actions within MDFT software, and these logs must be easy to understand. SPD must produce a publicly available annual audit report about its use of the technology.

## Camera Systems

### I. *Background*

Camera systems are a surveillance technology that enables law enforcement to monitor and record video and the sound of people's activities. SPD uses their camera systems in a "covert" manner, so that those who are the target of this surveillance (and ostensibly all others in proximity) are unaware they are being surreptitiously recorded. According to the SIR, "these covert cameras are disguised and used to record specific events related to an investigation."[111] They are either concealed on a person or hidden in or on objects.[112] The SIR states they are used by SPD to record activities "in plain view" where there is no reasonable expectation of privacy, and to record activities in a setting where a reasonable expectation of privacy exists.The SIR also indicates that SPD uses cameras "for video recording in the presence of a confidential informant or undercover officer as allowed by law." [113]

[111] Seattle Police Department, "2022 Surveillance Impact Report: Camera Systems," Accessed May 23, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Camera%20Systems.pdf.
[112] SPD, "Camera Systems," 6.
[113] Ibid.

The use of undercover or covert cameras raises serious privacy and civil liberties concerns. Research shows that law enforcement disproportionately target certain groups with camera surveillance, namely Black people, people of color, young people, and people living in poverty. One study out of Great Britain showed that Black people were surveilled at a rate one-and-a-half to two-and-a-half times higher than their representation in the public.[114] In general we expect the use of camera surveillance to track or mirror racial and socio-economic disparities in police practices more broadly,[115] so that neighborhoods that are over-policed to begin with are targeted for surveillance.[116] Covert camera systems may also be used to surveil and ultimately chill constitutionally protected First Amendment activities concerning religion, expression, and assembly. For example, the SIR explicitly mentions the use of camera systems to surveil "places of worship that have been seriously vandalized or whose congregants have been threatened."[117] Given the recent history of racialized surveillance of Muslims and mosques under the mantle of "homeland security" and "counter-terrorism,"[118] the use of this technology to potentially monitor religious minorities and their communities may chill the free exercise of religion and raise concerns about discrimination and racial profiling.

The SIR does not specify the vendor or product names of the camera systems SPD uses, nor does it provide much of any detail about the capabilities of those cameras. When asked about it at the 5/18/22 public engagement meeting, the SPD representative stated that SPD would not share information about vendor names because this information "could hinder investigative efforts."[119] Without this information, it is challenging to adequately assess all the privacy and civil liberties impacts of this technology, and SPD's need for it.

Camera systems vary widely in their complexity, interconnectivity, and capability. They may be able to tilt, pan, and/or zoom. Some capture high-

---

[114] Norris, Clive and Gary Armstrong, *CCTV and the Social Structuring of Surveillance,* Routledge, 2006, p. 162.
[115] Kasakove, "Seattle Bike Helmet Rule is Dropped Amid Racial Justice Concerns."
[116] See, for instance, Hitchcock, Ben, "You're Being Watched: Police Quietly Deploy Cameras Near Public Housing," *cvill.com,* January 15, 2020, https://www.c-ville.com/youre-being-watched-police-quietly-deploy-cameras-near-public-housing/ C-VILLE Weekly; Todd, Gracie, "Police Cameras Disproportionately Surveil Nonwhite Areas of DC and Baltimore, November 19, 2020, https://cnsmaryland.org/2020/11/19/police-cameras-disproportionately-surveil-nonwhite-areas-of-dc-and-baltimore-cns-finds/.
[117] SPD, "Camera Systems," 5.
[118] Khan, Saher and Vignesh Ramachandran, "Post 9/11 Surveillance Has Left a Generation of Muslim Americans in a Shadow of Distrust and Fear," *PBS.org,* September 16, 2021, https://www.pbs.org/newshour/nation/post-9-11-surveillance-has-left-a-generation-of-muslim-americans-in-a-shadow-of-distrust-and-fear.
[119] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

definition images so even small details can be detected. They can be panoramic or otherwise wide-angle, enabling wide-area coverage with a single camera. They may also be remotely operated and/or have a feed that can be monitored. Some cameras may also record at nighttime or in low light, and may even use infrared or heat vision for dark areas where night vision is not sufficient. They may rely on motion sensors or are otherwise motion-activated. SPD's fixed location covert cameras appear to be motion-activated, since the SIR states "they are most often set to record only when motion is detected."[120] Camera systems may have audio capabilities, too. According to the SIR, SPD's covert camera systems "capture images only, not sound,[121] but it is not clear whether audio is a setting that is turned off or if the cameras do not have the capability to record sound at all. In response to a question on the SIR asking about data retention policies, SPD writes: "Per the Washington Secretary of State's Law Enforcement Records Retention Schedule, investigational conversation recordings are retained 'for 1 year after transcribed verbatim and verified OR until disposition of pertinent case file, whichever is sooner, then Destroy" (LE06-01-04 Rev. 1)."" This appears to contradict earlier statements that audio is not recorded.

Some camera systems can be paired with other technologies, including automated license plate readers (ALPRs)[122] and facial recognition,[123] which renders the technology even more invasive. However, the SIR does not specify whether their camera systems have any of these features or otherwise interface with these other technologies.

Based on the SIR, there appear to be few barriers to SPD officers and detectives using covert camera systems, and the few hurdles that exist are very low. The Technical and Electronic Support Unit (TESU) manages, maintains, deploys and/or installs the covert camera systems that SPD uses.[124] An SPD officer or detective that wants to use a covert camera for their investigation must submit a request form to TESU that "outline[s] the equipment requested and the case number." It's noteworthy that in a different part of the SIR, it states that officers or detectives make a verbal request to the TESU and TESU personnel will complete a form for them.[125] All requests are screened by a TESU supervisor but the SIR does

[120] SPD, "Camera Systems," 6.
[121] Ibid.
[122] "Automated License Plate Readers," *ACLU*, Accessed May 30, 2022, https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers
[123] "Face Recognition Technology," *ACLU*, Accessed May 30, 2022, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.
[124] SPD, "Camera Systems," 7.
[125] Ibid., 8.

not specify what that screening process entails.[126] In addition to the form, to request a camera that will record in plain view, officers or detectives have only to show reasonable suspicion, which is a very low bar, ostensibly giving officers plenty of discretion to determine when, where, and against whom to deploy cameras. SPD's decisions around where to deploy cameras, for example, may reflect biases that already exist about which neighborhoods are considered "high crime" (i.e., neighborhoods that are already over-policed). It may also open the door to a fishing expedition, where officers aren't looking for anything in particular but plan to deploy cameras in the hopes of capturing criminal activity.

In general, "plain view" settings, which are an exception to the search warrant requirement under the Washington state constitution, are not defined in the SIR. SPD's characterization of plain view settings versus settings where there is a reasonable expectation privacy is vague and lacks nuance. SPD appears to use "plain view" as a proxy for "public area" without accounting for the multitude of scenarios in a public setting where there is a reasonable expectation of privacy. This raises concerns that SPD officers/detectives may be defining the plain view exception more broadly than permitted by law, especially as applied to a very intrusive technology.

To request a camera that will record in places where there is a reasonable expectation of privacy, a warrant or consent is required. The use of consent agreement in lieu of a warrant is concerning because of the power and information differential between police and members of the public, which could lead to a person consenting to the use of a camera system under duress (resulting in coerced consent).[127]

Moreover, with both consent agreements and the use of reasonable suspicion, it's unclear how the scope of data collection is narrowly tailored to the investigation (e.g. where cameras are installed, what data they collect, how long cameras are installed for, etc.) to ensure both that more data is not collected than necessary for the investigation, and that improper data collection (inadvertent or otherwise) doesn't occur (including the capture by cameras of the activities of people who are not under investigation). In general, it's unclear from the SIR how the scope of data collection is constrained in contexts where a warrant is not required. The SIR also does not specify what proportion of camera use is for plain view recording versus recording in a setting where there is a reasonable expectation of privacy, and for the latter, what proportion of cameras are deployed on the basis of a warrant versus a consent agreement.

---

[126] Ibid.
[127] Strauss, "Reconstructing Consent."

While the SIR lists some of the event types or investigations that camera systems may be deployed for, it does not provide a comprehensive list, nor does it specify any policies that limit use cases. Thus it's unclear whether camera systems are used for serious offenses as well as more minor/petty offenses (e.g. graffiti, trespassing). The SIR also does not specify any criteria SPD applies to determining whether hidden cameras are necessary and appropriate in the use of an investigation. A UN Office of Drugs and Crime report on the current practice of electronic surveillance for investigating serious crime provides useful guidance. Interestingly, the SIR quotes from this report to extoll the benefits of cover camera surveillance,[128] but does not mention this guidance. The report states that law enforcement's use of electronic surveillance "should not be an investigative tool of first resort" and that "its use should be considered when other less intrusive means have proven ineffective or when there is no reasonable alternative to obtain crucial information or evidence." In particular, this report cites to four principals or policy considerations that should inform the decision to deploy electronic surveillance (including hidden cameras): (1) the use of this form of data gathering is necessary to obtain the evidence required; (2) that there are mechanisms in place to protect the confidentiality of the information obtained, including the privacy of third parties that are not the subject of the investigation; (3) that the process of evidence gathering is overseen by a judge "or independent other of a certain requisite and specified authority"; and (4) that the privacy infringement is proportionate to the seriousness of the suspected offense and the evidence that will be collected.[129] However, none of these principles or policy considerations are reflected in the SIR as part of SPD's calculus for deploying covert cameras or limiting their use.

II. *Specific Concerns*

a. **Lack of clarity about Camera System Vendor and Product Names, and the Number of Camera Systems SPD Owns.** The SIR does not disclose vendor or product names of the camera systems it uses, or the number of camera systems it owns. At the 5/18/22 public engagement meeting, the SPD representative stated that SPD would not share information about vendor names because this information "could hinder

[128] SPD, "Camera Systems," 5.
[129] United Nations Office on Drugs and Crime, "Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime," 2009, https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.

investigative efforts."[130] Without this information, it is challenging to know the capabilities of these camera systems and comprehensively assess their impacts on privacy rights and civil liberties, as well as SPD's need for this technology.

b. **Lack of Clarity About How SPD Defines the Plain View Exception.** The SIR does not define the plain view exception to the search warrant requirement. It appears to cast plain view settings as a proxy for "public area" without explaining that even in a public area, there are situations where people have a reasonable expectation of privacy under the law. This is concerning because it suggests SPD is interpreting the plain view exception more broadly than permitted by the law, especially as applied to a very intrusive technology.

c. **Legitimacy of Consent-Based Use of Covert Camera Systems and Lack of Clarity on How Consent is Obtained.** It is unlikely that consent-based use of cover camera systems is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law enforcement, and individuals may fear that refusing to give their consent to police will lead to deadly consequences. Additionally, the SIR does not describe the process by which officers obtain consent from witnesses or confidential informants. It is unclear if this process is standardized and if there is a separate consent process for confidential informants.

d. **Lack of Clarity on How Many SPD Personnel Have Access to Camera Systems and How Cameras are Secured to Prevent Unauthorized Access.** The SIR indicates that camera systems are managed and maintained by SPD personnel within TESU but does not specify how many SPD personnel are trained and certified in the use of camera systems and/or otherwise have access to them. It also does not provide information about how cameras are secured to prevent unauthorized access, especially for body-worn cameras (the ones that can be concealed on a person), which are ostensibly

[130] City of Seattle IT Department, "Group 4b Surveillance Technologies Public Meeting #2."

small and discrete and therefore can be surreptitiously moved around. The SIR states that "access to the systems/technology is limited to TESU personnel via password-protected login credentials" but that doesn't account for how cameras are physically secured.[131]

e. **Lack of Clarity on Safeguards in Place for Protecting Data from Unauthorized Access.** The SIR states that for fixed location cameras, data is stored directly on the device, and must be returned to TESU, which extracts the data onto a thumb drive or external hard drive and provides this copy to the requesting Officer/Detective for inclusion in the investigation file. The investigation file is kept on SPD's password-protected server which is "limited to authorized detectives and identified personnel" but does not specify who qualifies as an "authorized detective and identified personnel." Moreover, the SIR does not specify who has access to the data on the thumb drive or to the investigation file, or what the access controls are for the those. For fixed location cameras, recorded data are stored on an SPD-owned server and requesting officers or detectives must log into the server to extract the data. Similarly, the SIR does not specify who has access to the data on the server or what access control mechanisms are in place for the data. Without adequate access control mechanism, private data are at risk of being improperly accessed.

f. **Lack of Clarity About Data Storage and Retention.** The SIR provides only a vague description of how extracted data are stored and for how long they are retained. It also does not specify what policies and practices govern data storage and retention on these mediums.

g. **Lack of Clarity on How Often Cameras are Deployed**. The SIR does not indicate how often camera systems are deployed, or the proportion of camera deployments that are concealed on a person versus installed in a fixed location. It also does not provide information about what proportion of cameras installed in a setting where a reasonable expectation of privacy exists are deployed based on consent agreement versus a warrant. Without this information, it is difficult to adequately assess the

[131] SPD, "Camera Systems," 11.

impacts on privacy rights and civil liberties, as well as SPD's need for this technology.

h. **Lack of Clarity and Transparency on What Other Tech Camera Systems Interface With.** The SIR does not specify which other tech, if any, SPD uses in conjunction with camera systems. Camera systems are capable of interfacing with a host of other technologies, such as automated license plate readers, facial recognition, or otherwise augmented with other forms of artificial intelligence.

i. **Lack of Policy on Purpose of Use and Usage Limits.** The SIR does not explain all of the use cases for camera systems and does not include policies placing limits on its uses.
    i. **Scope of data collection**. The SIR does not indicate how the scope of data collection is limited, especially in situations where the cameras are recording in plain view and all that is needed to deploy a camera system is reasonable suspicion, which is a very low bar.
    ii. **Type of offense or investigation**. The SIR does not specify if there are limits to the type of events (e.g., First Amendment protected demonstrations) or offenses that SPD will investigate (e.g., petty crimes like graffiti and trespassing) using camera systems.
    iii. **Tools camera systems interface with.** The SIR does not specify any limitations on the technology that camera systems can interface with.

j. **Inadequate Oversight Policies.** The SIR states that TESU maintains logs of requests (including copies of request forms and/or warrants) and extractions that are available for audit.[132] However, it is unclear if SPD has measures to prevent or detect the use of a covert camera system being used outside of the bounds of a case or legal investigation. It's also unclear how often audits on the use of camera systems are conducted and if there are any policies governing the frequency with which audits are done.

[132] Ibid., 12

k. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from covert camera systems with outside entities[133] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

a. What are the manufacturers, vendors, model names and numbers of the fixed location cameras and body cameras?
b. The SIR states: "Covert cameras may only be issued/deployed by TESU detectives. All TESU staff that deploy these cameras have received vendor training in their use." Do the SPD personnel who request to use camera systems from TESU for their investigation, and who ostensibly are involved with the camera system operation, also receive training?
c. What is the nature of the training that TESU personnel receive around camera systems?
    i. How many hours of training do they receive? What does the training cover?
    ii. Do they receive periodic updated training?
    iii. Are they provided privacy training specific to camera systems?
    iv. Is the training standardized and documented?
d. Are camera systems capable of capturing and recording audio?
e. How many fixed location cameras does SPD own? How many are currently deployed?
f. Where are fixed location cameras deployed (i.e., what neighborhoods)?
g. What is the distribution of fixed location cameras across these neighborhoods?
h. How many fixed location cameras are currently deployed in locations where there is a "reasonable expectation of privacy"?
i. Where are these deployed (e.g., what neighborhoods and blocks)?
j. What is the distribution of fixed location cameras across these neighborhoods?

[133] Ibid, 14

k. In general, where are the kinds of places that these cameras are covertly placed? Urban areas? Rural? Residential? Intersections? Etc.
l. How long are they typically deployed for? Days? Months?
m. How sophisticated are fixed location cameras? What capabilities do they have (e.g., can they zoom, pan, pivot)? Can they transmit video in real time? Is there a feed that can be monitored? Can the camera be remotely operated?
n. How many covert body-worn cameras does SPD own?
o. Are fixed location and body cameras used in conjunction with other tech?
p. What safeguards/access control mechanisms are in place to protect data stored on the SPD server, camera device, investigative file or USB drive and limit access to authorized users only?
q. What is the data retention policy for data on these various mediums?
r. What are the policies governing when data must be deleted or otherwise purged from these mediums?
s. How often are audits of covert camera use conducted? Is there a policy governing how often audits occur?
t. When was the last time a request audit and deployment audit were conducted by APRS or OIG?

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of covert camera systems. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The names of the manufacturers, vendors, model names, and model numbers are publicly disclosed.
- There is a policy defining the incident types for which SPD may use covert camera systems, and how they may be used.
- Covert camera systems are only used with authorization of a court-ordered warrant.
- The following are made publicly available: The frequency with which covert camera systems are used; the average and median length of time covert camera systems are deployed; how many camera systems SPD has; and how many people have access to the camera systems.

- There must be strong access controls (authentication, authorization, logging, etc.) in place for accessing data collected via covert camera systems, regardless of the medium they are stored on.
- There is a clear data retention policy.
- SPD should disclose/record to whom and under what circumstances camera system recordings are shared.
- There is adequate and standardized training for all personnel who use covert camera systems and the training includes a privacy component specific to the risks inherent to using covert camera systems as an investigative tool.
- There must be a detailed direct audit log of user actions with covert camera systems and SPD must produce a publicly available annual audit report about its use of the technology.

## Tracking Devices

### I. *Background*

Tracking devices are location-tracking tools that allow SPD to track vehicles electronically via interconnected hardware and software. Physical tracking devices are placed on or in a targeted vehicle and they report latitude and longitude coordinates on a pre-determined schedule that can be adjusted by users remotely. SPD uses a connected online portal that collects the information captured by the tracking device to map the locations and movement of vehicles.

Tracking devices raise serious privacy and civil liberties concerns because they can be used to comprehensively track and plot the movements of individual cars over time. These devices can be used to target individuals who visit sensitive places such as places of religious worship, protests, union halls, immigration clinics, or health centers. While SPD states that it uses tracking devices only with a warrant or after obtaining consent, data collected via these devices may be combined with other SPD data and analyzed with other invasive tools used by SPD such as GeoTime or IBM i2 iBase that can create very detailed, personalized maps and analyses of people's lives—even if they are not involved in a crime or an event being investigated.

Additionally, we have concerns about whether consent-based tracking is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law

enforcement, and as noted by one scholar, "many African Americans, and undoubtedly other people of color, know that refusing to accede to the authority of the police, and even seemingly polite requests—can have deadly consequences."[134]

## II. *Specific Concerns*

a. **Lack of Information on What Specific Tracking Devices are Used.** The public has not been provided the names of the manufacturers and the specific model numbers and names of the tracking devices used by SPD. Without this information, it is difficult, if not impossible to meaningfully review all the functions and capabilities of the tools in use and provide recommendations on how each tool should be regulated.

b. **Lack of Clarity on Usage Limitations and Types of Incidents for Which Tracking Devices are Used.** While the SIR states that officers/detectives will provide written consent and/or a court approved warrant for all vehicle-tracking technology deployments, it does not describe the incident types for which tracking devices are used. Especially with consent-based uses of tracking devices, it is unclear from the SIR how the use of tracking devices is constrained (whereas a judicial warrant would articulate formal parameters around data collection, such as time frame). Additionally, it is unclear whether SPD has a policy limiting the use of geolocation trackers to vehicles.

c. **Legitimacy of Consent-Based Tracking and Lack of Clarity on How and From Whom Consent is Obtained.** It is unlikely that consent-based tracking is legitimately consensual given the power and information asymmetry between police and members of the public, and particularly for communities that are disproportionately surveilled and policed. There are important racial differences in how individuals interact with law enforcement, and individuals

[134] "Given this sad history, it can be presumed that at least for some persons of color, any police request for consent to search will be viewed as an unequivocal demand to search that is disobeyed or challenged only at significant risk of bodily harm." Strauss, Marcy, "Reconstructing Consent." *Journal of Criminal Law and Criminology*, vol. 92, no. 1, 2001, pp. 242-243.

may fear that refusing to give their consent to police will lead to deadly consequences. Additionally, the SIR does not describe the process by which officers obtain consent from witnesses or confidential informants. It is also unclear from whom consent is being sought—the vehicle owner, driver, and/or passengers. Lastly, it is unclear if this process is standardized.

d. **Lack of Clarity About Data Storage, Safeguards, and Retention.** It is unclear whether the data collected via the physical tracking devices ever leaves SPD-owned equipment. The SIR states that "data is securely stored by the vehicle tracking technology vendor and will be transferred to the case investigator only via Seattle Police Department owned and authorized technology. At that time, vehicle tracking data collected by the tracking device is downloaded from the vendor software and resides only with the investigation file."[135] It is unclear if the data is within the SPD network on-premises or if it flows to a vendor providing Software-as-a-Service. Additionally, the SIR does not state if any data retention policy exists. The SIR states that SPD deletes tracking device data from the software and hardware after the conclusion of a tracking schedule, but it does not state how long the data are kept after being moved to an investigation file.

e. **Lack of Clarity on if TESU Personnel Training is Standardized and Documented.** The SIR states, "TESU personnel are trained by the vendor in the use of the hardware and software. When an Officer/Detective requests and deploys a tracking device from TESU, TESU personnel train the Officer/Detective in the tracker's use." It is unclear how the vendor trains the TESU personnel and how consistency in this training is ensured.

f. **Lack of Clarity on Which SPD Personnel/Units and How Many Have Access to Tracking Devices.** The SIR states "Only authorized SPD users can access the vehicle tracking devices or the data while it resides in the system," that "only SPD personnel involved in the investigation have

[135] Seattle Police Department, "2022 Surveillance Impact Report: Tracking Devices," Accessed May 23, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Tracking%20Devices.pdf, 9.

access to this information, and "[o]nly Technical and Electronic Support Unit personnel have access to vehicle tracking equipment and services" but it is unclear which units and how many people in total have access to the tracking devices.

g. **Lack of Clarity on Frequency of Usage of Tracking Devices.** It is unclear how many cases per year use tracking devices, how many deployments there are per year, and the average and median length of time tracking devices are deployed.

h. **Inadequate Oversight Policies.** The SIR states that no formal audits exist for tracking device deployments. It is unclear if SPD has measures to prevent or detect the use of a tracking device being used outside of the confines of a case or legal investigation.

i. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from tracking devices with outside entities[136] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

a. What are the manufacturers, vendors, model numbers, and model names of the tracking devices in use by SPD?
b. Is there any policy defining the incident types for which SPD may use tracking devices?
c. What is the process of getting consent?
d. Is the "online portal" hosted within the SPD network on-premise, or is it hosted on the vendor's website?
e. Does the data collected via the tracking device ever leave SPD-owned equipment
f. Are the trackers placed anywhere other than a vehicle?
g. Is the TESU personnel training standardized and documented?

[136] Ibid., 10

h. What is the retention period for data collected by tracking devices?
i. How many cases per year use tracking devices?
j. How many deployments of tracking devices are there per year?
k. How long is the average and median length of time tracking devices are deployed?
l. How many tracking devices does SPD have?
m. How many people have access to SPD's location tracking devices?
n. How many times has SPD deployed a tracking device on a vehicle either not owned by the suspect or owned by the suspect but also frequently used by other individuals?
o. Are there measures in place that would prevent or detect the use of a tracking device outside the confines of a case or legal investigation?
p. Have there been any audits of SPD's use of tracking devices? If so, when was the last audit and where can that audit report be found?

## IV. *Recommendations for Regulation*

Pending answers to the questions above, we can make only preliminary recommendations for regulation of tracking devices. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The names of the manufacturers, vendors, model names, and model numbers are publicly disclosed.
- There is a policy defining the incident types for which SPD may use tracking devices, and how they may be used.
- Tracking devices are only used with authorization of a court-ordered warrant.
- Data collected via the tracking device never leaves SPD-owned equipment.
- The following are made publicly available: The frequency with which tracking devices are used; the average and median length of time tracking devices are deployed; how many tracking devices SPD has; and how many people have access to the tracking devices.
- There must be strong access controls (authentication, authorization, logging, etc.) in place tracking devices.
- There is a clear data retention policy.
- SPD must disclose/record to whom and under what circumstances tracking device data are shared with third parties.

- There is adequate and standardized training for all personnel who use tracking devices and the training includes a privacy component specific to the risks inherent to using tracking devices as an investigative tool.
- There must be a detailed direct audit log of user actions with tracking devices and SPD must produce a publicly available annual audit report about its use of the technology.
- There must be measures in place to validate the accuracy of the data collected by tracking devices.

**Remotely Operated Vehicles**

I. ***Background***

Remotely Operated Vehicles (ROVs) are unarmed remote controlled vehicles with mounted cameras. Three SPD units use ROVs: SWAT, Arson/Bomb, and Harbor. These units use ROVs to access areas that are potentially dangerous for personnel to physically enter. The ROVs operated by the SWAT and Arson/Bomb units are wheeled vehicles while the ROV operated by the Harbor unit are designed as submersible underwater vehicles.

There are 14 ROVs used in total.

- The SWAT unit has 7 ROVs. Two are manufactured by Robotex, four are manufactured by Recon Robotics, and one is manufactured by Tactical Electronics.
- The Arson/Bomb unit has 5 ROVs. They are manufactured by TeleRob, Andros, ICOR, Talon, and PointMan. Each of these ROVs has a camera which transmits back to the handheld control unit.
- The SPD Harbor unit has 2 submersible ROV units. One unit is manufactured by Deep Ocean Engineering and has onboard video and sonar recording capability. The other ROV is manufactured by Seabotix and has onboard video and sonar recording capability as well as two interchangeable remotely controlled articulated arms.

ROVs pose privacy and civil liberties concerns because they may be used to surveil members of the public via cameras and may be used to carry weapons and deliver lethal force. In 2016, Dallas police officers used a bomb disposal remote control vehicle armed with explosives to kill a

man.[137] Given that SPD's ROVs are equipped with cameras and remotely controlled arms, these technologies have the potential to cause serious harm to members of the public.

## II. *Specific Concerns*

a. **Lack of Clarity on Usage Limits.** While the SIR explains some use cases for ROVs, it does not include specific policies placing limits on its uses. For example, the SIR does not describe any policies in place prohibiting the use of ROVs to surveil members of the public or to carry or deploy weapons.
b. **Lack of Clarity on if There are Auditable Logs of the Deployment of ROVs.** The SIR does not clearly answer what processes are required prior to each use or access to ROVs, such as a notification, or check-in, or check-out of the equipment. The SIR only states, "Authorized members of the SPD SWAT, Arson/Bomb, and Harbor units are given training in the appropriate use and application of these ROVs."[138] Lack of a check-in/check-out procedure is concerning because there may be no logs that could be audited of the deployment of the ROVs.
c. **Lack of Clarity on the Number of Cases for Which ROVs are Used.** The SIR does not make clear for how many cases per year the SWAT, Arson/Bomb, and Harbor units use ROVs, and the average and median length of time ROVs are deployed.
d. **Lack of Clarity on Whether SPD has Ever Used ROVs to Deploy Weapons.** Some ROVs can support recoilless disrupters that can shoot diverse types of projectiles which are intended to remotely disable an improved explosive device (IED), i.e., a bomb However, some ROVs, such as the SWORDS TALON ROV, support a diverse range of weapons.[139] A 12-gauge shotgun can also be mounted onto

[137] Sidner, Sara and Mallory Simon, "How Robot, Explosives Took Out Dallas Sniper in Unprecedented Way," *CNN*, https://www.cnn.com/2016/07/12/us/dallas-police-robot-c4-explosives/index.html.
[138] Seattle Police Department, "2022 Surveillance Impact Report: Remoted Operated Vehicles (ROVs)," Accessed May 30, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20ROVs.pdf, p. 6.
[139] Qinetiq, "Multi-Mission Explosive Ordnance Disposal Robot," https://www.qinetiq.com/en/what-we-do/services-and-products/talon-medium-sized-tactical-robot

the Pointman ROV.[140] The purpose of mounting weapons onto ROVs would be to harm or kill humans—not to disable an IED. SPD uses both TALON and Pointman ROVs and it is unclear whether SPD has ever used ROVs to deploy weapons or if SPD has a policy prohibiting the use of weapons with ROVs.

e. **Inadequate Data Storage, Safeguards, and Retention.** The SIR states that Harbor unit personnel delete the data on the hard drives inside the ROV only periodically when the software informs the users that it is nearing capacity.[141] It is unclear why there is no policy requiring the deletion of recorded data from the Harbor unit's ROVs when a deployment is finished. It is also unclear whether the statement that no images or data are stored or retained by ROVs used by SWAT and Arson/Bomb units also applies to SPD-provided cell phones, personal cell phones, or remote controllers and tablets that may also support recording data.

f. **Lack of Clarity on if ROV Training is Standardized and Documented.** The SIR states, "Authorized members of for the SPD SWAT, Arson/Bomb, and Harbor units are given training in the appropriate use and application of these ROVs. Unit commanders are responsible to ensure usage of the technology falls within the appropriate usage."[142] It is unclear if there is a standardized and documented training process.

g. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from ROVs with outside entities[143] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

- Is there any policy defining usage limits for SPD's use of ROVs?
- Is there a procedure for SPD personnel to get access to the ROVs?

[140] i-HLS, "Pointman Tactical Robot, Surveillance Systems Assist Law Enforcement in Urban, Security Ops," *Defense Update*, 2013, Accessed June 1, 2022, https://defense-update.com/20130504_new-tools-for-border-security.html
[141] SPD, "ROVs," 8.
[142] SPD, "ROVs," 6.
[143] SPD, "ROVs," 10.

- Is there an auditable log of the deployment of ROVs?
- For how many cases per year does the SWAT unit use ROVs?
- For how many cases per year does the Arson/Bomb unit use ROVs?
- For how many cases per year does the Harbor unit use ROVs?
- Is the training for members of the SPD SWAT, Arson/Bomb, and Harbor units standardized?
- Is there a policy requiring the deletion of recorded data from the Harbor unit's ROVs when a deployment is finished?
- Is there a policy prohibiting SPD personnel from recording data using SPD-provided cell phones or personal cell phones, or remote controllers or tablets that may be connected to the ROVs wirelessly?
- Has SPD ever used an ROV with weapons or for lethal force?
- Have there been any audits of SPD's use of ROVs? If so, when was the last audit and where can that audit report be found?

## IV. *Recommendations for Regulation*

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

- There is a policy defining the incident types for which SPD may use ROVs, how they may be used, and what the usage limits are.
- A court ordered warrant is required to use ROV to surveil any members of the public.There is a prohibition on the use of ROVs to deploy weapons.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for ROVs.
- Any data collected via ROVs that is not needed for an investigation is deleted immediately.
- Data collected via ROVs never leaves SPD-owned equipment.
- The following are made publicly available: The frequency with which ROVs are used; the average and median length of time ROVs are deployed; and how many people have access to the tracking devices.
- SPD must disclose/record to whom and under what circumstances ROV data are shared with third parties.
- There is adequate and standardized training for all personnel who use ROVs and the training includes a privacy component specific to the risks inherent to using ROVs as an investigative tool.

- There must be a detailed direct audit log of user actions with ROVs and SPD must produce a publicly available annual audit report about its use of the technology.

**Crash Data Retrieval**

## I. *Background*

Crash Data Retrieval (CDR) tools are used to reconstruct traffic collisions by connecting to a vehicle's Event Data Recorder (EDR) and translating the raw EDR data to a PDF format readable report. Nearly all passenger vehicles sold in the US since 2013 have an onboard EDR, which automatically records technical information during a critical event such as a collision. While the type of data collected by an EDR varies by manufacturer, the types of data that are recorded include GPS, throttle, brake pedal position, steering angle, and speed. After airbags are deployed, these data are saved permanently and can only be accessed through the vehicle's onboard diagnostics port.

CDR tools pose privacy and civil liberties concerns because EDRs can be used to track people's locations and record other sensitive information without their knowledge. In 2011, OnStar, a company that uses EDRs to track vehicle location and other operational data, changed it user contract terminology without notifying customers, in order to track people's driving habits and sell the information to third parties.[144] While the policy was eventually reversed due to public pressure, entities such as auto insurance companies may use increasingly powerful tracking systems to monitor policyholders, and that data may be accessed by law enforcement.

The SIR's lack of clarity on SPD's policies and the specific CDR tools in use raises concerns about SPD's use of this technology.

## II. *Specific Concerns*

a. **Lack of Information on What Specific CDR tools are Used.** The SIR does not provide the names of the manufacturers and the specific model numbers and names of the CDRs used by SPD. Without this information, it is difficult, if not impossible, to meaningfully review all the

[144] David Kravets, "OnStar Tracks Your Car Even When You Cancel Service," *Wired*, 2011, Accessed June 1, 2022, https://www.wired.com/2011/09/onstar-tracks-you/

functions and capabilities of the tools in use and provide recommendations on how each tool should be regulated.

b. **Lack of Clarity on Usage Limits.** While the SIR explains the general use case for CDR tools, it does not describe if SPD seeks to use CDR tools to gather EDR data every time an accident occurs, regardless of whether a citation has been issued or a crime has occurred.
c. **Lack of Clarity on the Breadth of Warrants to Collect Vehicle Data.** It is unclear if the warrants used by SPD specify that only EDR data are collected or if these warrants permit SPD to extract any data from the vehicle, including information from a car's system such as phone contacts and location history from past trip navigations.
d. **Lack of Clarity on if There are Audits on the Deployment of CDR Tools.** It is unclear if SPD has logs of CDR use and if there has been an audit of SPD's usage of CDR tools.
e. **Lack of Clarity on the Number of Cases for Which CDR Tools are Used.** The SIR does not make clear for how many cases per year CDR tools are used, and the average and median length of time CDR tools are deployed.
f. **Lack of Clarity About Disclosures to Other Agencies.** The SIR states that SPD may share data obtained from CDR tools with outside entities[145] but does not address whether SPD maintains a record of those disclosures. Without a record of all disclosures, it is impossible to know who has received these sensitive data.

## III. *Outstanding Questions that Must be Addressed in the Final SIR*

h. What are the manufacturers, vendors, model numbers, and model names of the CDR tools in use by SPD?
i. Is there any policy defining usage limits for SPD's use of CDR tools?
j. Are the warrants to get access to vehicle data after a crash limited to EDR data?
k. Are the audits on SPDs use of CDR tools?
l. For how many cases per year does SPD use CDR tools?

[145] Seattle Police Department, "2022 Surveillance Impact Report: Crash Data Retrieval Tool," Accessed May 30, 2022, https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20%20Crash%20Data%20Retrieval.pdf, 9.

**IV. *Recommendations for Regulation***

Pending answers to the questions above, we can make only preliminary recommendations for regulation of CDR tools. SPD should adopt clearer and enforceable policies that ensure, at the minimum, the following:

- The names of the manufacturers, vendors, model names, and model numbers are publicly disclosed.
- There is a policy defining the incident types for which SPD may use CDR tools, how they may be used, and what the usage limits are.
- There is policy requiring warrants sought for CDR use are narrowly tailored to only extract EDR data, and no other data from the vehicle.
- There must be strong access controls (authentication, authorization, logging, etc.) in place for CDR data.
- The following are made publicly available: The frequency with which CDR tools are used; the average and median length of time CDR tools are deployed; and how many people have access to the CDR tools.
- SPD must disclose/record to whom and under what circumstances CDR data are shared with third parties.
- There must be a detailed direct audit log of user actions with CDR tools and SPD must produce a publicly available annual audit report about its use of the technology.

Sincerely,

Jennifer Lee
Technology and Liberty Project Manager

Mina Barahimi Martin
Policy Analyst

City of Seattle

Upturn
Toward Justice in Technology

June 02, 2022

Seattle Information Technology
700 5th Ave, Suite 2700
Seattle, WA 98104

**RE: Upturn's Comments on "Computer, cellphone and mobile device extraction tools" in Group 4b Surveillance Technologies**

On behalf of Upturn, I write to offer our comments on one technology included in Group 4b of the Seattle Surveillance Ordinance implementation process.

Upturn is a nonprofit organization based in Washington, D.C. that works in partnership with many of the nation's leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of technology. One of Upturn's priorities is to ensure that technology does not exacerbate or entrench mass incarceration and racial inequity in the criminal legal system.

We write to comment specifically on Seattle Police Department's (SPD) use of mobile device forensic tools (MDFTs) — tools that allow police to extract and search a cellphone for every text, photo, piece of location data, online search history, and more.[1] In 2020, Upturn published *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (attached). Based on more than 110 public records requests, more than 12,000 pages of documents, and more than two years of research, this report is the most comprehensive examination of law enforcement's use of mobile device forensic tools to date.[2] Among the report's findings is that more than 2,000 law enforcement agencies have

[1] Under Group 4b the Seattle Surveillance Ordinance process describes these tools as "Computer, cellphone and mobile device extraction tools." We use the terminology "mobile device forensic tools" as we believe it is most technically accurate — regardless, this is the same technology that the Seattle Police Department uses.

[2] Our records requests asked law enforcement agencies for three common records: purchase records, records of use (describing in what cases and how often law enforcement agencies use mobile device forensic tools), and policies governing use. We supplemented our research through publicly available reporting; various open databases from city, county, and state governments; federal grantmaking databases; and GovSpend, a database of government contracts and purchase orders. In order to assess the technical capabilities of current mobile device forensic tools, we examined technical manuals, software release notes, marketing materials, webinars, and digital forensics blog posts and forums. We also visited the office of one of the few public defenders in the US with these forensic tools (and forensic staff) in-house.

Upturn
Toward Justice in Technology

purchased these tools in all 50 states and the District of Columbia. State and local law enforcement agencies have performed hundreds of thousands of cellphone extractions since 2015, often without a warrant. Few departments have detailed policies governing when and how officers can use this technology. The report also documents the existing technical capabilities of today's mobile device forensic tools, finding that the tools provide sweeping access to personal information on a phone. *Mass Extraction* documents a dangerous expansion in law enforcement's investigatory power.

In these comments, we highlight four issues with law enforcement use of mobile device forensic tools. We believe that MDFTs are simply too powerful in the hands of law enforcement and should not be used. Recognizing that MDFTs are already in widespread use across the country, we conclude with recommendations that we believe can, in the short term, reduce the use and harm of MDFTs.

## 1. Mobile device forensic tools are designed to be invasive. They are a dangerous expansion of law enforcement's investigatory power.

Every day, law enforcement agencies across the country search thousands of cellphones using MDFTs. MDFTs are a powerful technology that allows police to extract a full copy of data from a cellphone — all emails, texts, photos, location data, app data, and more — which can then be programmatically searched. As one expert puts it, with the amount of sensitive information stored on smartphones today, the tools provide a "window into the soul."[3]

Mobile device forensics is typically a two-step process: data extraction, then analysis. MDFTs help law enforcement accomplish both. An MDFT is a computer program and its supplemental equipment (*e.g.*, cables and external storage) that can copy and analyze data from a cellphone or other mobile device. The software can run on a regular desktop computer, or on a dedicated device like a tablet or a "kiosk" computer. These tools are sold by a range of companies, including Cellebrite, Grayshift, MSAB, Magnet Forensics, OpenText (formerly Guidance Software), Oxygen Forensics, and AccessData.

[3] C.M. "Mike" Adams, "Digital Forensics: Window Into the Soul," Forensic, June 10, 2019, *available at* https://www.forensicmag.com/518341-Digital-Forensics-Window-Into-the-Soul/.

Upturn
Toward Justice in Technology

According to records obtained from Seattle's Police Department, SPD has spent *at least* $240,000 on MDFTs from vendors including Cellebrite, MSAB, Magnet Forensics, and Grayshift.[4]

Modern cellphones are a convenient combination of many tools: they're phones, cameras, notebooks, diaries, navigation devices, web browsers, and more. Smartphones centralize patterns of life on a single device with seemingly endless storage. There has never been an easier, more centralized way to access troves of personal data about individuals. MDFTs allow law enforcement to access all of this data and more, often without individuals understanding how much information they are handing over.

Our technical analysis of how MDFTs work and their capabilities surfaces three key points:

1. **MDFTs are designed to copy all of the data commonly found on a cellphone.** Mobile device forensic tools are designed to extract the maximum amount of information possible. This includes data like contacts, photos, videos, saved passwords, GPS records, phone usage records, and even "deleted" data. A "logical extraction" of the phone extracts data as it is presented on the phone to the user, while a "physical extraction" of the phone allows for law enforcement to download data bit by bit from the phone, offering more information to be later reconstructed and analyzed.

2. **MDFTs make it easy for law enforcement to analyze and search data copied from phones.** A range of features help law enforcement quickly sift through gigabytes of data — a task that would otherwise require significantly more labor. MDFTs can chronologically sort all information on the phone, use location data to show every single place a person has been on a map, and use face recognition to search every image on the phone for a specific person. The tools allow for keyword searches of all data, sorting by file type regardless of its location on the phone (*e.g.*, all of the images on a phone, regardless where they came from) and even create networked graphs to show social relationships.

3. **MDFTs can circumvent most security features in order to copy data.** MDFTs exploit the security vulnerabilities or design flaws present in a wide range of

[4] This number comes from public records requests and is listed in the Appendix of *Mass Extraction*. https://www.upturn.org/work/mass-extraction/#. This total is an undercount, given that our public records project concluded in 2020 and SPD has likely renewed MDFT licenses and purchased new MDFTs in 2020, 2021, and 2022.

Upturn
Toward Justice in Technology

phones. Even in instances where full forensic access is difficult due to security features like strong password protection, mobile device forensic tools can often still extract meaningful data from phones. MDFTs take advantage of the fact that, in order to balance convenience and security, phones don't actually encrypt all data on a device. When all else fails, vendors offer "advanced services" in which the phone is sent to a vendor's lab for intensive unlocking attempts.

In 2018, the Seattle PD purchased 20 such "actions" for $33,000,[5] and email records show them using Cellebrite to unlock various iPhones within days or weeks.[6] For example, SPD sent Cellebrite an iPhone X with an unknown 6-digit passcode in August 2018: Cellebrite received it on August 24, began processing on August 28, finished processing on September 12, and shipped it back the same day. Cellebrite Premium allows law enforcement to bring these advanced unlocking capabilities in-house for $75,000 to $150,000, based on the frequency of use.[7]

Ultimately, MDFTs offer law enforcement a powerful window into almost all data stored on — or accessible from — a cellphone, including substantial amounts of data that regular users cannot see. Data extracted by an MDFT can be stored indefinitely and repeatedly searched. This would be like allowing law enforcement to repeatedly and indefinitely search a person's home, without that person knowing. MDFTs provide sweeping access to personal information on a phone, enabling "an extent of surveillance that in earlier times would have been prohibitively expensive."[8] In many circumstances, this access can be disproportionately invasive compared to the scope of evidence being sought and poses an alarming challenge to existing Fourth Amendment protections.

### 2. MDFTs are used as a general purpose investigative tool, even when the offense has no digital component.

The emergence of MDFTs represents a dangerous expansion in law enforcement's investigatory powers. In 2011, only 35% of Americans owned a smartphone.[9] Today, it's at

---

[5] *See* Seattle Police Department Purchase & Supply Request, https://beta.documentcloud.org/documents/20394507-installment_101.
[6] *See* Seattle Police Department, Cellebrite Advanced Services emails, https://beta.documentcloud.org/documents/20394508-installment_51.
[7] Cellebrite, "Premium access to all iOS and high-end Android devices," *available at* https://cf-media.cellebrite.com/wp-content/uploads/2020/07/ProductOverview_CellebritePremium.pdf.
[8] *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007).
[9] Pew Research Center, "Mobile Fact Sheet," June 12, 2019, *available at* https://www.pewresearch.org/internet/fact-sheet/ mobile/.

Upturn
Toward Justice in Technology

least 81% of Americans.[10] Moreover, many Americans — especially people of color and people with lower incomes — rely solely on their cellphones to connect to the internet.[11] For law enforcement, "[m]obile phones remain the most frequently used and most important digital source for investigation."[12] Seattle PD remarked in their own impact assessment that roughly 63% of investigations include digital evidence as part of the investigation.[13] While that percentage may seem high, if anything, it is a significant undercount of how often law enforcement agencies use MDFTs.

The records we've obtained demonstrate that law enforcement agencies use MDFTs as an all-purpose investigative tool for a broad and growing array of offenses. Law enforcement use MDFTs to investigate not only cases involving major harm, but also for graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offenses. Through our public records request, we received documentation from SPD that they conduct phone searches for offenses spanning from murder to robbery, violation of pretrial conditions of release, gun possession, and drug charges. This contradicts SPD's own claim that these tools are used for "collecting evidence related to serious and/or violent criminal activity."[14] Given how routine these searches are today, together with racist policing policies and practices, it's likely that these technologies disparately affect and are used against communities of color.

### 3. There are virtually no policies in place governing the use of these powerful tools.

In response to our records request, SPD did not provide us with any specific policies governing the use of MDFTs. Instead, SPD only provided general policies on searches, search warrants, and an irrelevant policy on locating a cellphone during an emergency. SPD's impact assessment only states that officers rely on warrants or consent for searches,

---

[10] *Id.* (Noting 96% own a cellphone of some kind.)
[11] Camille Ryan, U.S. Department of Commerce, Economics and Statistics Administration, U.S. Census Bureau, "Computer and Internet Use in the United States: 2016," American Community Survey Reports, August 2018; Jamie M. Lewis, *Handheld Device Ownership: Reducing the Digital Divide?*, March 2017, https://www.census.gov/library/working-papers/2017/ demo/SEHSD-WP2017-04.html.
[12] Cellebrite Annual Industry Trend Survey 2019: Law Enforcement, at 3.
[13] 2022 Surveillance Impact Report — Computer, Cellphone, and Mobile Device Extraction Tools, Seattle Police Department, at 4, *available at* https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Computer%2C%20Cellphone%2C%20%26%20Mobile%20Device%20Extraction%20Tools.pdf
[14] *Id.*, 5.

Upturn
Toward Justice in Technology

and does not describe any other policies to safeguard people's rights.[15] Indeed, SPD says that "[a]s it relates to extraction tools themselves, use is authorized, and constrained, only by consent or search warrant."[16] Section 4 of this testimony will describe in greater detail the profound limitations of consent and search warrants as measures to "safeguard people's rights."

As described in these comments already, MDFTs are some of the most powerful tools at law enforcement's disposal; and based on the available evidence, SPD has no policy to monitor, track, control, oversee, or even attempt to account for their use of these tools. This surveillance technology oversight process is an opportunity for the council to remedy this. Council must act to curb SPD's use of these tools and to protect the rights of Seattle residents.

Policies governing MDFTs should have specific requirements for how law enforcement write warrants and search phones, in order to guard against overbroad searches that violate peoples' rights. The Fourth Amendment requires warrants to describe with particularity the places to be searched and the things to be seized. This "particularity requirement" was designed to protect against "general warrants," such that law enforcement could not indiscriminately rummage through a person's property. While police departments' policies obtained by Upturn acknowledge the need to have a sound legal basis to search a phone (via consent or search warrant), few provide more clarity or direction beyond this general acknowledgement. When law enforcement downloads an entire copy of a person's phone, they violate the particularity requirement and leave individuals vulnerable to overbroad searches of their private activities, communications, and thoughts.[17]

In order for a cellphone search warrant to abide by the requirements of the Fourth Amendment, it must, at a minimum:

- Specify the particular items of evidence to be searched and seized from the phone;
- Ensure that the nexus between each category of information on a cellphone — such as texts, photographs, or emails — and the alleged criminal activity is specific and clear (cellphone search warrants must be based on more than the fact that a defendant possesses a phone);

[15] *Id.*
[16] *Id.*, 15.
[17] See an extended discussion of this in Section 4.

Upturn
Toward Justice in Technology

- Strictly limit search authorization to the narrowest time period for which probable cause has been properly established;
- Strictly prohibit a search of "any and all data," or of a laundry list of data on a phone; and
- Forswear reliance upon the plain view exception and general statements that say because digital data might possibly be disguised or manipulated, law enforcement must be able to search the entirety of a cellphone.

A specific cellphone search warrant policy should ideally describe these minimum features.

Further, SPD's current policies have no clear limits on data retention, or how that data may be used beyond the scope of an immediate investigation. Unlike a physical search of someone's home, once a copy of a person's phone has been downloaded, law enforcement can hold onto and repeatedly search that copy forever. Absent specific policies or laws that require notifying someone that their phone has been searched, it would be impossible for those under investigation to know of — let alone challenge — situations where law enforcement continues to rifle through previously extracted data for new or unrelated investigations.

Additionally, without specific prohibitions, law enforcement could copy data from someone's phone — say, their contact list — and add that information into a far-reaching police surveillance database that may harm an individual and their contacts for years to come. SPD might share information with other law enforcement agencies in the King County area, the state of Washington, or with other states and the federal government.[18] Law enforcement should also not be able to indiscriminately use cloud data extraction tools, which can access information that is not locally stored on the phone (SPD also has no policies for these tools).

There are a handful of state laws that do prescribe evidence retention periods specifically for digital evidence obtained from cellphones. For example, New Mexico's recently enacted Electronic Communications Privacy Act requires that "any information obtained through the execution of the warrant that is unrelated to the objective of the warrant be destroyed within thirty days after the information is seized and be not subject to further review, use

[18] The Wisconsin Supreme Court recently held that cellphone evidence obtained from a consent search in one jurisdiction can be shared with other law enforcement agencies pursuing unrelated investigations, without needing new legal authorization. *See State v. Burch*, 2021 WI 68, 961 N.W.2d 314 (Wis. 2021).

Upturn
Toward Justice in Technology

or disclosure."[19] The City of Seattle, too, should adopt meaningful limitations on retention of digital evidence.

### 4. Law enforcement regularly use MDFTs without a warrant – but even with warrants, little is done to minimize the harm of invasive searches.

In 2014, the Supreme Court held in *Riley v. California* that in order to search a cellphone, police must get a warrant.[20] However, courts have long held that "consent searches" are an exception to the Fourth Amendment's warrant requirement. Records Upturn obtained show that, for some agencies, law enforcement regularly rely on a person's consent as the legal basis to search cellphones. For the cellphone searches SPD documented and conducted between 2017 and 2019, one-third were consent searches.

However, "consent searches" are inherently coercive. Due to power and knowledge imbalances between residents and law enforcement, there is enormous disincentive to refuse to give consent, and it is much worse for people of color who are under threat of police violence. In fact, many states ban consent searches at traffic stops, and California[21] and New Jersey[22] have banned consent searches for minors, in order to address this racialized power imbalance. A recent study designed "specifically to examine the psychology of consent searches" highlights the problems in relying on a so-called "reasonable person" to adjudicate the lawfulness of consent searches.[23] Participants were brought into a laboratory and presented with a "highly invasive request: to allow an experimenter unsupervised access to their unlocked smartphone."[24] More than 97% of participants handed their phone over to be searched when requested — even though only

---

[19] *See* https://nmlegis.gov/Sessions/19%20Regular/final/SB0199.pdf. Similarly, California's Electronic Communications Privacy Act allows judges to, at their discretion, "require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings." *See* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178.
[20] *Riley v. California*, 573 U.S. 373 (2014).
[21] *See* John M. Broder, "California Ending Use of Minor Traffic Stops as Search Pretext," New York Times, Feb. 28, 2003, *available at* https://www.nytimes.com/2003/02/28/us/california-ending-use-of-minor-traffic-stops-as-search-pretext.html *and* California Senate Bill 203. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB203
[22] *See* Routine Automobile Consent Searches are Illegal in New Jersey. https://www.lsnjlaw.org/Criminal-Charges-and-Convictions/Motor-Vehicle-Laws/Pages/Ban-Routine-Automobile-Consent-Searches.aspx
[23] Roseanna Sommers, Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 Yale L. J. 1962 (2019).
[24] *Id.*, 1980.

Upturn
Toward Justice in Technology

14.1% of a separate group of observers said that a "reasonable person" would hand over their phone in such a situation.[25] This study reveals that there is a profound, "systematic bias whereby neutral third parties view consent as more voluntary, and refusal easier, than actors experience it to be."[26]

Additionally, MDFTs are not well understood by the public, and they are able to extract much more data than most people would assume. Many people may give consent to police to see their text messages or another specific category of data with the assumption that police will simply look at the phone manually, while police actually perform full extractions using MDFTs and retain data indefinitely. Consent searches of cellphones are especially egregious as people do not know the extent of the information they are giving away, and how that information will be searched and retained.

Warrants are not much better. As part of Upturn's public records research, we obtained and studied hundreds of search warrants that authorized law enforcement to search cellphones using MDFTs. Many of these warrants authorized a search of "any and all data" on a cellphone. Others authorized a search of a laundry list of effectively every type of data one could plausibly find on a cellphone. Others authorized a "full extensive download and/or search of the [phone] to include all compartments, and items within the electronic devices that may contain contraband or evidence of the crime, and the data stored within said devices." Still others authorized a search of a cellphone for "evidence related to this [narcotics offense] and other criminal offenses." And for many, regardless of the precise words used, the nexus between a phone's data and the alleged offense was tenuous. Repeatedly, across the country, we saw search warrants that authorized an unlimited, unrestricted search of a cellphone.

Relatedly, few policies provide guidance on what examiners should do if they encounter potential evidence of another crime that is not detailed in the initial search warrant. Using a search warrant to look for digital evidence of one potential crime, only to then search for digital evidence of a different crime is unconstitutional. Without clear and enforced guidance, law enforcement could go on a "fishing expedition" in search of evidence of any crime, far beyond the original justification for a search. We observed only two policies that provided any guidance on this point.[27]

---

[25] *Id.*, at 1980.
[26] *Id.*, at 2019.
[27] For example, the Santa Clara District Attorney's Office advises that if an "[e]xaminer discovers evidence of another crime(s) that is outside the scope of the submitted search warrant, the Examiner may continue the examination for items named in the warrant. The Examiner should contact the submitting agency and/or the prosecutor handling the case for guidance before conducting any searches for evidence not

Upturn
Toward Justice in Technology

The risk of overbroad searches is especially worrying given the fact that it's nearly impossible for those outside of law enforcement — such as defense lawyers — to repeat the steps that a forensic examiner took and to audit the scope of a search. A handful of agency policies do require examiners to document how a search was conducted, but the level of documentation required is still unlikely to allow a defense lawyer to meaningfully audit a search.

Legal scholars and courts have wrestled with the problems of overbroad digital searches for decades.[28] It's especially striking, given the prominence of these legal debates, that law enforcement agencies including Seattle Police Department have largely allowed officers and forensic examiners to search cellphones without detailed policies and with few constraints. SPD asserts that their cellphone searches are restricted to consent searches and warrants[29] — in practice, this means that residents of Seattle have no protections against overbroad violations of their rights.

---

named in the original warrant." *See* Santa Clara District Attorney's Office, Santa Clara County Crime Laboratory Computer Forensic Standard Operating Procedures, https://beta.documentcloud.org/documents/20394644-2019-08-19-pra-resp-email-att-standard-operating-procedures-rev-26-112820181. As another example, the San Diego Police Department says that if "an examiner discovers evidence of another crime(s) that is outside the scope of the submitted legal authority, the examiner will notify the assigned prosecutor and/or submitting investigator of the discovery and nature of any evidence of other crime(s) outside the scope of the original search warrant." *See* San Diego Police Department, Forensic Technology Unit Manual, https://beta.documentcloud.org/documents/20392583-forensic-technology-unit-manual-082218-current.

[28] *See, e.g.,* Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1 (2011); James Saylor, *Computers As Castles: Preventing the Plain View Doctrine From Becoming a Vehicle for Overbroad Digital Searches*, 79. Ford. L. Rev. 2809 (2011); Eric Yeager, *Looking for Trouble: An Exploration of How to Regulate Digital Searches*, 66 Vand. L. Rev. 685 (2013); Andrew D. Huynh, *What Comes after Get a Warrant: Balancing Particularity and Practicality in Mobile Search Warrants Post-Riley*, 101 Cornell L. Rev. 187 (2015); Adam Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in cellphone Searches*, 69 Vand. L. Rev. 585 (2016); Michael Mestitz, *Unpacking Digital Containers: Extending Riley's Reasoning to Digital Files and Subfolders*, 69 Stan. L. Rev. 321 (2017); Sara J. Dennis, *Regulating Search Warrant Execution Procedure for Stored Electronic Communications*, 86 Ford. L. Rev. 2993 (2018); Laura Donohue, *Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches*, 128 Yale L. J. Forum 961 (2019); Laurent Sacharoff, *The Fourth Amendment Inventory as a Check on Digital Searches*, 105 Iowa L. Rev. 1643 (2020); Cameron Cantrell, *A Dignitary Fourth Amendment Framework and Its Usefulness for Mobile Phone Searches*, 25 Va. J.L. & Tech 242 (2022).

[29] 2022 Surveillance Impact Report — Computer, Cellphone, and Mobile Device Extraction Tools, Seattle Police, *available at* https://www.seattle.gov/documents/Departments/Tech/Privacy/DRAFT%20SIR%20-%20Computer%2C%20Cellphone%2C%20%26%20Mobile%20Device%20Extraction%20Tools.pdf

Upturn
Toward Justice in Technology

5. **MDFTs are too powerful in the hands of law enforcement. Recognizing that they are already in widespread use across the country, several policies must be enacted to limit how MDFTs expand law enforcement's investigatory power.**

We believe that MDFTs are simply too powerful in the hands of law enforcement and should not be used. But recognizing that MDFTs are already in widespread use across the country, we offer a set of preliminary recommendations that we believe can, in the short-term, reduce the use and harm of MDFTs in Seattle:

- **Ban the use of consent searches of mobile devices.** Police consent searches in any context are troubling, but the power and information asymmetries of cellphone consent searches are egregious and unfixable. Accordingly, policymakers should ban the use of consent searches of cellphones.[30]

  As explained in Section 4, the doctrine underlying "consent searches" is a legal fiction.[31] When courts pretend that "consent searches" are voluntary, they fail to account for the important racial differences in how individuals interact with law enforcement.[32] As one scholar noted, "many African Americans, and undoubtedly other people of color, know that refusing to accede to the authority of the police, and even seemingly polite requests—can have deadly consequences."[33] Given the extreme power asymmetries, it's a "simple truism that many people, if not most, will always feel coerced by police 'requests' to search."[34] Further, most of the

[30] California's Racial and Identity *Profiling* Advisory Board recently suggested that policymakers should "should consider prohibiting consent searches of cell phones." *See* Racial & Identity *Profiling* Advisory Board, Racial & Identity *Profiling* Advisory Board Annual Report 2022, 112 (January 2022).
[31] Ric Simmons, *Not "Voluntary" but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773, 775 (2005) ("Over 90% of warrantless police searches are accomplished through the use of the consent exception to the Fourth Amendment.")
[32] Tracey Maclin, *"Black and Blue Encounters" Some Preliminary Thoughts About Fourth Amendment Seizures: Should Race Matter?*, 26 Val. U. L. Rev. 243, 248 (1991). ("Instead of acknowledging the reality that exists on the street, the Court hides behind a legal fiction. The Court constructs Fourth Amendment principles assuming that there is an average, hypothetical person who interacts with the police officers. This notion . . . ignores the real world that police officers and black men live in.")
[33] Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 242-243 (2001). ("Given this sad history, it can be presumed that at least for some persons of color, any police request for consent to search will be viewed as an unequivocal demand to search that is disobeyed or challenged only at significant risk of bodily harm.") Indeed, as another scholar argued, the "consent search doctrine is the handmaiden of racial profiling." See George C. Thomas III, *Terrorism, Race and a New Approach to Consent Searches*, 73 Miss. L. J. 525, 542 (2003).
[34] Marcy Strauss, *Reconstructing Consent*, 92 J.Crim. L. & Criminology 211, 221.(2001.)

Upturn
Toward Justice in Technology

"consent to search" forms Upturn obtained from law enforcement agencies don't clearly specify how they will search the phone, the tools they'll use, or the extent of the search.[35]

Some believe that officers should provide warnings to ensure consent searches are voluntary. Such warnings would inform the subject of the search that they are being asked to voluntarily, knowingly, and intelligently consent to a search. But warnings are not enough. One study found that participants who received a warning about their right to refuse a consent search were just as likely to comply with the search.[36] This is also consistent with an earlier analysis of data collected from the Ohio Highway Patrol on motor vehicle stops, which found no decrease in consent rates after a law requiring warnings was introduced.[37]

Banning consent searches is not a new suggestion.[38] Nor is it a perfect solution, as it's easy for law enforcement to obtain a search warrant. But banning consent searches of cellphones can help limit police discretion, limit the coercive power of police, and minimize the amount of information that can be collected from people

---

[35] The Denver Police Department's consent form mentions that devices may be submitted "to the computer forensic laboratory for copying and examination." *See* https://beta.documentcloud.org/documents/20390003-consent-for-search-of-cell-phone-tablet. The Tampa Police Department's mentions that "this search may require the temporary utilization of software and/or hardware." *See* https://beta.documentcloud.org/documents/20393153-tpd-form-142-e-consent-to-search-electronic-media-devices-english. The Colorado State Patrol's consent form mentions that they can "submit the electronic device described below to a computer/electronic forensic examiner . . . who has specialized training necessary to conduct such an examination." *See* https://beta.documentcloud.org/documents/20391059-csp-343-consent-to-search-electronic-device. The Illinois State Police's consent to search form mentions that their search "may include the duplication/imaging and complete forensic analysis of any data contained within the internal, external, andlor removable storage media of this device." *See* https://beta.documentcloud.org/documents/20391550-img_0001.

[36] Roseanna Sommers, Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 Yale L. J. 1962, 2000 (2019).

[37] Illya Lichtenberg, *Miranda in Ohio: The Effects of Robinette on the "Voluntary" Waiver of Fourth Amendment Rights*, 44 HOW. L.J. 349 (2001) (Examined highway stops in Ohio between 1987 and 1997. During that time period, the state introduced a law requiring police to inform motorists that they were free to leave before requesting consent. Lichtenberg found no decrease in consent rates among motorists before versus after the reform was adopted.)

[38] For example, the New Jersey Supreme Court outlawed consent searches during traffic stops where no reasonable suspicion exists. The California Highway Patrol banned its use of consent searches as part of a broader class action lawsuit brought because of racial profiling. And in Rhode Island, by law, "[n]o operator or owner-passenger of a motor vehicle shall be requested to consent to a search by a law enforcement officer of his or her motor vehicle, that is stopped solely for a traffic violation, unless there exists reasonable suspicion or probable cause of criminal activity."

Upturn
Toward Justice in Technology

under investigation. Seattle City Council should ban consent searches of cellphones.

- **Require easy-to-understand audit logs.** Seattle City Council should require that mobile device forensic tools used by law enforcement have clear recordkeeping functions, specifically, detailed audit logs and automatic screen recording. With such logs, judges and others could understand the precise steps that law enforcement took when extracting and examining a phone, and public defenders would be better equipped to challenge those steps. Audit logs and screen recordings would document a chronological record of all interactions that law enforcement had with the software, such as how they browsed through the data, what search queries they used, and what data they could have seen. This information would be stored in the MDFT itself as a log that is easily shareable with auditors, judges, and defenders.

There is an extreme power and resource imbalance between public defenders and law enforcement in general,[39] and especially when it comes to digital evidence. Few public defenders have access to MDFTs. Instead, defenders are forced to examine forensic reports that are thousands of pages long and "easily navigable only if you have a forensic company's proprietary software"— which they can rarely afford.[40] Further, defenders and judges often have no way of knowing whether law enforcement actually stayed within the bounds of a search warrant for a phone. For courts, simply taking law enforcement's word for it should be insufficient — lying

[39] Research has demonstrated that fewer than 30 percent of county-based and 21 percent of state-based public defender offices have enough attorneys to adequately handle their caseloads. *See* Bureau of Justice Statistics, Lynn Langton and Donald Farole Jr., County Based and Local Public Defender Offices, 2007 (2010), 8, https://www.bjs.gov/content/pub/pdf/clpdo07.pdf; Bureau of Justice Statistics, Lynn Langton and Donald Farole Jr., State Public Defender Programs, 2007 (2010), 12, https://bjs.ojp.gov/content/pub/pdf/spdp07.pdf. *Also see* Justice Policy Institute, System Overload: The costs of Under-Resourcing Public Defense, 2011, *available at* http://www.justicepolicy.org/uploads/justicepolicy/documents/system_overload_final.pdf; American Bar Association, Gideon's Broken Promise: America's Continuing Quest for Equal Justice (2004); Bryan Furst, A Fair Fight: Achieving Indigent Defense Resource Parity, Brennan Center, September 9, 2019, *available at* https://www.brennancenter.org/sites/default/files/2019-09/Report_A%20Fair%20Fight.pdf.

[40] Kashmir Hill, "Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone." New York Times, November 22, 2019, *available at* https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html.

Upturn
Toward Justice in Technology

under oath is endemic to the institution of American policing.[41] Thus, audit logs would be especially helpful for defenders trying to suppress evidence that was obtained illegally.

This recommendation even comports with principles articulated by law enforcement associations, like the Association of Chief Police Officers, which has said that "[a]n audit trail . . . of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result."[42] Seattle Police Department even wrote that "all device utilization is documented and **subject to audit** by the Office of Inspector General and the federal monitor at any time."[43] Having these logs ensure that actual, detailed audits are possible.

The critical caveat is that audit logging is unlikely to be an effective tool for broad transparency and police accountability. This tool will not necessarily improve police behavior, but on a case-by-case basis, this tool could give public defenders

[41] *See, e.g.*, Irving Younger, "The Perjury Routine," The Nation, May 8, 1967; Myron R. Orfield, *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 Chi. L. Rev. 1016 (1987); Commission to Investigate Allegations of Police Corruption and the Anti-Corruption Procedures of the Police Department, City of New York, Commission Report (1994) at 38; Stanley Fisher, *"Just the Facts, Ma'am": Lying and the Omission of Exculpatory Evidence in Police Reports*, 28 N. Eng. L. Rev. (1993); Joseph Goldstein, "'Testilying' by Police: A Stubborn Problem," The New York Times, March 18, 2018, *available at* https://www.nytimes.com/2018/03/18/nyregion/testilying-police-perjury-new-york.html; Peter Keane, "Why cops lie," San Francisco Chronicle, March 15, 2011; Michael Oliver Foley, Police Perjury: A Factorial Survey, (2000); Samuel Gross, et al., *Government Misconduct and Convicting the Innocent: The Role of Prosecutors, Police and Other Law Enforcement*, National Registry of Exoneration, September 1, 2020, *available at* https://www.law.umich.edu/special/exoneration/Documents/Government_Misconduct_and_Convicting_the_Innocent.pdf.

[42] Association of Chief Police Officers, *APCO Good Practice Guide for Computer based Electronic Evidence*, March 2012, *available at* https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. *Also see*: Rick Ayers, Sam Brothers, Wayne Jansen, *Guidelines on Mobile Device Forensics*, NIST Special Publication 800-101, Revision 1, National Institute of Standards and Technology, May 2014, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. (noting that "[p]roper documentation is essential in providing individuals the ability to re-create the process from beginning to end."); Scientific Working Group on Digital Evidence, SWGDE Best Practices for Mobile Phone Forensics, Feb. 11, 2013, *available at* https://drive.google.com/open?id=18dwENQNztbEa0G9GLSUeDxZxeDEeUc-3 (noting that documentation should include "sufficient detail to enable another examiner, competent in the same area of expertise, to repeat the findings independently.").

[43] Computer, Cellphone, and Mobile Device Extraction Tools. Seattle Police Department. https://www.seattle.gov/documents/Departments/Tech/Privacy/Computer%2C%20Cellphone%2C%20%26%20Mobile%20Data%20Extraction%20One%20Pager.pdf

Upturn
Toward Justice in Technology

and judges a significantly clearer window into the nature and extent of cellphone searches.

- **Enact robust data deletion and sealing requirements.** Seattle City Council should require law enforcement to delete any extracted cellphone data that is not related to the objective of the warrant within thirty days of the date the information is obtained.[44] In addition, for cases that result in a conviction, data that was deemed relevant should be sealed at the conclusion of the case. For other cases, where charges are dismissed or do not result in conviction, all data should be deleted, relevant or not. Data deemed relevant in one case should never be used for general intelligence purposes or used in unrelated cases.

  In the absence of clear law or policy, law enforcement could use personal information like contact lists, photos, and location data to fuel harmful police surveillance systems. This is true not only for the person whose phone was searched, but also for anyone they have used their phone to contact — friends, family, colleagues, or even new acquaintances. Cellphone searches are unlike traditional seizures because law enforcement extracts all of the data on the device and only after this seizure do they search for case-relevant information. Maintaining information outside the scope of the warrant is akin to law enforcement maintaining the ability to indefinitely and limitlessly search a home.

- **Require public logging of SPD use of MDFTs.** The City of Seattle should require public reporting and logging of how law enforcement use mobile device forensic tools. These records should be released at least monthly, as this would allow more immediate access to information by advocates, policymakers, and the public seeking to understand the capabilities and practices of their police agency. Agencies should additionally release annual reports on overall department usage.

  These records should include aggregate information such as:

  - How many phones were searched in a given time period.
  - Whether those searches were by consent (though consent searches should be banned), or through a warrant.
  - Warrant numbers associated with searches, when applicable.
  - The types of offenses being investigated.

[44] The only exception should be for exculpatory information.

Upturn
Toward Justice in Technology

- How often MDFTs led to successful data extractions.
- Explanations for any failed extractions.
- Which tools were used for extraction and analysis, and their version numbers.

## Conclusion

Mobile device forensic tools are far too powerful to be in the hands of law enforcement. Phones centralize more information about a person than previously possible and MDFTs are designed to extract the maximum amount of information from them. The racial disparities in who police target for searches and surveillance mean that Black and brown people living in Seattle are far more likely to be harmed by cellphone searches. That these tools have no real limits or policies governing their use is untenable.

Short of an outright ban of MDFTs, there are many ways to immediately reduce the harm these tools currently create: Audit logs, clear public logging, data deletion, and sealing can reduce the scale at which MDFTs create and exacerbate harm. Banning consent searches in general, and especially for cellphones, would protect individuals from coercive searches by police and from unwittingly turning over essentially all of their personal information.

I hope that this information is useful to the Council and Surveillance Working Group. Thank you for the opportunity to comment on these technologies.

Sincerely,

Urmila Janardan
Policy Analyst, Upturn
urmila@upturn.org

City of Seattle

# Appendix E: Questions and Department Responses

| Question | Response |
|---|---|
| About that, um, could you share, for the [MBSTs?] what vendors provide SPD the extraction tools -- and how many extraction tools SPD currently owns? | SPD is asking that we not be required to disclose these vendors at this time. If Council requires it, we will comply. |
| Concerning the mobile device extraction tools, does SPD (and others audio was distorted) use what would be called white glove type services from the digital forensic providers tool that entails either physically handing the device over to the tool provider or providing an image or the device to the tool provider? | Yes. On occasion, when time is a critical factor, we will send a phone to the vendor and they will return it with the extracted files. Not as often since we are able to do it ourselves better now. |
| Regarding the extraction tools, given that in 2017 SPD handed a phone over to the King County Sherriff's office to do a chip off extraction and in 2018 and SPD gave the phone to the King County Sherriff's office to decide for a pin -- and in 2019 the King County sheriff's office attempted to alter the phone's operating system to disable the password. When these kinds of events occur, do those kinds of events entail the detective working out of the facilities or the phone's physical given to King County? | KCSO took custody of the devices, maintaining the chain of custody as required for evidence, then returned the devices to us along with the extracted files. |
| Could you could you share what safeguards are specifically in place to protect data from unauthorized access and is there a way for SPD to provide an audit trail?<br><br>(Re: the mobile device extraction tools)<br><br>(Re: any data collected with this tool from unauthorized access. This is regarding 4.10.)<br><br>What is the data protected and what sort of audit mechanisms are there? And if there's any sort of safeguards encryption or access control mechanisms, etc.? | Extracted information is turned over to the case detective and handled in accordance with electronic evidence policies. The unit that does the extraction does not keep files. Users keep logs associated with the use of the extraction tools, subject to audit by OIG, Monitor and SPD Audits. |
| Going back to the mobile device extraction tools, would you describe what kinds of investigations these tools are used for besides sexual assault and child abuse investigations or could you describe the range? | The sexual assault and child abuse are definitely two of the high points and are high utilizers of that -- but we also have our internet crimes against children group that would benefit from the gathering of information in a cell phone could be a user of that. Now that being said, these devices are not scattered throughout every single investigative units, only the units that use them |

| | |
|---|---|
| | the most, which would be our Internet crimes against children and our sexual assault child abuse unit detectives are the ones that actually have the devices, but any investigation that would benefit from the information inside a device that needs to be extracted, would be able to apply for a warrant with the help of the detective who is able to use that device. But any investigation that would benefit from the information inside the device would be able to apply for a warrant with the help of the detective who is able to use that device. |
| In the SIR it is stated that 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 report order warrant, the device is purged in its entirety and no data is provided to the requesting officer or detective for the investigation file. Could you clarify under what circumstances would no data be collected and could you share how often that happens?<br><br>That's in section 4.2. | Data collect if I recall the, what you just quoted from the said, no data is collected, that is relevant to the investigation, or within the scope of the consent warrant. Is that correct? Sure, I'll double check and see if I can get a determination of how percentage wise, how frequently that occurs during the use of this technology. I could imagine a situation where, uh, the detective develops probable cause and obtains a warrant to search a phone only. To find that prior to getting securing the phone to serve the warrant, that it's been wiped clean of any of the information that was relevant to the investigation. So that would be a situation. I could see where no data is collected during the extraction. That would be relevant to the investigation so I could see that being a case, you know, very, very broadly. Like that could occur. |
| Could you share when an officer or detective requests use of the data extraction tool, does that officer or detective need to articulate something that they're specifically looking for? I guess also asking what, what would constitute probable cause, or or can they request the use of the tool just hoping they're able to find something? | No, it's all subject to the requirements set in the warrant. So they have to convince a judge. They have probable cause to believe that evidence of the crime they are investigating exists within the device that they are trying to extract from. It's up to the judge to determine if the office, if the detective, our officers probable cause is accurate and appropriate. That's why we use the warrant process. |
| Similar question to the one about GeoTime; is, in this case, is there any SPD policy defining the incident types that can use the mobile device extraction tools -- or would you be permitted to use these for instance for when someone is associated with civil unrest and protesting, but not affliated or suspected in any serious crimes, not homicide or those kinds of things. | Well, we would need to we need to apply with the intelligence. Intelligence work. As it relates to people's right to free assembly and laws related to that. We also need to judge that we have probable cause that they weren't that a evidence exists of. Crime within that device, so the policy wouldn't necessarily say, you can't use it for this type of crime or that type of crime. But civil unrest is not something where we would where |

we would just throw it in there. Unless we were investigating a crime and had probable cause that we could present to a judge in the warrant process.

Could you share how much [and] what data (this is regarding the mobile device extraction tools) once the data has been extracted from the device using this tool, could you share how much of that data is typically stored on the extraction device before it is downloaded to the investigation file? Is it immediate deletion of data on the extraction device?

Uh, I'm double checking on that right now. Um, I guess it would depend on how quickly it can be extracted to wherever it's going to wherever it's being stored. I would also. Depend on the size and nature of the data that's being pulled. I imagine that pulling text messages off a single cell phone is significantly smaller than copying an entire hard drive off of the computers. So it would depend on the size of the files.

So, to clarify the only limitation that, that would not lead to the immediate deletion of data on the extraction devices is just the time it takes for that to happen.

And the time it would take to review the data that was extracted to ensure that it is not associated. With the crime that's being committed, or that's being investigated.

For the mobile device extraction tools, once the extracted file data is saved, [distorted audio] how many employees not directly involved with the case have access to the files?

No, not all SSP employees have. It's subject to the security related to all of our evidence policies. So when it's submitted to evidence, was it digitally or physically person has to have a reason and association with the investigation staff to clear it out of the. To review it.

[For example] if someone deals with robberies or stolen cars, that kind of stuff, that would be one kind of access, as compared to those with access to assault and homicide? So I'm wondering can they accessed by all SPD employees? Or is that somehow on segmented?

City of Seattle

# Appendix F: All Comments Received from Members of the Public

**ID:** 114044272857

**Submitted Through:** SurveyMonkey

**Date:** 6/2/2022 11:10:04 PM

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

SPD: Computer, cellphone and mobile device extraction tools

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

These tools are very likely to sweep up incidental data – potentially including other people's data as well as the people who are consenting to their use. Surveillance technologies are typically used disproportionately to target people of color, LGBTQ+ people, unhoused people, and activists. Unless there's clear policies and procedures in place, and officers have been given sufficient training, that's very likely to be the case with these technologies as well. Third-party vendors and other governmental entities may misuse the data shared with them. This data may well be processed as part of automated analyses that introduce further racial bias risks. While some sections of the SIR (including 3.2 and 2.5) say that the tools can only be used with consent or a warrant, other sections in the SIR (including 2.4 and 7.1) discuss usage under RCW 9.73.210, and Section 4.2 discusses use by a court order.

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

The technology can make it possible for SPD to collect some kinds of evidence that they would not otherwise be able to, or provide proof of chain of custody for information they are collecting with consent. This potential value needs to be weighed against the possibility of over-collection, misuse of data, and discrimination.

**Do you have any other comments?**

What specific devices does SPD currently use for these tasks? What devices are being considered for future use? What are the contractual agreements with the vendors? What purposes do any of the agreements with vendors allow them to use the data for? For example, they can presumably use it to diagnose problems with their software. Can they also use it to improve their product? Develop future products? "Legitimate business purposes"? Are there any technical safeguards in place to prevent third-party vendors misusing the data? Is any automated analysis done by vendors, SPD, or any of the entities the data is shared with? If so, is there an Algorithmic Impact Report or algorithmic audit? Has SPD audited third-party vendors to ensure that they are not misusing the data? What restrictions are in place on the entities listed in 6.1 further sharing the data? Do any of the entities listed in 6.1 share data with Fusion Centers? Does training for SAU, TAU, supervisors and commanders, specifically cover discriminatory uses and the possibilities of extraction also including people's data? How detailed is the information currently being tracked about how these systems are used? Is there enough information there to identify discriminatory patterns, and whether other people's data has been obtained? What percentage of deployments have been audited by the Office of the Inspector General? Do these audits specifically look at discriminatory uses and whether other people's data has been obtained? Have any of these reports been published? What percentage of deployments have been audited by the Federal Monitor? Do these audits specifically look at discriminatory uses, and whether other people's data has been obtained? Have any of these reports been published? What percentage of deployments have been audited by SPD's Intelligence and Analysis Section? Do these audits specifically look at discriminatory uses, and whether other people's data has been obtained? Have any of these reports been published?

---

City of Seattle

**ID:** 114044214670

**Submitted Through:** SurveyMonkey

**Date:** 6/2/2022 8:27:25 PM

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

SPD: Computer, cellphone and mobile device extraction tools

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

During the 2020 protests, SPD arrested protesters without cause or on weak grounds. It is disturbing that, unless real safeguards are in place, SPD can use this technology on virtually anyone they target.

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

**Do you have any other comments?**

---

City of Seattle

**ID:** 114043245083

**Submitted Through:** SurveyMonkey

**Date:** 6/1/2022 5:49:18 PM

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

SPD: Computer, cellphone and mobile device extraction tools

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

1) The majority of SPD's consent-based searches were limitless, with no date or data type limitation; whereas only a quarter of all warrant-based searches were limitless (based on PRA data, 66% of consent-based searches were limitless compared to 24% of warrant-based searches). An unlimited extraction of a device is very likely to be disproportionate to the scope of evidence detectives are seeking. This problem likely exists due to many people who provided consent not having legal representation advising them about their full rights in the situation. Given the power imbalance between an SPD officer and member of the public, many people would not feel they have the power to deny a request to search their device by SPD. It may not take much for people to feel coerced into giving consent. 2) Nothing prohibits SPD from using coercion to gain consent to use these tools (such as, arresting a bunch of people at a protest and saying "Anyone who doesn't want to spend the night in jail, just let us search your phone"). 3) Nothing prohibits SPD from gaining consent from a minor to extract all the data on their phone without any legal representation for the minor. 4) These devices can capture a wide range of data (i.e. calls/texts, contacts, location/search history, app files, cloud service passwords, deleted files, deleted apps, screenshots of open windows used by the device's app switcher menu, and much more). A person providing consent for these tools to be used on their devices is very likely unaware of the full range of data that's on the device and thus what SPD would have. This lack of awareness for consent-based searches seems to be confirmed by the fact that so few of them are limited by date or data-type, unlike the warrant-based searches. 5) If cloud service passwords are extracted, then this would give SPD unfettered access to whatever data is stored outside of the device in the cloud. This would be well beyond the scope of extracting the physical device locally. This would be like SPD having access to search your home whenever they want simply because you consented once to letting them search your home. This is another aspect that many people would not be aware of the risk to their privacy when consenting to have their device extracted. SPD should explicitly request access to the cloud services in either the warrant request or consent request. 6) Nothing restricts the use of these tools to only violent offenses. Given the wide range of data these tools collect, they are very privacy invading. As such, their use should be limited to serious or violent offenses. 7) Its known from PRA data that at a minimum SPD has used digital extraction/forensic tools from Cellebrite, GrayShift, Octoplus, Medusa Pro, MSAB Inc (aka Micro Systemation, XRY), and possibly also Magnet Forensics. While there's only been enough time during the public comment period to investigate one out of these six manufacturers, the one that has been investigated is very problematic. Specifically, Cellebrite is an Israeli company that is known to sell their products to autocratic repressive regimes (even after Cellebrite said they would stop). For example, this article ( https://theintercept.com/2022/02/08/cellebrite-phone-hacking-government-agencies/ ) states, "Cellebrite’s technology is cheaper and has been used in China to surveil people at the Tibetan border, in Bahrain to persecute a tortured political dissident, and in Myanmar to pry into the cellphones of two Reuters journalists." And the Cellebrite employee who stated, "As a former Cellebrite employee, I can say from personal experience that the company does nothing to prevent the abuse of its products by customers. It knowingly sells products and services to users of dubious repute, belonging to autocratic regimes" ( https://www.haaretz.com/israel-news/2021-07-27/ty-article/i-worked-at-israeli-phone-hacking-firm-cellebrite-they-lied-to-us/0000017f-f652-d460-afff-ff764fae0000 ). And Cellebrite products have been found available for sale still in countries that Cellebrite said they

would stop doing business with. This article ( https://theintercept.com/2021/08/26/cellebrite-china-cellphone-hack/ ) further states, "[Eitay] Mack [,a human rights lawyer] said Cellebrite's sales in countries like China raise the question of why the U.S. government hasn't put more pressure on Israel's Ministry of Defense, which issues a license to Cellebrite. 'I don't understand how the U.S. and the EU governments are turning a blind eye to the businesses that the Israeli government is allowing,' he said. 'This is a privilege that the Israeli government and Israeli companies have that other countries don't have.'" This led to this open letter from a coalition of 30 organizations & individuals signed on regarding Cellebrite's involvement in human rights abuses, https://www.accessnow.org/cms/assets/uploads/2021/07/CSO_Open-Letter_on_Cellebrite.pdf . This is on top of the fact, that Cellebrite's tools rely on Cellbrite not participating in what's known in the security industry as "responsible disclosure". Instead, Cellebrite, intentionally hacks various phones to find weaknesses they can bundle into their products without reporting that security vulnerability to Apple/Google/Microsoft. These exploits are used by SPD when they do extractions of locked devices and this would be illegal if done by any member of the public to another member of the public. Additionally, while Cellebrite tries to find weakness in mobile phones, it doesn't appear to apply very much due diligence to the security of it's own tools. Instead, Cellebrite's flagship product was found to have numerous security vulnerabilities, https://signal.org/blog/cellebrite-vulnerabilities/ . Based on the SIR and PRA data, SPD is spending at least $200k - 240k per year for digital extraction tools. While not all of that expense is paid to Cellebrite, a likely large percentage of it is. Seattle and specifically SPD should not be funding this unethical product from an unethical company. Divest from Cellebrite. 8) SPD has not named in the SIR the digital extraction tools they use, so the public's assessment of this technology is very incomplete. SPD should not be permitted to use any secret surveillance technologies. One of the purposes of the surveillance ordinance is to provide transparency to the public. The PRA data we have is multiple years old and is unknown what tools SPD is currently using. The public also has not seen any of the contracts, terms or service, customer agreements, privacy policies, or any other legal documents governing the use of these tools. It's very problematic to have a city department attempt to hide information from the public, whom they are accountable to and is funding these tools in the first place. Moreover, for this same transparency reason, SPD should be prohibited from signing an NDA with any surveillance technology manufacturer/vendor/reseller. 9) The process of extracting and copying data from the device should be done in a forensically sound manner (i.e. non-writing, not leaving digital artifacts on the device). This includes that SPD should not install software onto the device without the device owner's explicit consent for that installation. Specifically, SPD should be prohibited from installing key loggers (like GrayShift's HideUI, https://www.nbcnews.com/tech/security/iphone-spyware-lets-cops-log-suspects-passcodes-when-cracking-doesn-n1209296 ) or other spyware onto the device. Consent is for extraction only, not writing anything to the device. Installing a key logger is unethical and instead SPD should get a court-approved warrant compelling the device owner to provide the password/passcode or otherwise provide unlocked access to the device. If such court-approved warrant cannot be attained, then the detectives should seek other pathways of investigating the case. 10) Nothing prohibits SPD from using biometric tools (face/gait/voice/etc analysis) on the data they extract from the device. 11) Potentially disproportionate use of these tools. It is known that there are racial disparities in arrest rates.

Therefore, it is likely that the digital extractions also reflect a racial disparity in their use. 12) Nothing prohibits an SPD employee from using one of these tools for their own personal use, outside the confines of a legal criminal investigation. Specifically, these tools could be used for the purpose of domestic abuse where the SPD employee extracts data from the device owned by their wife/gf/partner so as to see her deleted pictures, location history, deleted apps, or other information. As such, there needs to be an explicit prohibition against individuals using these tools for personal use and holding them criminally/civilly liable if they do. 13) Given the vast range of data these devices can collect, data that is unrelated to the objective of the warrant (unless it is exculpatory data) should not be retained, propagated, or further reviewed after the fact. 14) Nothing prohibits the propagation of data SPD attains via digital extraction, such as to partner agencies uninvolved with the investigation and/or to Fusion Centers. This is specially concerning when that data was for a case were charges were dropped or the person wasn't convicted; or the data was shared before the data gets validated via the court proceedings process (so the data might be so poor in quality to not be admissible in court but is already shared with an outside agency or Fusion Center in that unvalidated state). It would also be concerning if such data was shared without a warrant. 15) The logs these tools generate can be insufficient to provide transparency or auditability. This can make it hard to tell if the extraction was indeed contained to the scope of the warrant or consent, which places judges and defenders in a place of having to rely simply on trusting the police department. There's no valid reason that should be the case with digital extraction. There is ample opportunity for the tools to log the details of their extractions in such a way that a judge/defender can clearly retrace the steps without having the extraction tool themselves. As such, City Council should require that digital extraction tools used by SPD must have detailed audit logs and automatic screen recording. 16) Data that was attained during an investigation where that suspect either had the charges dropped or was not convicted should not be retained by SPD. Once charges are dropped or there's no conviction, then that person is legally innocent. As such, their data should not be retained or re-used (unless needed for exculpatory reasons). 17) Item 2.5 in the SIR is misleading and incorrect. It states, "All data extracted is stored securely on premises within SAU – not accessible to any vendor" and "Extraction is conducted in-house ... No data is stored by a vendor, as the necessary tools are maintained entirely offline and on-premises." However, SPD has acknowledged in the second public engagement meeting that they do use "white glove" type services from the tool providers that entails physically handing the device over to the tool provider. Based on PRA data, we know that about 7% of all SPD extractions were sent to "CAIS", which is Cellebrite Advanced Investigative Services, meaning that Cellebrite had the phone, not SPD. So these extraction are not limited to the SPD premises and the chain of custody enters the hands of a private company (Cellebrite). Given the SIR is incorrect, it's important that is corrected in the SIR so that public has an accurate understanding. 18) Item 3.3 in the SIR refers to SPD Policies 5.001 and 5.002, but neither of those are specific to digital extraction devices. It doesn't appear that there's any SPD policy specifically governing this exact type of technology. City Council should heed the concerns and recommendations from the public so as to fill this gap. 19) Item 4.6 in the SIR states, "On occasion, extraction may be utilized in the field." It is unclear to the public under what circumstances an extraction would ever be done in the field. With both consent and warrant, the device is handed over to SPD. There should be no urgent reason to do an extraction in the

field. It would also seem likely that an extraction done in the field was probably done under consent, not warrant, which again confirms the presence of likely coercive consent being attained by SPD due to lack of legal representation for the device's owner. 20) Item 8.2 in the SIR states, "No formal audits exist for extraction tool requests or deployments..." This is concerning since if I understand correctly, SPD's use of these tools have never been audited. 21) The SIR does not mention that SPD at times will give a device over to the King County Sheriff's Office (KCSO) for them to conduct the extraction; and that specifically, the types of techniques that KCSO uses are more advanced than the tools SPD uses, such as chip-off extractions or altering the operating system. The public should know the full scope of how SPD attains digital extractions, including the use of outside government or private services. It's also unknown to the public if the KCSO is the only external governmental entity that assists SPD with digital extractions. 22) It's unknown the public the scope of the use of these tools, such as: What percentage of cases per year use the digital device extraction tools? Roughly how many incidents per year does SPD use the digital device extraction tools for? How many hours per week are the digital device extractions tools used on average? How many people have access to use these tools? 23) It's unknown to the public what percentage of devices that were extracted are owned or primarily used by people who are under the age of 18.

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

Any value must be weighed against it's risks. The risks here are quite substantial. Given that plus the low likelihood for City Council adding the safeguards the public has requested, I don't think the value is useful enough. There must be sufficient safeguards in place before I'd consider these tools anything but simply dangerous.

**Do you have any other comments?**

---

City of Seattle

**ID:** 114034986368

**Submitted Through:** SurveyMonkey

**Date:** 5/20/2022 2:18:50 PM

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

SPD: Computer, cellphone and mobile device extraction tools

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

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

**Do you have any other comments?**

1. Which vendor(s) provide SPD the extraction tools they use? 2. How many extraction tools does SPD currently own? 3. What is the cost to obtain and maintain each? What funding source(s) does SPD use to cover these costs/expenditures? 4. With what frequency/how often does SPD use extraction tools? a. How many times a week/for how many investigations a week is it used? 5. Besides sexual assault and child abuse investigations, what kinds of investigations are extraction tools used for? Describe the range of investigations and what kinds of investigations they are mostly used for. 6. How often are extraction tools used in the field vs. at a unit work station? Under what circumstances are they used in the field vs. at a unit work station? 7. What does the training and certification for these extraction devices entail? a. How many hours of training do they receive? What does the training cover? b. Do they receive periodic updated training? c. Is there a privacy component to the training that is specific to the privacy risks of this tech? (response to 7.2 indicates no.) 8. What does the process of obtaining consent from the phone owner look like? a. In what context does an officer/detective typically ask a person for consent to access their phone? Is the person under arrest at the time they are asked for consent? b. Are they provided the opportunity to consult with a lawyer before they make a decision? c. Verbal consent? Written consent? Is there a script that officers/detectives follow? If so, what does that script say? d. What information is the phone owner provided about how their data will be extracted and what data? Is the person informed both verbally and in writing that the extraction tool will extract a full copy of data from their device—all emails, texts, photos, location, app data and more—which can then be programmatically searched? e. How is the consent process different for non-English speakers, if at all? 9.4.1—"Extraction tools of mobile devices, excluding computer imaging, collects information from electronic devices, including contact lists, call logs, Short Messaging Service (SMS) and MultiMedia 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." When an officer/detective requests use of a data extraction tool, do they need to articulate something they are specifically looking for? Or can they request it just hoping they are able to find something incriminating? (i.e. fishing expedition) 10. 4.2—SPD states: "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." Under what circumstances would no data be collected? How often does that happen? 11. 4.10 asks about safeguards in place for protecting data from unauthorized access and to provide an audit trail. SPDS's response is not very detailed or satisfactory. What safeguards are in place for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (view logging, modification logging, etc.)? 12. How often is a deployment audit performed? How often is a request audit performed? When was the last time an audit was performed for each? 13. 5.1—SPD states: "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." How much time is data typically stored on an extraction device before it is downloaded to the investigation file? Is it immediate? Is deletion of data on the extraction device also immediate? Is that reflected in the training? 14. Who has access to the data on the extraction device? How many

people have access to the data? 15. Who has access to the data once it has been downloaded? How many people have access? 16. 6.1—To clarify, is the data obtained via extraction tools subject to the PRA?

---

City of Seattle

**ID:** 114034404791

**Submitted Through:** SurveyMonkey

**Date:** 5/19/2022 10:05:12 PM

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

SPD: Computer, cellphone and mobile device extraction tools

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

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

**Do you have any other comments?**

A) What percentage of cases per year use the digital device extraction tools? Roughly how many incidents per year does SPD use the digital device extraction tools for? How many hours per week are the digital device extractions tools used on average? B) Is the King County Sheriff's Office the only external governmental entity that assists SPD in conducting a digital extraction? C) What if the extraction for a single device results in some data assisting in the pursuit of the investigation but other data does not? For example, if the text messaging history between the suspect and long-time friend implies that the subject did commit a serious crime, but there is other text messaging history say between the subject and their grandmother where she's asking for help getting her medical prescriptions, then what happens with the texts between the subject and the grandmother; Are they retained as well? Which department would be responsible for excluding, removing, or deleting that out of scope data? D) SIR item 4.6 states that "On occasion, extraction may be utilized in the field." Could you elaborate on why an extraction would ever be needed in the field, since for both consent & warrant, the device would be handed over to SPD which would be much more convenient to simply process in-house instead of in the field? E) When was the last audit of SPD's Sexual Assault and Child Abuse Unit (SAU)? Where can that audit report be found? F) Are there any SPD policies that specifically govern the mobile device forensic tools (not just generic policies about data retention, storage, etc)? G) Is data from extraction tools subject to PRA? That is, can someone is not the owner of the device (nor a legal representative of them nor a legal representative of their opposition - just some rando), request and attain(via PRA) the data gathered by SPD using the digital extraction tools? H) Given that item 2.5 in the SIR states "The SAU Unit manages extraction tools that they utilize within their unit. ... All data extracted is stored securely on premises within SAU – not accessible to any vendor." and "Extraction is conducted in-house ... No data is stored by a vendor, as the necessary tools are maintained entirely offline and on-premises."; but when asked "Do either SPD's SAU or TESU use 'white glove' type services from the digital forensic tool providers that entails either physically handing the device over to the tool provider or providing an image of the device's storage to the tool provider?", SPD answered, "Yes on occasion, but not very often, very rarely used", then will 2.5 in the SIR be updated to reflect that? Not very often is not the same as never and the SIR should accurately articulate that the device/data does leave the SPD premises (though if the 'white glove' services are the vendor coming on site to SPD facilities then that would be an improvement to also specify in the SIR). I) How many people have access to the mobile device extraction tools?

---

City of Seattle

**ID:** 114023313332

**Submitted Through:** SurveyMonkey

**Date:** 5/9/2022 10:50:10 AM

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

SPD: Computer, cellphone and mobile device extraction tools

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

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

**Do you have any other comments?**

---

City of Seattle

**ID:** 114019066849

**Submitted Through:** SurveyMonkey

**Date:** 4/27/2022 10:01:32 PM

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

SPD: Computer, cellphone and mobile device extraction tools

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

I think that this is great. It gives me peace of mind. We need more cameras around the city so that people can walk around safely even at night alone.

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

People can have more safety and more people doing bad stuff can be caught easier. It's hard to catch them on the phones and now you can.

**Do you have any other comments?**

I would like to see how the technology is helping us.

---

# Email Comment

**Questions:**

- Is any of the data from device extraction tools shared or accessed by Fusion Centers? Does the Fusion Center access SPD data, and is a warrant?
- What are the names of the specific manufacturers and their individual product names of the computer, cellphone and mobile device extraction tools (physical tools and software) that SPD is using, has or plans to purchase, and used in the past?
- Is legal representation required in order for a person to give consent to the use of these tools on their device?

**Key Concerns:**

- It's unclear whether the deployment of this technology is disproportionately used against marginalized and minority individuals and communities.
- Consent for SPD to use these tools may be coerced from low-level offenders, for instance as a bargaining chip to avoid detention or arrest, or as a threat.
  Note: Based on Upturn's PRA records from 2017-2019, the majority of SPD's consent-based searches were limitless, with no date or data type limitation; whereas only a quarter of all warrant-based searches were limitless (66% of consent-based searches were limitless compared to 24% of warrant-based searches).
- The SPD uses extractive tools that access ALL DATA on a device, scooping up many people's data from their electronic devices, including cell phones, smart phones, tablets, computers and other devices.
- Data collected via extraction tools can include contacts, call logs, messages, GPS locations, images, apps, files and possibly anything else on the device. Computer extraction collects an entire copy of a computer's hard drive at a specific point in time.

**Recommendations:**

- **Scoping** – City Council should restrict the use of these extraction tools to only cases involving an event type flagged in the system as a violent and/or serious offense involving a non-property crime.
- **Coercion** – City Council should prohibit the use of these tools with consent without legal representation present, the next best would be to at least prevent such for minors.
- **Restricted use** – City Council should restrict the covert use of SPD's deployment of device extraction technology to cases that are serious and violent offenses, and must provide evidence of such in warrant applications for their use. The use of covert technologies, being major intrusions into privacy, must be proportional

to the seriousness of the suspected offense (UNODC, United Nations Office of Drug and Crime).

- **Remedies/Penalties** – City Council should state that the use of digital extraction device except pursuant to that defined in the final SIR exposes the user to criminal or civil liability.
- **Regulation and Transparency Report** – City Council should require that each use of such technology be registered with the city and compiled into monthly transparency report, accessible on the City's website, to include the following details: Make and Model of technology, reason for use (type of offense being investigated), length of use, the number of parties' and devices' data captured and/or searched; when the extraction(s) occurred and whether the extraction mechanism is/was ongoing or taken as a snapshot in time; whether the extraction(s) resulted in an arrest or conviction; whether those searches (by extraction device) were by consent (though consent searches should be banned), or through a warrant (and include warrant numbers associated with searches, if legal and applicable); whether the extraction(s) were related in any way with political protest, demonstration or other public assembly; whether the extraction data is/was shared with or uploaded to any other software program, entity, company, agency or person, outside of the SPD officer employing the technology, and, the name of such shared with.
- **Contractual** – City Council should request the Purchase orders and contracts for each of the extractive tool vendors SPD has used, is using, or plans to use in the future, and update the SIR to include this information.
- **Prohibition** – City Council should disallow the installation and use of spyware and/or key-logger-type functionality from any MDFT onto a suspect's device, and must instead rely on the process of judicially compelling the suspect to provide the passcode.
- **Prohibition** – City Council should disallow SPD from signing an NDA with any manufacturer, vendor, or reseller of a surveillance technology (as defined in the SSO). [Note that some other cities' CCOPS ordinances include prohibition of NDAs, but the SSO does not have that language.]
- **Process and Data Deletion** – City Council should:
  **a)** require that any information obtained through the execution of a warrant that is unrelated to the objective of the warrant (unless it is exculpatory information) be destroyed within thirty days after the information is seized and be not subject to further review, use or disclosure.
  **b)** City Council should require that any MDFTs used by SPD have detailed audit logs and automatic screen recording, so that judges, defenders & other involved parties would be able to obtain a better understanding of the "precise steps that law enforcement took when extracting and examining a phone."
  **c)** City Council should also require that if charges are dismissed or do not result in a conviction, all MDFT data is promptly deleted.

City of Seattle

# Email Comment

QUESTIONS
Is any data from these tools shared with Fusion Centers?

CONCERNS
SPD's consent-based use is often limitless.
Using coercion to obtain consent (e.g. as bargaining chip to avoid arrest).
Vast amounts of data (contacts/call logs/app files/passwords/deleted content/location data/etc).
Device owners not fully informed.
Disproportionate use of this technology.

RECOMMENDATIONS
Restrict use to violent offenses.
Require legal representation for all consent-based use (especially minors).
Require that use outside of what is in the SIR exposes user to criminal/civil liability.
Require that contracts governing these are public.
Prohibit installation of spyware/key-loggers.
Prohibit SPD from signing NDAs with any surveillance tech manufacturer.
Require monthly a transparency report that includes: tool make/model, offense, length of use, number of devices searched, time, whether ongoing, consent vs warrant, warrant numbers, where/who data was shared with, & whether extraction resulted in arrest/conviction.
Require detailed tool audit logs.
Require non-exculpatory data unrelated to the investigation be deleted in 30 days.
Require data deletion if charges dropped, not brought, or non-conviction.

# Email Comment

**Questions:**

- Is any of the data from device extraction tools shared or accessed by Fusion Centers? Does the Fusion Center access SPD data, and is a warrant?
- What are the names of the specific manufacturers and their individual product names of the computer, cellphone and mobile device extraction tools (physical tools and software) that SPD is using, has or plans to purchase, and used in the past?
- Is legal representation required in order for a person to give consent to the use of these tools on their device?

**Key Concerns:**

- Consent for SPD to use these tools may be coerced from low-level offenders, for instance as a bargaining chip to avoid detention or arrest, or as a threat.
- Note: Based on Upturn's PRA records from 2017-2019, the majority of SPD's consent-based searches were limitless, with no date or data type limitation; whereas only a quarter of all warrant-based searches were limitless (66% of consent-based searches were limitless compared to 24% of warrant-based searches).
- The SPD uses extractive tools that access ALL DATA on a device, scooping up many people's data from their electronic devices, including cell phones, smart phones, tablets, computers and other devices.

**Recommendations:**

- **Scoping** – City Council should restrict the use of these extraction tools to only cases involving an event type flagged in the system as a violent and/or serious offense involving a non-property crime.
- **Coercion** – City Council should prohibit the use of these tools with consent without legal representation present, the next best would be to at least prevent such for minors.
- **Restricted use** – City Council should restrict the covert use of SPD's deployment of device extraction technology to cases that are serious and violent offenses, and must provide evidence of such in warrant applications for their use. The use of covert technologies, being major intrusions into privacy, must be proportional to the seriousness of the suspected offense (UNODC, United Nations Office of Drug and Crime).
- **Prohibition** – City Council should disallow the installation and use of spyware and/or key-logger-type functionality from any MDFT onto a suspect's device, and must instead rely on the process of judicially compelling the suspect to provide the passcode.
- **Prohibition** – City Council should disallow SPD from signing an NDA with any manufacturer, vendor, or reseller of a surveillance technology (as defined in the SSO).

[Note that some other cities' CCOPS ordinances include prohibition of NDAs, but the SSO does not have that language.]

# Email Commment

QUESTIONS

Is any data from these tools shared with Fusion Centers?

CONCERNS

SPD's consent-based use is often limitless.

Using coercion to obtain consent (e.g. as bargaining chip to avoid arrest).

Vast amounts of data (contacts/call logs/app files/passwords/deleted content/location data/etc).

Device owners not fully informed.

Disproportionate use of this technology.

RECOMMENDATIONS

Restrict use to violent offenses.

Require legal representation for all consent-based use (especially minors).

Require that use outside of what is in the SIR exposes user to criminal/civil liability.

Require that contracts governing these are public.

Prohibit installation of spyware/key-loggers.

Prohibit SPD from signing NDAs with any surveillance tech manufacturer.

Require monthly a transparency report that includes: tool make/model, offense, length of use, number of devices searched, time, whether ongoing, consent vs warrant, warrant numbers, where/who data was shared with, & whether extraction resulted in arrest/conviction.

Require detailed tool audit logs.

Require non-exculpatory data unrelated to the investigation be deleted in 30 days.

Require data deletion if charges dropped, not brought, or non-conviction.