City of Seattle

2022 Surveillance Impact Report Executive Overview

Extraction Tools

Seattle Police Department

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

The purpose of this Executive Summary is to highlight policies, technology and practices regarding the surveillance technologies under Council review. This document outlines information, including policies and practices, about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. All information provided here is contained in the body of the full SIR document but is provided in a condensed format for easier access and consideration.

1.0 Purpose

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.

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.

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.

2.0 Data Collection and Use

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."

3.0 Data Minimization & Limitations

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

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.

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.

4.0 Access & Security

Access

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.

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.

Security

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.

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.

5.0 Data Sharing and Accuracy

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.

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.

6.0 Data Retention

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.