City of Seattle

## 2022 Surveillance Impact Report Executive Overview

# Crash Data Retrieval 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

Crash Data Retrieval (CDR) tools are important technology used to aid investigators in the reconstruction of traffic collisions. Nearly all passenger vehicles (cars, light trucks, SUVs, etc.) sold in the US since 2013 has an onboard Event Data Recorder (EDR) which automatically records important technical information during a critical event such as a collision. These EDR units only record information when certain events such as when airbags deploy or when sensors detect a collision and do not have interfaces which display the information.

The Crash Data Retrieval (CDR) tools used by SPD consist of hardware and software components. The hardware interface modules and associated cables and adapters are vehicle make and model dependent and connect either to a vehicle's on-board diagnostics port or directly to the module containing the EDR. These hardware interface modules connect to a computer workstation running the CDR vendor software which translates the raw EDR data into a PDF format readable report.

# 2.0 Data Collection and Use

CDR tools collect information stored in vehicle EDR units. These tools are utilized only after legal standards of consent and/or court-issued warrant have been met in the investigation of a traffic collision.

# 3.0 Data Minimization & Limitations

The Traffic Collision Investigation Squad (TCIS) is a detective unit responsible for scene response and investigative follow-up for collisions involving vehicles, bicycles, pedestrians, boats, trains, light rail vehicles, and aircraft. Only TCIS sworn investigators utilize the Crash Data Retrieval (CDR) tools. TCIS investigates collisions involving specific circumstances such as the death of any person, life-threatening injuries, hit and run collisions, collisions involving substantial bodily injury where it appears a driver was negligent or under the influence of alcohol and or other drugs, vehicular homicide, felony eluding, felony DUI, and other vehicular crimes. The Crash

Data Retrieval (CDR) tools are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.

The Crash Data Retrieval (CDR) tools are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.

# 4.0 Access & Security

## Access

Supervisors and commanding officers are responsible for ensuring compliance with policies.

There is a 16+ hour System Operators Course required prior to use of the Crash Data Retrieval (CDR) tools and then annual training on analysis and updates of the data.

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 TCIS sworn investigators utilize the Crash Data Retrieval (CDR) tools, and then only once appropriate consent and/or a court issued warrant has been obtained. The CDR tools used by SPD consist of hardware and software components. The hardware interface modules and associated cables and adapters are vehicle make and model dependent and physically connect either to a vehicle's on-board diagnostics port or directly to the module containing the EDR. These hardware interface modules connect to a computer workstation running the CDR vendor software which translates the raw EDR data into a PDF format readable report.

The PDF reports created by the CDR software are uploaded into the Evidence.com evidence system.

### Security

The PDF reports created by the CDR software are uploaded into the Evidence.com evidence system.

These records are available to any auditor, including the Office of Inspector General and federal monitor.

## 5.0 Data Sharing and Accuracy

SPD has no data sharing partners for the CDR tools or reports. No person, outside of SPD, has direct access to the devices or software.

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 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. 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.

The scope of CDR tools usage authorization is outlined in consent and court-ordered warrants. Any data that is collected outside the established scope is purged by the investigating detective.

SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense Report. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation.

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 secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's 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.

# 6.0 Data Retention

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

The Traffic Collision Investigation Squad (TCIS) is a detective unit responsible for the CDR tools.

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.

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.