



Seattle Office of Inspector General

Surveillance Technology Usage Review: Coplogic (2021)

As Required by Seattle Municipal Code 14.18.060

April 28, 2023

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064
oig@seattle.gov
(206) 684-3663

Foreword from the Inspector General

Enclosed is OIG's first Annual Surveillance Usage Review on the use of Coplogic by the Seattle Police Department (SPD). This review was performed pursuant to Seattle Municipal Code 14.18.060, which specifies that OIG conduct annual reviews of SPD's use of Surveillance Technologies. Coplogic is one of sixteen SPD Surveillance Technologies currently approved by City Council.

OIG contracted with cybersecurity firm Critical Insight to conduct this review, and we thank them for their work, as well as their ongoing partnership in overseeing SPD's use of approved Surveillance Technologies.

Throughout this process, OIG directed and reviewed the work of Critical Insight. OIG also facilitated stakeholder feedback from SPD, the American Civil Liberties Union, and City Council staff. We appreciate the time and effort these stakeholders devoted to this review. These consultations and perspectives helped to ensure the work was thorough and inclusive, and that our conclusions and recommendations are based on the most complete information available.

In performing this review annually, OIG will continue to engage with SPD and other stakeholders to ensure responsiveness to community concerns and innovate in the area of evaluating how SPD uses Surveillance Technologies to further public safety while protecting the rights of individuals in our community.



Critical Insight

CITY OF SEATTLE SURVEILLANCE TECHNOLOGY REVIEW LEXISNEXIS COPLOGIC

SOW-2022-271

APRIL 28, 2023

Notice

Critical Insight has made every reasonable attempt to ensure that the information contained within this statement of work is correct, current and properly sets forth the requirements as have been determined to date. The parties acknowledge and agree that the other party assumes no responsibility for errors that may be contained in or for misinterpretations that readers may infer from this document.

Trademark Notice

2023 Critical Insight, Inc. dba CI Security. All Rights Reserved, CI Security®, Critical Insight™, the Critical Insight and Kraken logos and other trademarks, service marks, and designs are registered or unregistered trademarks of Critical Insight in the United States and in foreign countries.



© Copyright 2023 Critical Insight, Inc.



Table of Contents



Summary of Assessments and Recommendations Related to SMC 14.18.060	4
<i>Technology Description</i>	7
<i>Purpose and Objectives</i>	7
<i>A. Surveillance Technology Usage</i>	10
Retail Track Usage	12
Purpose Of Use	15
False Reporting	15
<i>B. Data Sharing with External Partners and Other Entities</i>	17
<i>C. Data Management and Safeguarding of Individual Information</i>	18
Contract with LexisNexis.....	18
Data Retention.....	20
Safeguarding of Individual Information	20
<i>D. Impact on Civil Liberties and Disproportionate Effects on Disadvantaged Populations</i>	22
Retail Track Bias	22
Accessibility of Coplogic.....	23
<i>E. Complaints and Concerns Received</i>	24
Office of Police Accountability (OPA) Complaints	24
Customer Service Bureau Complaints.....	24
Internal Audits or Assessments.....	24
<i>F. Costs</i>	24
<i>G. Feasibility of Locating the Coplogic Application on a City Server</i>	25

This Executive Summary highlights our major findings and recommendations pertaining to the six elements of SMC 14.18.060, which structures OIG’s review. The summary below lists our significant audit results associated with SMC 14.18.060.

Summary of Assessments and Recommendations Related to SMC 14.18.060

14.18.060 Provision	Compliance Determination	Auditor’s Findings	Recommendations
<p>A. How surveillance technology has been used, usage frequency, and whether usage patterns have changed.</p>	<p>Needs Work</p> 	<p>Of the estimated 23,040 reports taken via Coplogic in 2021, 22,929 of these were received from the individual track, and 111 were received from the retail track.</p> <p>Utilization of the retail track appears very low in 2021 data, with 6 different businesses in 14 locations submitting reports via the retail track.</p> <p>Submissions through the retail track reflect a lack of firm criteria to govern how or when suspects are detained and identified. Some retailers appear to compile a collection of offenses for a suspect before submitting to SPD.</p>	<p>Recommendation 1 SPD should work with Seattle IT and applicable vendors to modify Coplogic and Mark43 integration so that retail and individual track reports in Coplogic are identified as such after import into Mark43</p> <p>Recommendation 2 SPD should update policy 15.200 and/or other applicable guidance to establish criteria for submissions through Coplogic or any equivalent submissions system under the Retail Theft Program, giving specific consideration to:</p> <ul style="list-style-type: none"> a) The minimum PII necessary to establish a suspect’s identity b) Specific methods a retailer identifies suspects c) How soon an incident should be reported d) When a suspect should be detained
<p>B. How often surveillance technology or its data is shared with other entities, including government agencies.</p>	<p>Yes</p> 	<p>External sharing of reports originating from Coplogic appear to conform to processes described in the SIR. However we were unable to identify all reports shared through public records requests.</p>	

14.18.060 Provision	Compliance Determination	Auditor's Findings	Recommendations
<p>C. How well data management protocols are safeguarding individual (personal) information.</p>	<p>Needs Work</p> 	<p>The City's contract with Lexis Nexis for use of Coplogic appears to have sufficient language to prohibit the use of PII for other purposes. Further, data retention controls within the Coplogic system appear to be functioning as described in the SIR.</p> <p>Neither Seattle IT nor SPD are conducting regular access audits of either Coplogic or the Mark43 Records Management System (RMS) which stores reports accepted from Coplogic. Access to these systems is not monitored to detect patterns of access that could indicate account compromise or unauthorized sharing of accounts.</p>	<p>Recommendation 3</p> <p>SPD should work with Seattle IT and LexisNexis to formalize that Coplogic records will be deleted from LexisNexis servers after 120 days.</p> <p>No recommendation made at this time, as the policies and processes related to system access are broader than the scope of this technology review. OIG will continue to monitor this concern, and explore potential follow-up work to address the systemwide concerns</p>
<p>D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated.</p>	<p>Needs work</p> 	<p>At this time there is no evidence of disproportionality on the basis of race within the retail track of Coplogic, but limitations in data reliability exist and analysis should be repeated in future years.</p> <p>The Coplogic web and mobile applications are only available in English. There are no localizations available for non-English languages.</p> <p>Coplogic is not fully compatible with screen-readers and may be inaccessible for blind users</p>	<p>Recommendation 4</p> <p>SPD should work with Seattle IT and LexisNexis implement localizations for the major language groups used in the Seattle metro area for the Coplogic web and mobile applications</p> <p>Recommendation 5</p> <p>SPD should work with Seattle IT and LexisNexis to ensure Coplogic web and mobile applications are fully compatible with screen-reader devices and applications used as accessibility aids by blind users</p>

14.18.060 Provision	Compliance Determination	Auditor's Findings	Recommendations
E. A summary of any complaints or concerns about the surveillance technology and results of internal audits or assessments of code compliance.	<p style="text-align: center;">Yes</p> <div style="text-align: center;">  </div>	No relevant complaints about LexisNexis Coplogic were received by OPA or the CSB in 2021.	
F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.	<p style="text-align: center;">Yes</p> <div style="text-align: center;">  </div>	See Section F for cost breakdown.	
G. Feasibility of Locating the Coplogic Application on a City Server application on-premises	<p style="text-align: center;">N/A</p>	LexisNexis Coplogic exists only as a "Software as a Service" (SAAS) application and cannot be moved to an on-premises server.	

Technology Description

LexisNexis Coplogic is a crime reporting software tool that allows members of the public to submit police reports online through a web-based interface. Coplogic is a Software-as-a-Service (SaaS) application available for web and mobile devices, and the system is created and maintained by LexisNexis. SPD utilizes this technology in two ways:

- 1) As an online public interface, referred to as the “individual track” within Coplogic, allowing individuals to report a low-level, non-emergency crime in which no known or describable suspect is available, and for which individuals may need proof of police reporting (i.e., for insurance purposes), without waiting for an officer to dispatch and take a report;
- 2) As an online password-protected interface, referred to as the “retail track” of Coplogic, allowing retailers to enter information about retail theft on their property in which a suspect is known and suspect information is available.

Purpose and Objectives

The purpose of this review is to document the findings of an analysis of the Surveillance Impact Report (SIR) and associated departmental policies and processes for the LexisNexis Desk Officer Reporting System, also known as Coplogic. This analysis was conducted by Critical Insight consultants at the request of the Office of the Inspector General for Public Safety at the City of Seattle under City Ordinance 125376, under Chapter 14.18.060, which requires an annual review of actual usage of surveillance technologies by the Seattle Police Department (SPD). This review is required to include, but is not limited to, the following:

- A. How surveillance technology has been used, how frequently, and whether usage patterns are changing over time;
- B. How often surveillance technology or its data are being shared with other entities, including other governments in particular;
- C. How well data management protocols are safeguarding individual information;
- D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated, including, for SPD, an

examination of whether deployments are pursuant to warrants or not and how SPD's surveillance technology is used to analyze patterns to predict suspect, individual, or group-affiliation behavior;

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; and

F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.

For LexisNexis Coplogic, the City Council also requested that the Office of the Inspector General for Public Safety include an analysis of the costs and benefits of hosting the LexisNexis Coplogic application on a City-owned server that operates on City premises. This analysis can be found in Section G of this report.

In the course of this review, consultants reviewed both the information disclosed in the SIR, Seattle Police Department policy relating to accepting reports and evidence from the public, records retention, data destruction, and other areas. This review also includes a survey of concerns raised by the Privacy and Civil Liberties Assessment and Public Comment sections of the SIR. Consultants interviewed personnel from SPD and the City of Seattle's IT Department and reviewed relevant contracts and vendor agreements.

This report will highlight risks discovered by Critical Insight consultants in the areas above, and give recommendations on how to remediate additional risks identified in this review, with attention to the following areas, which are also called out in the relevant Surveillance Impact Report (SIR) for that technology:

- Is the description of the technology in the SIR complete and accurate?
- Are there a clear usage and data management policies in place?
- Do policies delineate how and when the surveillance technology will be deployed, and by whom?
- How and where will data gathered by this surveillance technology be stored?
- How long will data be retained?
 - What process is used to destroy data that are no longer retained?
- How is access to data secured?
 - How is unauthorized access prevented?

- What access reviews are being performed?
- How are data shared outside of the department, and how is sharing or access to that data monitored and audited?
- Are there any auditability concerns about the technology, its cost and its usage in general?
 - Example: Instances where access authorization cannot be reviewed because log data is not available
 - Example: Instances of the use of a particular surveillance technology not being tagged properly in case notes.

A. Surveillance Technology Usage

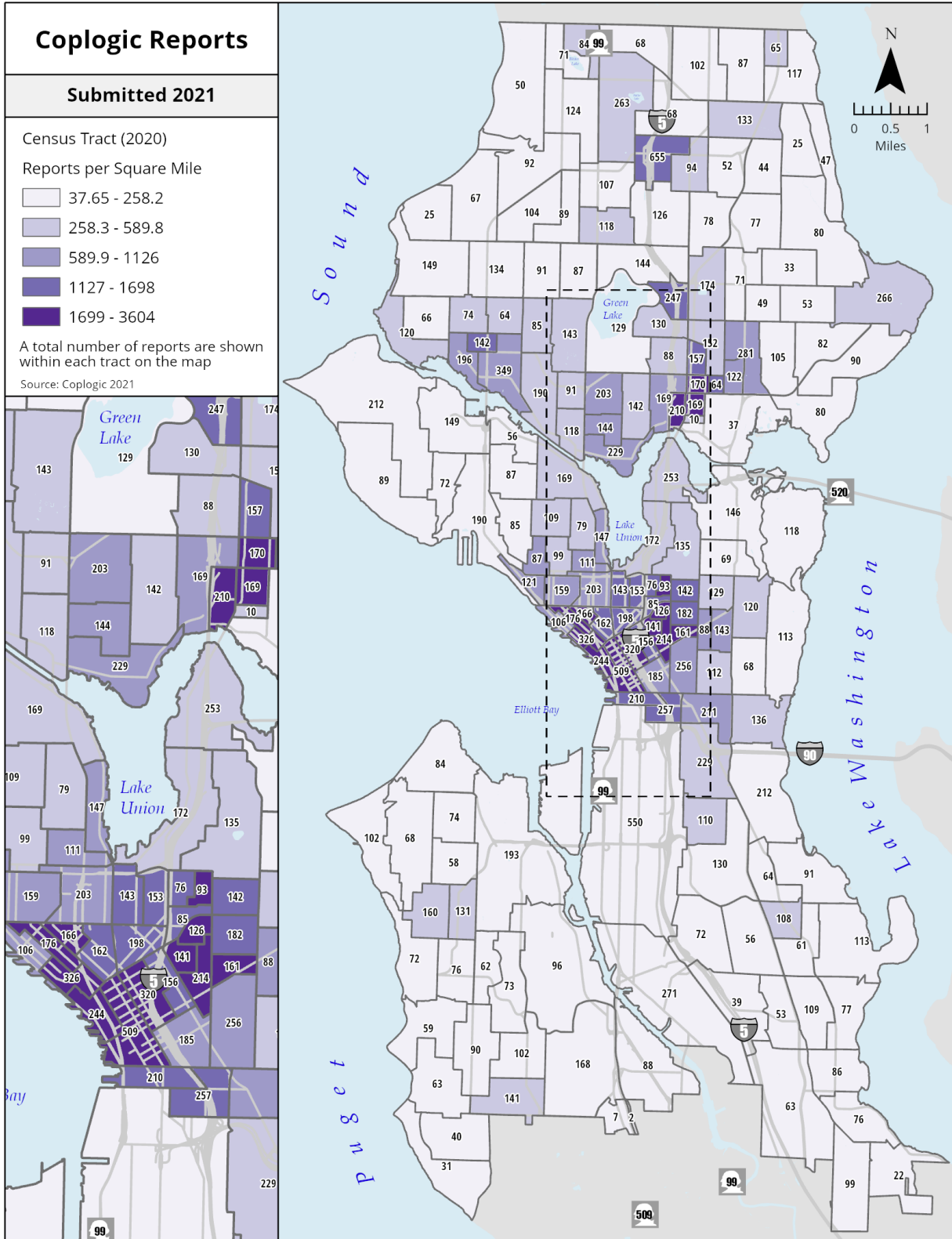
This assessment includes usage data available in the Mark43 Records Management System (RMS) on reports filed via Coplogic during 2021. Data from Mark43 were used because all reports taken via Coplogic are deleted from the Coplogic platform within 120 days, rendering the original dataset no longer available. Review of the usage of this technology was thus confined solely to the reports that were accepted and approved during calendar year 2021.

The following page contains a “heat map” of the greater Seattle area, along with a detailed view of the downtown core. This map shows the number of reports taken from both the retail and individual tracks of Coplogic in each census tract in the city during calendar year 2021. This map was prepared by the City of Seattle’s Geographic Information Services (GIS) team based on data gathered for this review—we thank them for their assistance.

Each tract is numbered to indicate the number of reports received from that tract during 2021, and each tract is also assigned a color gradient that represents the number of reports received per square mile within that tract. Deeper colors represent a higher density of reports, as indicated by the legend at left.

SPD accepted 23,040 original reports via Coplogic during calendar year 2021.¹

¹Mark43 can be searched for the date an event occurred, not when a report was submitted. To address this, reports that occurred in 2020 but were not submitted until 2021 are included in this review. Any events that occurred prior to 2020 that were reported in 2021, were not included.



Retail Track Usage

Critical Insight found that available data in Mark43 did not support a clear differentiation of reports originating from either the retail or individual tracks of Coplogic. Once Coplogic reports are imported into Mark43, they do not retain a datapoint that can be used for filtering by track provenance. Absent a clear datapoint, we instead identified a population by searching for reports approved by the SPD detective who manages the Retail Theft Program. SPD personnel agreed this would be the most reliable method of identifying the population of retail track reports.

Recommendation 1: SPD should work with Seattle IT and applicable vendors to modify Coplogic and Mark43 integration so that retail and individual track reports in Coplogic are identified as such after import into Mark43

Provided the data limitations explained above, we found that SPD accepted 111 reports through the retail track in 2021. The SPD detective managing Retail Theft Program identified that this number may be artificially low because within the review period, some retailers submitted reports through the individual track.² The detective also informed us that SPD is no longer accepting retail reports submitted through the individual track. However, this process change is not reflected in the 2021 data. For 2021, only 6 different businesses across 14 addresses within the city appear to have submitted reports through the retail track:

- 4 nationwide big-box retail department stores with multiple locations in Seattle
- 1 local grocery store
- 1 bar/nightclub

33% of these 111 reports were randomly selected for a closer review of the written narrative, evidence uploaded to each case, and the amount of personally identifying information (PII) uploaded in each report. We found that:

- All sampled reports pertained to stolen property, typically shoplifting.
- The majority of sampled reports involved repeat offenders.
- In each case where video evidence was provided, it was provided by the retailer on a physical DVD, not via upload to the Coplogic platform. SPD retains these data on physical DVD indefinitely.

² We note that a perjury attestation is required for submission through the retail track.

Along with the observations above, the following are concerns related to observed use of the retail track:

Detainment and Identification of Suspects

The Coplogic SIR section 3.2 details the legal standards or conditions, in any, that must be met before the technology is used. It states that:

Retailers may use CopLogic to report a retail theft on their property when:

- 1) The retailer participates in SPD's Retail Theft Program and has obtained a unique login identifier and password;*
- 2) They have detained the suspect;*
- 3) The suspect does not have any outstanding warrants; and*
- 4) They verify the identification of the suspect and upload copies of the suspect's identification, if available.*

Further, SPD's public-facing Retail Theft Program page identifies that RTP participants "will do" the following, among other requirements;³

- *Detain the suspected shoplifter per store policies/procedures.*
- *Obtain or attempt to identify the subject.*

Although detaining suspects is a requirement stated in both the SIR and on the Retail Theft Program webpage, our review found that suspects were frequently not detained by store personnel. Among the reviewed cases, no retailers appear to have uploaded copies of the suspects' identification. When a suspect was not detained, reports typically contained the name of the suspect, a summary of the incident, and a photo of them within or leaving the store. Photos provided as evidence typically showed suspects using heavy, concealing clothing with combinations of masks, hoods, hats, and sunglasses to conceal their features.

Retailers often do not articulate how they identified a suspect, and frequently only state that the suspect is "known to the store." Some reports mentioned that suspects were identifiable because of their body language or consistent use of the same *modus operandi*. A small number of sampled reports did contain photos of individuals with their faces clearly shown. SPD reports that in cases where the suspect's identity is still in doubt, the Detective reviewing the report will search the suspect's name in Washington Crime Information Center (WACIC) and Department of Licensing (DOL) databases to corroborate information provided by the store. Once a suspect's identity

³ <https://www.seattle.gov/police/community-policing/community-programs/retail-theft>

has been verified, the case is linked to that suspect's profile in Mark43, which typically contains full PII: name, address, date of birth, SSN, and DLN.

When an individual was detained by store security, some retailers provided SPD with the Driver's License Numbers (DLN) and Social Security Numbers (SSN). At least one retailer participating in the Retail Theft Program regularly uploaded "trespass forms" of their own design which included hand-written DLNs and SSNs.

Compiling of Offenses

We found that some store detectives and corporate loss prevention staff use the retail track of Coplogic to document repeated offenses by the same individual to build cases for prosecution under the City Attorney's High Utilizer Initiative. The High Utilizer Initiative is a program created by the Office of the City Attorney to identify offenders responsible for repeated crimes across Seattle and reduce their impact on public safety. Under the High Utilizer Initiative, individuals who have been referred by police to the City Attorney's Office 12 or more times within 5 years and at least once within eight months would be eligible for booking into jail for otherwise non-bookable misdemeanor offenses and warrants. These individuals are then ineligible to participate in the Seattle Municipal Court's diversionary court program.

Some retailers appeared to be submitting reports of shoplifting by a given individual only via the retail track of Coplogic, with no calls to 9-1-1 or other direct engagement with SPD outside of the Coplogic report. Reports were sometimes submitted to SPD in batches – in some cases a month after an incident took place. This is notable because absent an interaction with SPD, suspects in these cases may not have been aware that they were building toward a potential felony charge under the High Utilizer Initiative.

Policy Guidance

SPD policy "15.200 – Retail Theft Program" applies to arrests made by security officers working participating stores. The policy and procedures are concerned with how SPD officers respond to a retail theft incident, but do not contain criteria for SPD in reviewing or accepting reports filed in Coplogic or any other form of retailer-generated complaints where an SPD officer is not responding to the scene.

When a retailer is reporting an incident, it may not be necessary to detain a suspect and copy their identification in order to establish their identity. This is particularly true when the suspect has been detained previously. If store security detains a suspect and records their identification, the risk of physical altercation, improper handling of PII, and bias are all increased. However, by not detaining an individual or

having an officer respond to the scene, there is a greater risk of misidentification or missed opportunities for diversion. SPD should, through policy, and then through training, establish criteria for what actions and information it expects from retailers participating in the retail track of Coplogic.

Recommendation 2: SPD should update policy 15.200 and/or other applicable guidance to establish criteria for submissions through Coplogic or any equivalent submissions system under the Retail Theft Program, giving specific consideration to:

- a) The minimum PII necessary to establish a suspect's identity
- b) Specific methods a retailer identifies suspects
- c) How soon an incident should be reported
- d) When a suspect should be detained

Purpose Of Use

Within the 2021 review period, we did not find evidence that indicated Coplogic was used to analyze patterns or predict behavior of individuals or groups. The patterns of use around Coplogic were consistent with public usage of other methods of reporting crime, such as calling 9-1-1 or the SPD non-emergency line. Due to Coplogic's web-based format, victims of crimes can upload photographic evidence and documents during the reporting process, which is not possible when reporting a crime via telephone. While Coplogic facilitates submission of digital evidence at the convenience of victims of or witnesses to crimes, it also offers a smaller range of reportable crimes than SPD's other collection methods (filing a police report either by telephone or in-person). Incidents that can be reported through Coplogic include: commercial burglary, credit card fraud, graffiti, harassing phone call, identity theft, lost property, narcotics activity report, property destruction, residential burglary, simple shoplift, theft, theft of automobile parts/accessories, theft of property inside a vehicle, and theft of wages.

False Reporting

During townhall meetings as part of the SIR process, community members asked what measures, if any, exist in Coplogic or in SPD's processing of reports submitted thereof to identify and remedy abuses of the system (e.g., submitting false reports). Most of these comments focused on targeted and malicious false reporting in order to harass a particular individual belonging to a protected class. This review did not assess the likelihood or existence of false reports submitted into Coplogic, but false reporting is prohibited and penalized under RCW 9A.84.040.

Another comment documented in the SIR expressed concerns about the Coplogic system being rendered ineffective due to large quantities of false reports with the explicit purpose to prevent legitimate reports from being attended to. While this review did not find that to be the case within the 2021 data, it is notable that AI text generators such as ChatGPT are already capable of generating highly realistic, fully unique crime report narratives in bulk; as AI image generators improve, they will soon also be capable of providing generated suspect photos.

Critical Insight is not making a specific recommendation about this risk at this time, but instead request that SPD consider how it will account for the possibility of targeted and AI-generated false reporting in any current or future system designed to accept reports from the public.

B. Data Sharing with External Partners and Other Entities

The SIR states that Coplogic data may be shared outside of SPD with the following agencies, entities, or individuals within legal guidelines or as required by law:

- 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
- Members of the public pursuant to the Washington Public Records Act, Chapter 42.56 RCW

According to interviews of SPD personnel, local agencies must request copies of specific case files from SPD's Legal Unit. Data from Coplogic are never given directly to outside agencies without first being added to Mark43. At no point do external entities have direct access to reports in Coplogic or Mark43. Once a report filed via Coplogic is accepted into Mark43, it is immediately removed from Coplogic. From that point on, the data contained in the report are stored only in Mark43.

In a review of 33% of the reports made via the retail track, there were at least two cases where SPD shared video data – with the King County Prosecutor's Office and with the City Law Department. In both cases, video evidence was provided on an evidence-grade DVD copied from SPD's stored original.

Requests for records from the public are submitted via the GovQA⁴ online web portal. Following a review of SPD's GovQA requests, we determined that – due to limitations in search parameters – it is not currently feasible to generate an accurate assessment of the number of Coplogic reports released to individual members of the public.

⁴ GovQA is the public records management system used by the City of Seattle, including SPD, to receive and respond to records requests submitted by the public. The public-facing portion of this system is known as the Public Records Request Center.

C. Data Management and Safeguarding of Individual Information

Contract with LexisNexis

In retroactively approving the use of this surveillance technology, the Seattle City Council directed OIG to review SPD's contractual relationship with LexisNexis in support of SPD's use of Coplogic technology, including SPD's required records retention and sharing policies.

A consultant agreement with LexisNexis is available on the City of Seattle website.⁵ According to Seattle IT personnel, this agreement is the sole contract of services between LexisNexis and the City for use of Coplogic. Although the effective dates of this agreement have passed, Seattle IT informed us that this agreement maintains the effective terms of the present arrangement for ongoing use of Coplogic. Data retention and use is covered in section 27, pp 10-11. The Consultant Agreement states on page 11:

"The Consultant may use, transmit, distribute, reproduce, display and store the City Data solely for the purposes of (i) providing the Services as contemplated in this Agreement, and (ii) enforcing its rights under the Agreement. The Consultant shall not use City Data / Personal Information to engage – or enable another party to engage – in marketing or targeted advertising."

The agreement defines "City Data" as follows on page 11:

"City Data" shall mean all information collected by or on behalf of the City, and maintained by Consultant."

The agreement defines "Personal Information" as follows:

"Personal Information" shall mean any information that (a) identifies an individual or that may be used to track, locate or identify an individual (for example, an individual's name, address, telephone number, email address, date of birth, Social Security Number, or financial account number or credit card number) or (b) is related to an identified or identifiable individual (for example, credit card transaction of an identified or identifiable individual). Personal information shall include, without limitation, the following:

- *First and last name including full name, any current or former names/monikers, name and initials in any combination*

⁵ https://www.seattle.gov/Documents/Departments/Tech/Lexis_Nexis_Consultant_Agreement.pdf

- *Address, household information*
- *Nationality, racial or ethnic origin*
- *Telephone number (home telephone number, personal cellular, mobile or wireless number)*
- *E-mail address*
- *Mother's maiden name*
- *Date of birth, age*
- *Sex and/or Gender, marital status, sexual behavior or sexual preference, religious, philosophical or political beliefs*
- *Trade union membership*
- *Government identification number (including Social Security Number (including truncated SSN's), Passport number, driver's license number, or state identification number)*
- *Financial or credit/debit card information, billing information, account information, consumer purchase or billing history*
- *Username and password or security question and answer*
- *Information on medical or health conditions. Unique biometric information and physical appearance (including scars, marks and tattoos)*
- *Geolocation information, including such information generated from an electronic communications device*
- *Machine identifiers (e.g. IP/MAC addresses)*
- *Customer services/account/consumption information*
- *Criminal justice and court information*
- *Student information (School record or other educational information)*
- *Minor, youth information"*

This language appears sufficient to preclude LexisNexis from sharing or using data collected from Coplogic reports for any purpose other than to provide the Coplogic service for the City. It specifically precludes using City Data or Personal Information (as defined above) to engage in, or enable another party to engage in, marketing or targeted advertising.

While the end date of the agreement was October 31, 2018, Seattle IT informed us that this agreement has been renewed annually since then as part of SPD's subscription to the LexisNexis Coplogic application, which operates as "software-as-a-service" and remains resident on LexisNexis's own computers. The terms of the agreement have not been changed or amended by either party.

Data Retention

While the existing agreement appears to preclude the sharing or use of data, it has no specific provision regarding data retention and no limit on how long LexisNexis may retain City Data or Personal Information.

Although the SIR states that the agreement governs the 120-day retention lifespan on LexisNexis servers, no such provision explicitly exists in the agreement. While Critical Insight consultants reviewed data stored in Coplogic and found that there were no reports older than 120 days in the system, it could not be assessed if any reports continued to exist on the LexisNexis servers longer than 120 days.

Recommendation 3: SPD should work with Seattle IT and LexisNexis to formalize that Coplogic records will be deleted from LexisNexis servers after 120 days.

Safeguarding of Individual Information

Although reports are retained in Coplogic for a maximum of 120 days, accepted reports are imported into Mark43 where they are retained indefinitely. Because of this, the security of Mark43 is a significant factor in reviewing how SPD safeguards the information of individuals it receives via Coplogic.

In 2022, the FBI audited SPD's overall Criminal Justice Information Services (CJIS) and noted violations of CJIS security policy with respect to Mark43. The following sections give the text of each relevant finding and the current status of remediation.

Auditing of Access and Activity Logs

CJIS Security Policy, Version 5.9, June 2020, 5.4 Policy Area 4: Auditing and Accountability, pp. 27-28

*Policy Finding: **OUT** [of compliance]*

Ensure logs for Mark 43 are reviewed weekly and retained for a minimum of one year.

From interviewing SPD personnel, we understand that the City is in the process of exploring how Mark43 access could be reviewed in real time by the City's Security Operations Center. This appears to be a capability which Mark43 does not currently provide. SPD is working with Mark43 to address these security needs; however, this means that Mark43 is not CJIS-compliant until these security needs have been addressed.

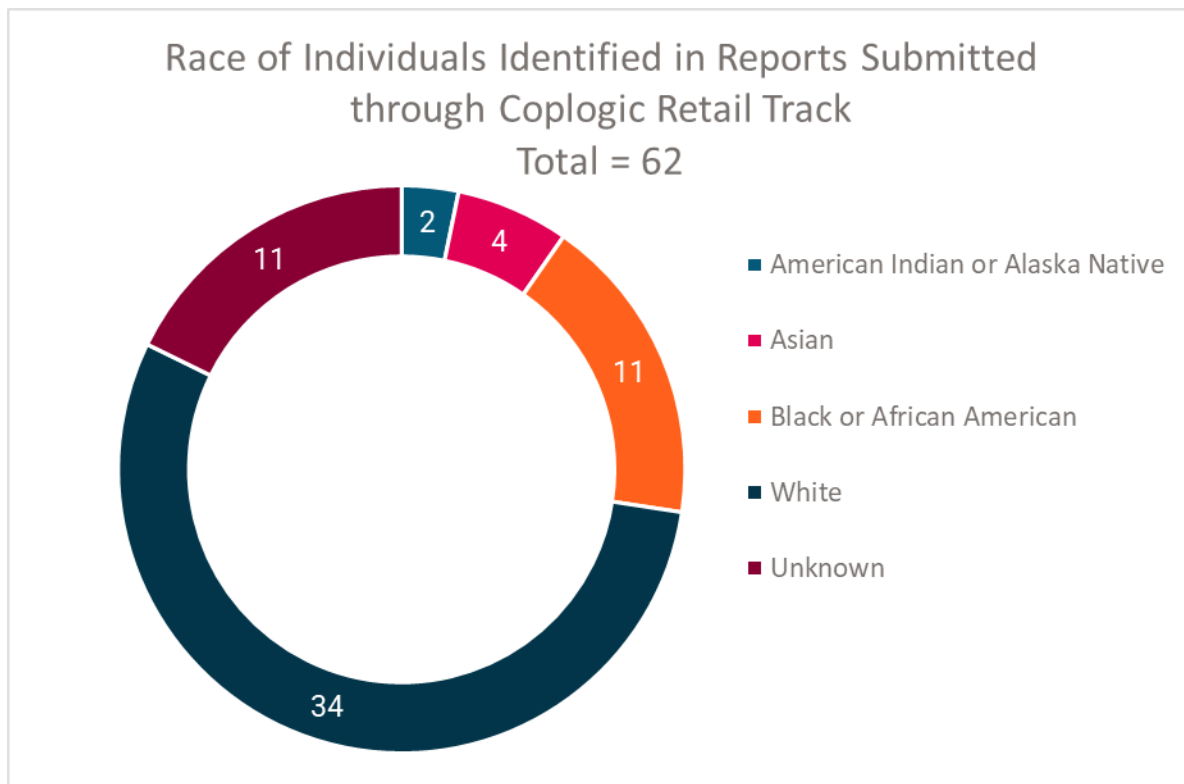
Critical Insight is not making recommendations at this time, as the systems, policies, and processes addressed in this section are broader than the scope of this technology review. OIG will continue to monitor this concern and explore potential follow-up work to address the systemwide concerns.

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

Retail Track Bias

One concern raised in the Privacy and Civil Liberties Assessment within the SIR was that the retail track of Coplogic was at risk of reinforcing practices of racial profiling among retailers, leading to disparities in arrests.

The reliability of retail track data used within this review is limited by the small number of retailers and locations submitted reports through the retail track, as discussed in Section A of this report. Among the 111 retail track reports identified, 62 unique individuals were listed as suspects.⁶



From the data above, we did not find clear evidence of disproportionality in reports submitted through the retail track over the period of our review. However, we emphasize that our analysis is significantly limited by the size of this population, and

⁶ In some incidents, multiple suspects are listed.

if the number of participating retailers increases as expected in following years, this analysis should be repeated.

Accessibility of Coplogic

Our review of Coplogic found the following potential access issues for disadvantaged communities:

- The Coplogic web and mobile applications are only available in English. There are no localizations available for non-English languages. Therefore, this service is not accessible to non-English speakers, people for whom English is not their first language, or illiterate users.
- The Coplogic web and mobile applications depend on the user's ability to read text. This means users with visual impairments may not be able to use Coplogic.
- The Coplogic web and mobile applications also require that users have access to a computer or smartphone. This creates a barrier for individuals who cannot afford computers, smartphones, or Internet access. Additionally, Coplogic's web-based format makes it less likely that the elderly and other users with low technological literacy will use it.

During the public comment period, community members identified these same access concerns. Community members noted that although Coplogic streamlines crime reporting, they did not want it to replace other forms of reporting. To that end, these comments request an expansion of access to Coplogic, often noting that the above-mentioned disadvantaged communities may be among the most vulnerable to crime.

During interviews, SPD personnel noted that because of a shortage of available officers, the SPD non-emergency telephone line has been staffed less in recent years, meaning that non-emergency telephone assistance is available fewer hours of the day. While we found no indication that the adoption of the Coplogic system directly relates to this staffing reduction, we are concerned that limited availability of the SPD non-emergency telephone line may render non-emergency reporting inaccessible for members of the community who are unable to read, write, use a computer, or use the Internet.

We recommend the following remediations:

- **Recommendation 4:** SPD should work with Seattle IT and LexisNexis implement localizations for the major language groups used in the Seattle metro area for the Coplogic web and mobile applications

- **Recommendation 5:** SPD should work with Seattle IT and LexisNexis to ensure Coplogic web and mobile applications are fully compatible with screen-reader devices and applications used as accessibility aids by blind users

E. Complaints and Concerns Received

Office of Police Accountability (OPA) Complaints

We found no complaints submitted to OPA regarding the Coplogic surveillance technology in 2021.

Customer Service Bureau Complaints

At least two Seattle residents attempted to report an incident type that is not accepted through Coplogic (assault and attempted break-in); because they could not correctly file the incidents, they contacted the Seattle Customer Service Bureau.

Another Seattle resident filed a complaint with the CSB, fearing their online-submitted police report would go unaddressed because they stated that Coplogic indicated no follow up would occur.

Internal Audits or Assessments

According to SPD's Audit, Policy and Research section, no internal audits or assessments have been conducted on this technology.

F. Costs

The estimated 2021 costs of Coplogic were \$285,435.67. This estimation accounts for two types of costs:

- Personnel costs associated with the usage of the technology, such as hours billed by SPD officers while reviewing and approving reports submitted via Coplogic.
- The technology's annual license fees and maintenance costs.

In 2021, SPD assigned five officers to review, validate, and accept police reports submitted through Coplogic. The combined salaries totaled approximately \$275,074.51. According to Seattle IT, the 2021 annual application licensing costs totaled to \$10,361.16, which coincides with the figure quoted in the SIR (\$10,365 annually). In Section A of this report, we estimated that 23,040 reports were accepted through Coplogic in 2021. This represents an estimated average cost of \$12.39 per accepted report in 2021.

G. Feasibility of Locating the Coplogic Application on a City Server

The Seattle City Council requested that OIG include in this annual surveillance usage review an analysis of the costs and benefits of locating the Coplogic program on a City server.

It is not presently possible to relocate the Coplogic program on a City server because no “on-premises” version of the software exists. LexisNexis designed Coplogic as a pure “Software-as-a-Service” (SaaS) solution, and all competing solutions with similar functionality to Coplogic are also SaaS-based.

RECOMMENDATION RESPONSES FROM SPD

1. SPD should work with Seattle IT and applicable vendors to modify Coplogic and Mark43 integration so that Retail and Individual track reports in Coplogic are identified as such after import into Mark43

Management Response

Concur Do Not Concur

Estimated Date of Implementation: None provided

Proposed Implementation Plan: SPD is replacing Coplogic with a new system which will go through the PA/SIR process. We will ensure the new system conforms with this recommendation. We are still working through the process, so it isn't possible to give an estimate for when this work will be done.

2. SPD should update policy 15.200 and/or other applicable guidance to establish criteria for submissions through Coplogic or any equivalent submissions system under the Retail Theft Program, giving specific consideration to:
 - a. The minimum PII necessary to establish a suspect's identity
 - b. Specific methods a retailer identifies suspects
 - c. How soon an incident should be reported
 - d. When a suspect should be detained

Management Response

Concur Do Not Concur

Estimated Date of Implementation: None Provided

Proposed Implementation Plan: SPD is replacing Coplogic with a new system which will go through the PA/SIR process. We will ensure the new system conforms with this recommendation. We are still working through the process, so it isn't possible to give an estimate for when this work will be done. Implementing the new system will include and update of policy, including related to the Retail Theft Program.

3. SPD should work with Seattle IT and LexisNexis to formalize that Coplogic records will be deleted from LexisNexis servers after 120 days.

Management Response

Concur Do Not Concur

Estimated Date of Implementation: None Provided

Proposed Implementation Plan: SPD is moving away from Coplogic

4. SPD should work with Seattle IT and LexisNexis to implement localizations for the major language groups used in the Seattle metro area for the Coplogic web and mobile applications

Management Response

Concur Do Not Concur

Estimated Date of Implementation: None Provided

Proposed Implementation Plan: SPD is moving away from Coplogic

5. SPD should work with Seattle IT and LexisNexis to ensure Coplogic web and mobile applications are fully compatible with screen-reader devices and applications used as accessibility aids by blind users

Management Response

Concur Do Not Concur

Estimated Date of Implementation: None Provided

Proposed Implementation Plan: SPD is moving away from Coplogic

NON-AUDIT STATEMENT

This review was not conducted under Generally Accepted Government Auditing Standards. However, OIG has reviewed the work of Critical Insight to provide reasonable assurance that evidence used in this review was sufficient and appropriate.