Minneapolis Police Department

Biennial Automated License Plate Reader Audit

Abstract

This document has been drafted to provide an audit of the Minneapolis Police Department’s use of Automatic License Plate Readers (ALPR).

WILDCARD®

CYBERSECURITY • WEB DEVELOPMENT • IT SOLUTIONS

Biennial Automated License Plate Reader Audit

This biennial audit report has been prepared for the Minneapolis Police Department satisfying requirement of Minnesota statute 13.824. The Automated License Plate Reader Audit focused on the compliance and operational efficiencies of the Minneapolis Police Department.

Wildcard wishes to acknowledge the cooperation and efforts of the Minneapolis Police Department in the execution of the audit. Particularly the Strategic Information Center, Business Technology Unit, and the Records Information Unit. We would also like to thank Internal Audit for facilitating audit activities. of the staff at the agencies included in our audits.

Talin Senner
Chief Executive Officer
Wildcard Corporation
12 November 2019

Executive Summary

Objectives - Two audit objectives were identified for the biennial audit of the Automated License Plate Reader (ALPR).

- Assess the Minneapolis Police Department (MPD) use of ALPR to determine it's compliance with Minnesota statute 13.824.
- Review, examine, and assess MPD policies and procedures for the operation of ALPR to determine if there are any potential for improvement to support compliance efforts and operation.

Scope

Wildcard has conducted a biennial audit of the Minneapolis Police Department's use of Automatic License Plate Readers (ALPR). The objective of this engagement is to audit compliance with ALPR laws and regulations, and review relevant policies, procedures and security controls, as required by the State of Minnesota Statute 13.824. The audit was an independent review of the MPD's implementation of ALPR technology and processes to determine how data is currently classified, used, and destroyed. Wildcard also verified that the system access was appropriate.

The audit was conducted by evaluating the use of the system via observing relevant artifacts, conducting interviews with personnel, and examining the system. Our observations ranged from the time of the conclusion of the previous audit August 1, 2017 to July 31, 2019. **We have determined that MPD's operation of ALPR technology is in compliance with Minnesota Statute 13.824 and all associated relevant statues.**

Wildcard worked with MPD to determine that:

- MPD ALPR policy includes provisions for all mandated elements
- ALPR data collected is limited to what is allowed by statute
- ALPR data is private unless part of a criminal investigation
- ALPR data access is limited to those authorized is use is limited to that which is allowed by policy

Areas of Improvement

While MPD is in compliance, Wildcard has identified some areas of improvement. The areas we focused on are capabilities that support compliance activities. Each area of improvement is specified in the following paragraphs along with our recommendations.

1) Standard Operating Procedures (SOP) for operation of the ALPR has not been established for SIC personnel.

While working with personnel designated as administrators of the ALPR system, Wildcard discovered that there was not a defined SOP in place. ALPR operation is governed by state laws and has defined activities that are necessary for proper operation. The implementation of an SOP will facilitate the proper use of ALPR software and data for all SIC personnel. The SOP will allow for efficient and consistent operations. The SOP will also facilitate future ALPR audits and also offer protection from potential liability.

On October 31, 2019, The SIC created a draft SOP that is being developed to facilitate the handling of ALPR operations.

2) Breach Detection and Incident Response Capabilities

There are currently no controls in place to determine if the ALPR system has been compromised by a malicious actor. The MPD is not actively monitoring if unauthorized users are connecting to and exfiltrating data from the system. There also is not a formalized process within the SIC once a breach has been determined to have occurred or is in process. This finding does not appear to be limited to the SIC. Wildcard recommends that all of the units within the MPD coordinate with the City of Minneapolis Information Technology (IT) and relevant stakeholders to create and implement a cohesive breach detection and incident response plan for all information technology systems.

IT and the City Clerk's office are working to establish a department wide incident response plan to supplement their detection capabilities. Incident handling is currently institutional knowledge but I is actively working to establish more formalized processes. IT will coordinate with MPD and anticipates an incident response plan to be in place by January 2020.

Introduction

The audit objectives, scope and methodology are described in Appendix A.

ALPR Audit

The audit of MPD use of ALPR covers the period of August 1, 2017 to July 31, 2019. Wildcard collected artifacts and conducted interviews with ALPR operators to determine its compliance with Minnesota statute 13.824. The ALPR is defined as an electronic device mounted on a law enforcement vehicle or positioned in a stationary location that is capable of recording data on, or taking a photograph of a vehicle or its license plate and comparing the collected data and photographs to existing law enforcement databases for investigative purposes. Automated license plate reader includes a device that is owned or operated by a person who is not a government entity to the extent that data collected by the reader are shared with a law enforcement agency.

General Observation

MPD has put in place formal and informal policies and procedures to operate the ALPR system in compliance with Minnesota Statute. MPD has written policies in place, collect allowed data, restricted system access, applied appropriate automated data retention controls, and has system logs tracking application use.

Policy

Observation **-** The MPD has an established policy that addresses the mandates associated with Minnesota Statute 13.824. The policy is defined as 4-222 Automated License Plate Reader (ALPR) and last updated on July 29, 2015.

Analysis - Wildcard conducted interviews and evaluated artifacts to conclude that MPD generally follows the formalized defined policy associated with ALPR use. In reviewing the policy, we have determined that it generally addresses the mandates established in the Minnesota Statute 13.824.

Recommendation - None

Data Collection

Observation **–** The MPD ALPR system data collected is limited to license plate numbers, date/time/ location of collected data on vehicles, and pictures are limited to license plates, vehicles, and areas surrounding the vehicle.

Analysis -Wildcard evaluated a sample of data collected by the ALPR system. Each instance of data associated with ALPR was limited to that defined by the Mandate.

Recommendation - None

Classification

Observation – ALPR data is automatically classified as nonpublic. Access to data is limited to MPD personnel. System access to use ALPR readers limited to officers that have been trained and have been granted permissions. ALPR administrative access is limited to SIC personnel who have been authorized by Commander Gerlicher. ALPR lookup requests are limited to MPD and authorized agencies.

Analysis - Wildcard evaluated who has access to the ALPR system. The SIC provided a list of personnel who have been granted access to the system. Most access is limited to operation of mobile ALPR units. Administrative access is limited to select SIC personnel who are capable of conducting lookups of ALPR hits.

Recommendation – None

User Restrictions

Observation – ALPR data is only matched with internal databases. ALPR data is not collected from or placed into a centralized repository. The SIC has created user roles that restrict access to ALPR data. These roles have been granted limited permissions within the software. The permissions allow for personnel to perform their role within the SIC without granting excessive access.

Analysis - Wildcard conducted interviews with SIC personnel. We also evaluated ALPR usage data to determine if systems access is limited. We have observed the defined roles within the system and associated those roles with accounts. Those that are designated as administrators are limited to those explicitly authorized by Commander Gerlicher.

Recommendation – Wildcard recommends that detective controls be put in place to detect if there is any unauthorized use/abuse of the system. These detective controls would serve in support of incident response support. These controls could be developed in support of the City of Minneapolis Information Technology department.

Management Response – MPD is working with City of Minneapolis Information Technology (IT) and the City Clerk's office to establish a department wide incident response plan to supplement their detection capabilities. Incident handling is currently institutional knowledge but MPD is actively working to establish more formalized processes. City IT anticipates an incident response plan to be in place by the first quarter of 2020.

Data Destruction

Observation **–** MPD Configured the ALPR system to automatically destroy collected ALPR data after a period of 60 days.

Analysis **-** Wildcard observed the system configured to remove data after 60 days. The SIC executed a query of the database to verify that the system is deleting any data stored passed retention threshold. Any data that is associated with an active investigation is delivered to the officer in a PDF file. That file is then retained in a separate system.

Minnesota statute Chapter 5B is for individuals attempting to escape from actual or threatened domestic violence, sexual assault, or harassment or stalking frequently establish new addresses in order to prevent their assailants or probable assailants from finding them. ALPR data related to a Chapter 5B participant must be destroyed at the time of collection or upon receipt of the request, unless the data are active criminal investigative data. There have been no Chapter 5B requests over the audit period. A Chapter 5B request would require the MPD to remove associated data.

MPD has in place processes to handle Chapter 5B requests. Despite lacking the capability to destroy data at the time of collection, MPD has in place mitigating controls that minimizes the ability of data access for unauthorized individuals. The controls are designed to meet the spirit of the Chapter 5B program while enabling the department's ability to conduct investigations. The data will be protected until automatic retention settings of software remove Chapter 5B associated data or another request has been submitted.

Recommendation **-** Wildcard recommends that formalized procedures be created and documented for the handling of Chapter 5B requests.

Management Response **-** On October 31, 2019, The SIC created a draft SOP that is being developed to facilitate the handling of ALPR operations.

Sharing among law enforcement agencies

Observation **–** ALPR requests to the SIC are made via email, phone, and office drop ins. MPD personnel and other government agencies submit requests that can include dates, license plate numbers and case numbers. Wildcard reviewed a sample of requests from internal officers and external agencies.

Analysis **-** Wildcard observed ALPR requests being submitted to the SIC. If there is a hit, SIC personnel respond with a PDF export from the ALPR software. The report has the device that captured the data, a timestamp, the location, and the image of the captured data. SIC personnel have indicated that requests are only fielded from a few agencies. The agencies authorized to request ALPR data is not currently explicitly defined in policies or procedures.

After reviewing the agency sharing requests and fulfillment, Wildcard observed that the SIC does not explicitly state how the receiving agency is expected to handle data classification, destruction, and security of the data as mandated by Minnesota Statute 13.824 Subd 4(b).

***Recommendation* -** Wildcard recommends the creation of standardized operating procedures (SOP) that define which agencies SIC personnel are authorized to share data. Currently, the process in place is ad hoc and institutional knowledge. Formalizing the authorized agencies limits the potential for abuse of ALPR data and limit liability.

Wildcard recommends that whenever fulfilling a request for an external agency, a note is added to notify the agency how the data should be classified, destroyed, and secured. This note could be a part of a standard email template that is used by all SIC personnel authorized to provide ALPR data to other agencies. The process could also be incorporated into an SOP that can allow for efficient and consistent operations across all personnel.

***Management Response* -** On October 29, 2019, MPD has directed SIC personnel to include the following language to email signatures:

"Confidentiality Notice: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, be aware that any unauthorized disclosure, copying, distribution or use of the contents of this information is prohibited and punishable by law. If you have received this electronic transmission in error, please immediately notify the sender by return email. This email is for criminal investigation law enforcement purposes and may not be used for background or employment investigations."

ALPR Logging

***Observation* –** MPD's implementation of ALPR software logs maintain the time data was collected, total number of vehicles/plates recorded, Number of vehicles/plates that are associated with crimes or investigative data, and location data was recorded. Plates associated with crimes have the data retention requirements assigned to them in other systems.

ALPR inventory is tracked within the SIC. This information is not available to the public because they have been categorized as sensitive with the Minnesota Bureau of Criminal Apprehension (BCA).

***Analysis* -** The SIC provided ALPR data over the retention period that confirms that they log appropriate data. The ALPR software has extensive logging capabilities and satisfies mandates associated with Minnesota Statute 13.824.

Recommendation - None

Appendix A: Methodology

Audit Objectives

Two audit objectives were identified for the biennial audit of the Automated License Plate Reader (ALPR).

- Assess the Minneapolis Police Department (MPD) use of ALPR to determine it's compliance with Minnesota statute 13.824.
- Review, examine, and assess MPD policies and procedures for the operation of ALPR to determine if there are any potential for improvement to support compliance efforts and operation.

This audit is a biennial audit mandated by state law. Our findings are that MPD operates in compliance with state statutes. The recommendations that are included in this report are supplemental to ALPR compliance. To ensure a wide coverage for compliance assurance, interviews were conducted with ALPR administrators, system logs and settings were evaluated, policy was reviewed, and training materials were assessed.

The methodology used during the audit has been refined using well known frameworks integrating:

- American Institute of Certified Public Accountant (AICPA)
- Information Systems Audit and Control Association (ISACA)
- Control Objectives of Information Technology (COBIT)
- Infrastructure Library for Information Technology (ITIL)

The audit was conducted in three distinct phases:

- During the Planning phase criteria were developed to support the audit objectives and an audit program was produced to identify the information that will be collected during the audit execution phase.
- During the Execution phase artifacts were collected to evaluate relevant information (interviews, document reading, and log/system evaluation) on the ALPR operational functions.
- During the Reporting phase, information analysis is finalized. Findings are presented in draft report and presented to stakeholders for evaluation. Stakeholders have the opportunity to review findings and provide a rebuttal. We then finalize the report and structure working paper files.

Appendix B: Interviewed Roles

- 1 Commander
- 2 Supervisors
- 1 Administrator
- 2 Records Management Specialists