City of Seattle

~~2024~~ 2025 Surveillance Impact Report Executive Overview

Real-Time Crime Center

Seattle Police Department

Overview

This Executive Overview documents information about the collection, use, sharing, security, and access controls for data that is gathered through Seattle Police Department's (SPD) Real-Time Crime Center (RTCC). All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

Real-Time Crime Center (RTCC) software provides a centralized location for real-time information and analysis. At its core, RTCC software integrates dispatch, cameras (such as CCTV and traffic monitoring cameras), officer location, 911 calls, records management systems, and other information into one "pane of glass" (a single view). The software is used to alert RTCC staff to a serious criminal event, see multiple streams of information overlaid on a map view, and convey information to officers responding in the field.

2.0 Purpose

The purpose of RTCC software is to provide situational awareness to increase officer and citizen safety, and reactively investigate incidents. Having real-time, accurate information in one place helps increase reliability regarding the location of victims and suspects – enabling quicker aide and safer apprehension. Having better visual and spatial suspect information will help reduce unnecessary stops by officers, focusing their efforts on verified locations and accurate descriptions.

3.0 Data Collection and Use

The RTCC software integrates data from other SPD systems into a centralized location for real-time information and analysis. Data feeding into RTCC could come from dispatch, CCTVs, SDOT traffic monitoring cameras, officer location, 911 calls, records management systems (RMS), ALPR, geographic information systems (GIS), and other information systems. Information from some of these systems may be stored in storage related to the RTCC software to provide a comprehensive record of an incident. Storage of information not used for investigations or law-enforcement uses would be for 30 days maximum.

SDOT traffic monitoring cameras (as referenced in the "Closed Circuit Television 'Traffic Cameras' (Transportation)" SIR) will be utilized in the RTCC software for law enforcement purposes.

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

4.0 Data Minimization & Retention

The RTCC software is used to integrate data from various sources used by SPD into one place, a single view. All data sources have their own pre-existing controls in place to minimize inadvertent or improper collection, as outlined in previous surveillance impact reports for the relevant technology.

The RTCC software itself will store some of the data from the integrated systems to provide a comprehensive picture of an incident. Data that is not part of a criminal investigation will be subject to a 30-day retention

policy, after which it will be purged from the system.

5.0 Access & Security

Access

Only authorized SPD, OPA, and OIG users can access the RTCC software platform. Access to the systems/technology is limited to authorized personnel via password-protected login credentials.

Data extracted from the system/technology and entered into investigative files is securely inputted and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

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.

All use of the RTCC will be for legitimate law enforcement purposes only. Personal or inappropriate use or dissemination of information can result in internal discipline, termination, and penalties under federal or state law.

Security

Any incident or multimedia data extracted from the system will be stored in a method compliant with the FBI's CJIS requirements. The specific details are vendor dependent, but could include either cloud storage or on-premise storage. The storage configuration may vary from vendor to vendor, but SPD expects similar industry standards when it comes to cloud storage and access controls.

Retention period for data stored in RTCC software storage will be 30 days, data will be overwritten after that retention period expires. Data associated with criminal investigations will get saved as evidence in SPD's digital evidence locker consistent with retention guidelines for evidence.

Audits from the OIG or other official auditors will be allowed as needed.

6.0 Data Sharing and Accuracy

Data obtained from the technology 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.

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 RTCC software 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 provided by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the devices.

7.0 Equity Concerns

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 Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior and other accountability measures. This pilot will be data-informed and guided. It will terminate if data suggests the technology is ineffective. Utilizing the abilities of the Performance Analytics and Research Unit, the Seattle Police Department has a plan to actively manage performance measures reflecting the "total cost of ownership of public safety," Equity, Accountability, and Quality ("EAQ"), which includes measures of disparate impact and over policing. In addition to a robust *Continuous Intervention Assessment* designed to inform, in real-time, the active development of a safer and more effective, Evidence-Based Policing (EBP) competency, the EAQ program assures *just right* policing is achieved with undue collateral harm.

It's worth noting that many factors can contribute to disparate impacts in policing, most of which occur early in a person's life, long before there is engagement with the police. For example, systems and policies that perpetuate poverty, the failure to provide children with the strong and fair start they deserve in the crucial birth-to-five years, inadequate public education, and a lack of economic opportunity can all contribute to disparate outcomes. In addition, family dynamics and peer pressure can also create negative outcomes. We recognize these factors and strive to do our part to mitigate them, but we can't expect our police officers by themselves to cure these contributory factors. However, we do expect our officers to do their jobs respectfully and fairly as they interact with community members.

These technologies are location-specific, with a place-based focus, meaning they will record people who choose to be in a public place where the technologies are being used. This mitigating factor reduces, to an extent, the possible disparate impact of potential police actions.