Seattle Office of Inspector General

Surveillance Technology Usage Review Computer, Cellphone, and Mobile Device Extraction Tools 2023

As Required by Seattle Municipal Code 14.18.060

December, 2024

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064

206.684.3663
oig@seattle.gov

Purpose

OIG's Charge Under the Surveillance Ordinance

Per Seattle Municipal Code 14.18.060, OIG is required to annually review the Seattle Police Department's (SPD) use of surveillance technology and the extent to which SPD is in compliance with the requirements of Chapter 14.18.

Table of Contents

Technology Description

CCMDE Tools: the collection of hardware and software tools that perform the extraction of digital information from devices.

Device: any computer, cellphone, or mobile device containing data that SPD extracts for a specific investigative purpose and pursuant to a consent agreement or a warrant.

Extract: the digital files extracted from a device.

Extraction: the process of using these tools and their associated software to capture data stored in a device.

Imaging: the reconstruction of extracted data from a device's hard drive so that officers can search for evidence in connection to the investigation.

Computer, Cellphone, and Mobile Device Extraction (CCMDE) Tools consist of both hardware and software that extract digital information and image the hard drives of devices after establishing consent or obtaining a search warrant. SPD purchased and licensed these tools from Cellebrite.

While there are many different brands and models of devices requiring different tools to extract data, CCMDE Tools work similarly to one another. To extract data from a device, that device is physically connected to either an SPD computer workstation with specialized, locally installed software or a stand-alone tool with extraction software installed on it. In both cases, the software bypasses, deciphers, or disables (depending on the brand and model of the target device) any password protection and extracts files. The stand-alone tool can save the extracted files to either a removable storage drive (e.g., a USB drive) or onto a computer workstation. Extracted files can then be accessed with software that reads and organizes the data into information packets for examination. As Section 2.3 in the SIR states: "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."

Reporting Limitation

The efficacy of CCMDE Tools, and the safety of those who use, them is highly dependent on confidentiality about the specific technology and the manner of use. To complete this assessment, SPD has provided all information and access deemed necessary by OIG for appropriate oversight. This report is intended to provide information necessary to demonstrate there is proper oversight of and knowledge about the use of these tools, while maintaining certain information as confidential, due to safety considerations.

SECTION A Frequency and Patterns of Use

SMC 14.18.060, § A: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

In 2023, SPD extracted data from 591 devices. About 80% of those extractions targeted mobile devices, including phones, tablets, external hard drives, or USB thumb drives, while about 20% targeted computers. Two units –the Technical & Electronic Support Unit (TESU) and Internet Crimes Against Children (ICAC) – own and operate CCMDE Tools. TESU shares their CCMDE Tools with a few task-force officers (TFOs) who assist in investigations with other law enforcement entities such as the Secret Service or the Federal Bureau of Investigations.

Extractions by Entity and Device Type, 2023

Entity Conducting Extraction	Mobile Device* Extractions	Computer Extractions	Total
TESU	234	0	234
TFOs	13	4	17
ICAC	229	111	340
Total	476	115	**591**

*Mobile Device here includes cellphones, external hard drives, USB thumb drives, tablets, and other hand-held devices.

Purpose of Use

Of 234 extractions, TESU performed 219 for the Investigations Unit, ten for Patrol, and five for an outside law enforcement agency. TESU personnel report that SPD may conduct an extraction on behalf of another law enforcement entity in the Puget Sound region if the investigation has elements pertaining to Seattle and if it is unclear where the case will be adjudicated (federal, state, or municipal court).

SPD's ICAC is the lead agency in the Washington State Internet Crimes Against Children Task Force. As the lead agency, personnel from SPD's ICAC may perform extractions for jurisdictions outside of Seattle once the other law enforcement agency provides the device(s) and proof of either a warrant or consent document. ICAC personnel reported that their extractions are generally ICAC-related crimes but a small number of may be homicide and human trafficking cases.

The following case summaries showcase the variety of cases where SPD personnel extracted data from mobile devices and computers. Consent agreements authorized the extractions for the first three cases while warrants authorized the last three cases.

Case Examples

Domestic Violence/Assault	A family member called 911 reporting a domestic violence/assault. The victim reported being assaulted, held at knifepoint and gunpoint, and threatened. During the investigation, SPD confiscated multiple firearms. The subject consented to cellphone extraction.
Robbery/Felony Warrant	Officers identified a passenger in a vehicle who matched a description of a warrant suspect. They conducted a traffic stop and placed the suspect into custody without incident. The driver permitted officers to search the vehicle, including a cellphone inside the vehicle.
Homicide/ Narcotics	A subject checked into a hospital covered in blood, claiming to have killed someone. Hospital staff had collected a hatchet and a case containing illicit substances. Officers mirandized the subject, who confirmed their understanding, volunteered a statement, and consented to a cellphone search.
Exploitation of a Minor	ICAC personnel performed an undercover operation to identify a potential felony sexual offense targeting minors. Once ICAC personnel collected enough evidence of potential exploitation of a minor, they obtained a search warrant, apprehended the subject, collected the cellphone, and extracted cellphone data.
Kidnapping, Imprisonment, and Robbery	Multiple victims reported being abducted, assaulted, threatened, held at gun point, and robbed. A warrant was issued for the subject. A month later, an officer detained the subject and confirmed the identity matched the warrant. Officers obtained an additional search warrant to extract data from the subject's cellphone.
Dealing in Depictions of a Minor Engaged in Sexually Explicit Conduct	ICAC personnel followed up on a cybertip they received. The cybertip included descriptions of sexually explicit images involving minors posted to social media by the subject. ICAC personnel established enough probable cause and evidence to obtain a search warrant for the subject's cellphone, mobile devices, and other electronic devices at the subject's residence.

SECTION B Data Sharing with External Partners and Other Entities

SMC 14.18.060, § B: How often surveillance technology or its data are being shared with other entities, including other governments in particular.

As outlined in Section 6.1 of the SIR, SPD may share data with various external agencies and entities within legal guidelines or as required by law.[1] However, OIG could not determine how often these data were shared and with whom, because there is not a centralized entity or staff member that manages data sharing of these video recordings. Both TESU and ICAC control their respective physical inventories of CCME Tools and oversee extractions. For TESU extractions, TESU personnel store them on an external disc drive and provide them directly to the case officer. TESU personnel do not retain copies of the extract; the case officer is the de facto custodian of the extract, and as data custodians, case officers are responsible for all data sharing. For ICAC extracts, ICAC personnel store extracts in a secure server with limited access. SPD Policy 7.010 requires that all evidence must be sent to the Evidence Unit (EU), but the EU does not track the origin of evidence submitted to them. As a result, OIG was not able to verify that physical discs containing extracts had been appropriately stored according to SPD policy.

OIG issued a recommendation in the Audio Recording Systems 2022 Annual Usage Review pertaining to the tracking of all instances of data sharing related to that technology. SPD concurred with that recommendation and estimated December 2024 to be the potential date of implementation. That recommendation should be extended to include Computer, Cellphone, and Mobile Device Extraction Tools as well. The recommendation excludes those parties immediately involved in the criminal justice process, as there are already processes in place to track those instances of data sharing.

Recommendation 1: Create a Tracking Process

SPD should develop a process for identifying and tracking all instances whenever extracts from Computer, Cellphone, and Mobile Device Extraction Tools are shared with external entities excluding those immediately involved in the criminal justice process associated with the case in which the data were collected.

1 Such as prosecuting attorney's offices, insurance companies, courts, federal and state law enforcement agencies, and members of the public can access their own information pursuant to a public records request.

SECTION C Data Management and Safeguarding of Individual Information

SMC 14.18.060, § C: How well data management protocols are safeguarding individual information.

Initial Certification and Continual Training Required

TESU and ICAC personnel reported that officers must receive certifications prior to the use of CCMDE Tools. TESU requires their authorized CCMDE users to attend a week-long, in person training conducted directly by Cellebrite, which concludes with an examination. After that, officers who completed the initial training and passed the initial examination must participate in re-training and a re-examination every two years. ICAC personnel also reported that, as the lead agency in a state-wide task force, they host the annual Northwest ICAC Conference. ICAC personnel are either Certified Forensic Computer Examiners or EnCase Certified Examiners.

Access Controls

Whenever not in use, ICAC secures their CCMDE Tools in a forensics lab, where only ICAC personnel and the lab manager have access.1 Items obtained by warrant or consent are first catalogued in the Evidence Unit before they are sent to ICAC's forensics lab for extraction. Once at the lab, data from the device are extracted, and the resulting extract is an imaged copy of the hard drive of the device. The lab analyzes the content, flags criminal evidence, and prepares a report. The imaged copy is stored in a secure server, administrated by the lab manager who provides detectives access to their unit-specific folder.

Whenever TESU personnel perform an extraction, it occurs within TESU's workspace, which is a sensitive compartmentalized information facility (SCIF). As a result, their extractions do not occur in the field. TESU uses a SCIF to ensure that only select TESU personnel have physical access to the devices and workstations.

Third Party Extractions

Personnel from both TESU and ICAC reported that none of their extractions attempted in 2023 were conducted by third party vendors. ICAC personnel reported that if their forensics lab cannot extract data from a device, then they could escalate to Cellebrite for advanced extraction services. Because devices escalated for advanced extraction services are physically shipped to and from Cellebrite and could be lost or damaged in transit, the vendor agreement states that – unless SPD indicates otherwise – Cellebrite will retain any extracted data for three months to ensure they can provide SPD the extracted data. If Cellebrite retains extracted data in this manner, the vendor agreement does not permit Cellebrite to use those data for any other purposes except to provide extraction services to SPD. These services

1 ICAC personnel reported that, generally, the mobile forensics lab van is present during a warrant service, thus the CCMDE tools are used on-scene to determine which device(s) contain contraband. The full extraction is later performed in their forensics lab at a secure SPD facility.

may have been used in prior years: a memorandum from the American Civil Liberties Union published in the SIR documents SPD's 2018 purchase of vouchers for advanced extraction services. However, personnel from ICAC and TESU reported that they did not use Cellebrite's advanced extraction services in 2023.

SECTION D Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations

SMC 14.18.060, § D: How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations (…).

Unauthorized extractions constitute the greatest civil liberties risk associated with CCMDE Tools. Section 3.2 of the SIR states that SPD may use data extraction devices only after legal standards of consent or court-issued warrant have been met.1 Personnel who use CCMDE Tools reported that warrants authorized about 93% of extractions performed in 2023, and consent agreements authorized the remaining 7% of extractions. OIG conducted a qualitative review of 26 cases involving device extractions and found all met the requirements stated in the SIR: warrants authorized use in 21 cases while the remaining five cases involved consent agreements.

TESU personnel explained that varied circumstances may result in a consent-based extraction. For example, a victim, a deceased victim's next-of-kin, a witness, or a suspect.2 Similarly, ICAC personnel reported that their ten consent cases were from human trafficking victims collaborating with SPD. ICAC personnel explained that consent-based extractions occur with adults, generally sexual assault victims. They also reported that a small number of other specialized investigative units (e.g., the Homicide and Assault Unit) may request ICAC's forensics lab to perform an extraction following a consent agreement with a victim.

Entity Performing Extraction	Number of Extractions Authorized by Warrant	Number of Extractions Authorized by Consent
TESU	207	27
TFOs	15	2
ICAC	330	10
Total	552	39

1 In the event that SPD escalates an extraction to Cellebrite, the vendor agreement requires SPD to provide evidence that SPD has obtained necessary authorization required to permit Cellebrite to perform an advanced extraction.

2 According to TESU personnel, these extracts contain evidence of the incident or have investigative significance. In the case of an SMS text-based conversation, for example, raw extracted data are more reliable in prosecutions than screenshots of the same conversation.

SECTION E — Complaints, Concerns and Other Assessments

SMC 14.18.060, § E: A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance.

Office of Police Accountability Complaints

No relevant complaints pertaining to this surveillance technology were cited in OPA complaints filed in 2023.

Customer Service Board Comments

No relevant comments pertaining to this surveillance technology were cited in Customer Service Board comments posted in 2023.

Internal Audits/Assessments

No internal audits or assessments of this surveillance technology were conducted in 2023.

SECTION F — Total Annual Costs

SMC 14.18.060, § F: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

ICAC estimates about $120,000 in annual costs from 2023 associated with their use of CCMDE Tools. They reported that most of this amount is for licensing.

According to TESU personnel, costs incurred for CCMDE Tools follow multi-year cycles, depending on contract lengths. TESU personnel provided the contract amounts for all forensic-related purchases from 2023. Therefore, OIG estimates $10,834.84 in total costs for licensing and maintenance.[5] Personnel costs associated with use are not possible to determine since SPD does not separately track this activity in time increments.

5 These costs include replacement materials, and evidence-grade hard drives, DVDs, and CD-Rs.

APPENDIX A: Management Response

1. SPD should develop a process for identifying and tracking all instances where data from Computer, Cellphone, and Mobile Device Extraction Tools are shared with external entities excluding those immediately involved in the criminal justice process associated with the case in which the data were collected.

SPD Management Response

● Concur ○ Do Not Concur

Estimated Date of Implementation: Q1 2025

Proposed Implementation Plan: SPD's TESU will implement unit procedures to document any such data sharing as a supplemental to the master case file in Mark43. Additionally, SPD's Legal Unit will track any such request made through either public disclosure or a subpoena duces tecum in any case unrelated to the case in which the data were collected.

Non-Audit Statement This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.