Seattle Office of Inspector General

# Surveillance Technology Usage Review Crash Data Retrieval 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.

## Crash Data Retrieval Tools No Longer A Surveillance Technology

At the time of publication, this technology has been re-classified and no longer implicates SMC 14.18. As a result, this will be the final report on this technology and does not issue recommendations. The Seattle Office of Inspector General thanks Seattle Police Department for their collaboration in examining the use of this technology.

# Table of Contents

## Technology Description

**Crash Data Retrieval Tools:** analyze vehicle data seconds before and after a serious traffic collision.

Crash Data Retrieval (CDR) are forensic tools that analyze vehicle data and reconstruct the series of events seconds before and after a serious traffic collision. CDR tools rely on Event Data Recorders (EDRs) and/or other On-Board Diagnostics (OBDs) systems, which are standard components in most vehicles manufactured in the United States. CDR tools consist of both hardware and software components. The physical tools interface with vehicles' EDR or OBD ports and download stored technical data about the vehicle in a format that can only be opened by specialized CDR software. Once data are extracted, the CDR tool interfaces with a computer and the corresponding proprietary software translates those data into a CDR report.

**TCIS: Traffic Collision Investigation Squad:** the sole users of CDR Tools.

**ACMs:** Airbag Control Modules record vehicle safety systems and basic operations.

Personnel from the Traffic Collision Investigation Squad (TCIS) report that they have one CDR toolkit and one departmental computer with Robert Bosch LLC CDR software installed. TCIS personnel also report that five TCIS detectives share the toolkit and the computer. The TCIS CDR toolkit can only access Airbag Control Modules (ACMs), which measures vehicle restraint safety systems like airbags and seatbelts as well as sensor detections, pre-crash vehicle speed, the status of the braking system, throttle position, and steering input. TCIS personnel are only able to use their CDR toolkit given the following conditions:

1. Compatibility: the vehicle's ACM is compatible with the CDR toolkit; and,
2. Authorization: a warrant or consent document authorizes extraction. Alternatively, if the sole owner of a vehicle dies in a collision, neither a warrant nor a consent document is necessary to extract ACM data.

## 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.

### CDR Toolkit Use Conforms to SIR

The SIR states that TCIS personnel use the toolkit in "specific circumstances such as the death of any person, life-threatening injuries, hit and run collisions, collisions involving substantial bodily injury […] vehicular homicide, felony eluding, felony DUI, and other vehicular crimes."1 This review found that TCIS detectives used their CDR toolkit according to this policy. In 2023, they analyzed seventeen collisions.2 Fatalities occurred in ten of those seventeen cases, and the remaining seven cases involved life-threatening injuries. Pedestrians were fatal victims in four cases.

During the acquisition process for this technology, members of the community raised concerns about the extraction of records from Bluetooth-connected mobile devices (such as call records and cellphone contacts). In addressing this concern, TCIS personnel informed OIG that their CDR toolkit extracts data solely from Airbag Control Modules (ACMs) and cannot access data from Bluetooth-connected mobile devices. OIG reviewed all case files related to CDR uses in 2023 and confirmed that the TCIS CDR toolkit only accessed the technical data stored in vehicle's ACM.

### Cases Involving Crash Data Retrieval Tools by Precinct, 2023

| Precinct | Number of Uses |
|---|---|
| South | 6 |
| West | 5* |
| North | 3 |
| Southwest | 2 |
| East | 0 |
| Outside of Jurisdiction | 1** |
| **Total** | **17** |

* Indicates that one of the West Precinct uses was to investigate a fatal collision involving an SPD vehicle and a pedestrian; all other uses analyzed collisions involving only civilians.

**In another case, TCIS personnel assisted in the extracting ACM data in an outside jurisdiction. In that case, Port Authority requested mutual aid assistance for a collision that occurred at SeaTac Airport.

1 Furthermore, paragraph 6 of SPD Policy 15.260 – Collision Investigations, establishes that TCIS responds to certain collisions involving "death or injury likely to cause death; collisions where there is probable cause for vehicular homicide, vehicular assault, or hit-and-run investigations with serious bodily injury; collision during a police pursuit that results in serious injuries to any party; [and] collisions involving City equipment with serious bodily injury."

2 Not all investigations of fatal collisions involve the ACM extraction, because only some vehicles' ACMs are compatible with the TCIS CDR toolkit. Washington State Traffic Safety Commission recorded 28 fatal vehicle collisions in Seattle in 2023, and TCIS investigated ten of those cases using their CDR toolkit. Use patterns, as a result, reflect those instances where at least one involved vehicle is compatible with the TCIS CDR toolkit and where extraction followed a warrant, consent agreement, or driver fatality as described in the Technology Description.

## 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.

Data analyzed from the use of the CDR toolkit may be shared externally with other law enforcement. As stated in Section 6.1 of the SIR:

> "discrete pieces of data collected by the CDR tools 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."

TCIS personnel report that extracts of ACM data are rarely, if ever, shared with external entities. Conclusions based on the information and analysis from the CDR reports, however, may be shared with the following entities:

- 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

3 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.

4 TESU controls the physical inventory of Camera Systems, oversees the extraction of recordings from wires after use, and assists in exporting recordings from fixed location cameras. Once recordings are extracted or exported, TESU stores those recordings on external disc drives and provides them directly to the case officer. For wires, TESU personnel then purge the recordings and overwrite the files on the wire multiple times to ensure complete deletion. TESU personnel do not retain copies of video files from either Camera System type; the case officer is the de facto custodian of recordings once they receive the original copy by disk or disc. As data custodians, case officers are responsible for all data sharing.

5 That report can be accessed here: **https://www.seattle.gov/documents/Departments/OIG/Audits/SurveillanceTechnologyUsageReview-AudioRecordingSystems%282022%29.pdf**

## SECTION C Data Management and Safeguarding of Individual Information

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

### Physical Storage Conforms to SIR

Section 4.10 of the SIR states that "this equipment is physically housed inside locked SPD facilities. The CDR software is locally installed on select SPD workstations [sic.] in the TCIS Unit."[1] TCIS personnel confirmed that their CDR toolkit and computer containing the Bosch CDR software are locked in a TCIS office whenever not in use.

### Data Security

TCIS personnel store CDR extracts and reports in SPD's digital evidence management system (DEMS), where they are accessible to SPD staff. CDR extracts are stored in their native filetype, which requires specialized software to translate. The DEMS records logs of all views and downloads of its stored files.

### Training Requirements Outlined in the SIR Do Not Align with Current Practice

Section 3.3 of the SIR states, "there is a 16+ System Operators Course required prior to use of the Crash Data Retrieval (CDT) tools and then annual training on analysis and updates of the data." According to TCIS personnel, all five detectives who use the CDR toolkit have completed the CDR Technician training, and four of the five detectives have also completed CDR Analyst training. However, TCIS personnel have not attended annual training since 2013 due to costs and staffing limitations.

## 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 (…).

### Use Governance Conforms to SIR

Section 3.1 of the SIR states that these tools "are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapter 9.73 RCW." A review of the digital evidence and the records management systems showed that in eight of the 17 use cases from 2023, detectives uploaded warrants, consent documents, or noted the death of a driver/vehicle owner. In the remaining nine use cases – all of which were active during the report writing period – the lead detective for each case confirmed with OIG their use followed one of these three legal standards prior to extracting ACM data.

1 Section 4.10 of the SIR erroneously reports that the CDR software is installed on select workstations; however, TCIS personnel report they have only one dedicated computer.

## 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.

OIG estimated $5.083.13 in licensing costs associated with this technology. Personnel costs associated with use are not possible to determine since SPD does not separately track this activity in time increments.

## APPENDIX A: Management Response

SPD provided that it has no substantive response to this review as no matters requiring a response are raised, but SPD appreciates the opportunity to review.

**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.