Biennial Audit of the Shakopee Police Department Automated License Plate Reader System Conducted by LEADS Consulting

Audit Summary Report
Submitted August 1, 2017

Pursuant to Minnesota Statute 13.824 LEADS Consulting conducted an audit of the Automated License Plate Reader (ALPR) System at the Shakopee Police Department to ensure compliance with state law. The audit was conducted on July 20, 2017. Captain Chris Dellwo was the point of contact for auditors.

A copy of the Shakopee Police Department policy regarding ALPR was reviewed and is attached to this audit as appendix A. Verbal information regarding operations and practices was received from Shakopee Captain Chris Dellwo who supervises the ALPR system. The audit examined the policies and practices of the department in regards to the use and operation of Automated License Plate Readers including the following functions:

1. ALPR Data Collection Limitations
2. Classification of ALPR Data
3. Destruction of ALPR Data
4. Access to ALPR Data
5. Sharing of ALPR Data
6. Audit Trail of ALPR Data
7. Public Log of Use

Shakopee ALPR System

The Shakopee Police department utilizes the ELSAG "Plate Hunter" system. They have three mobile squads equipped with cameras. The system has been in operation since September of 2013.

At the time of the audit on July 20, 2017, the system had recorded 131,791 "reads" and 1358 "hits" or "alarms" during the previous 60 days. 1055 alarms were a result of a drivers license suspension or revocation infraction, 64 indicated the vehicle was stolen and 15 indicated the owner of the vehicle was wanted or had a warrant for his/her arrest.

"Reads" are defined as a data collection event in which a license plate is believed to have been "read" and recorded in the system. A "hit" or "alarm" is defined as an indication from the system that the vehicle is stolen, the owner is suspended, revoked, cancelled or has a warrant, or the vehicle has a KOPS alert in the system.

ALPR Data Collection Limitations

Minnesota Statute 13.824 Subd. 2 limits the collection of data by an automated license plate reader system to license plate numbers; time, date and location data on vehicles; and pictures of license plates, vehicles and areas surrounding the vehicles. The Shakopee Police Department ALPR policy also reflects state statute.

To verify compliance, LEADS conducted a sequential random audit of 131,791 "reads" from the last 60 days. We examined 610 "reads".

All 610 data "reads" and photographs were in compliance with Subd. 2.

The following observations were noted during the audit/examination of 610 "reads".
Eighteen "reads" were missing GPS location data.
One read had a person in the photograph near a vehicle plate being read but their image was not discernible.
Twenty-four false reads were generated by street signs, mail boxes, or bumper stickers containing words or numbers.

A more detailed analysis of the "1358" "hits" during the most recent 60 days revealed that several of the "hits" were duplicate "reads". In one case a license plate registered an alarm 58 times by the system of a vehicle that was impounded at the

police department. In addition some false “hits or alarms” were generated as the system can not identify the specific state of the license plate.

Classification of ALPR Data

The Shakopee Police Department Policy states that “All data collected by an ALPR is classified according to Minnesota State Statute 13.82.”

Captain Chris Dellwo who supervises the ALPR system is well versed in the law pertaining to ALPR and the classification of data.

The Shakopee Police Department data classification is in compliance with Minnesota Law.

Destruction of ALPR Data

Section V of the Shakopee ALPR policy states that “Data collected by an ALPR that are not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection.” More detail regarding the Shakopee Police “Data Storage” and destruction policy can be found in appendix A of this report.

Our examination of the Shakopee ALPR data base revealed that there was no data maintained in the system beyond the 60 day restriction. Several electronic searches were conducted for data older than 60 days with negative results. Captain Chris Dellwo confirmed that no data has been retained beyond 60 days.

The examination indicates that the Shakopee Police Department is in compliance with the destruction of data provision.

Access to ALPR Data

Section VI of the Shakopee Police Department policy states that “Access to ALPR data base must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation and must include a record of the factual basis for the access and any associated case number, complaint or incident that is the factual basis of the access.”

The policy also requires the searching officer to document the basis for the query by creation of an "LPR Search" Incident Record that can be compared against the system's electronic audit trail.

The department also uses "role-based access" rules corresponding to official duties.

The Shakopee Police Department policies and practices regarding access to ALPR data are in compliance with state law.

Sharing of ALPR Data with other Law Enforcement Agencies

Section VII of the Shakopee Police Department policy states that data may only be shared with law enforcement for "legitimate law enforcement purposes." The policy also states that any requests must be sent to the Chief of Police or his designee, who at the time of the audit was Captain Chris Dellwo.

Captain Dellwo maintains a file of emails sent to the department requesting searches of the ALPR system which document the legitimate law enforcement need.

An interview with Captain Chris Dellwo of the Shakopee Police Department and a review of his file revealed that requests from other agencies for ALPR data are rare but compliant with state law.

The department is in compliance with state statute regarding the sharing of ALPR data.

Audit Trail of ALPR Data

The ELSAG software system maintains a detailed audit trail of all activities indicating access to the data base which was examined by the auditor.

The department is in compliance with the audit trail requirement.

Public Log of Use

The ELSAG software system is capable of producing reports required by the Subd. 5 of the statute. Captain Chris Dellwo maintains several detailed "logs" or reports

that reflect summary data collected by the ELSAG system. These reports do not include any license plate identifying information. Reports include a Daily Activity "Statistics Report" on ALPR unit "reads" by date/time and a "Reads/Alarms Report" that keeps a record of the number of "Hits/Alarms" the system recorded and the reason for the alarm.

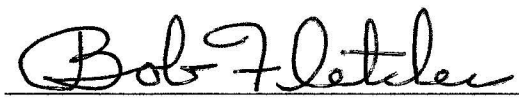
The department has no stationary or fixed license place readers.

The department is in compliance with the Public Log of Use requirement.

Audit Conclusion

The Shakopee Police Department has a detailed ALPR policy that reflects MN statute 13.842 and contains significant specific regulations to ensure compliance with the statute. The department's policies and practices are consistent with state law. The ALPR system utilization is professionally monitored and supervised by Captain Chris Dellwo who is well versed in the requirements of Minnesota Law .

LEADS Consulting finds the Shakopee Police Department to be in compliance with Minnesota Statute 13.824.



Bob Fletcher
Director,
LEADS Consulting
Law Enforcement Audit and Data Services
www.leads50.com

Appendix A - Shakopee Police ALPR Policy

41.3.9 AUTOMATIC LICENSE PLATE RECOGNITION SYSTEM (ALPR)

I. Policy Statement

The Shakopee Police Department recognizes the use of the Automatic License Plate Recognition System (ALPR) as an effective tool to identify vehicles and/or vehicle owners who are associated with criminal activity, driver license violations, and missing and endangered persons.

II. Definition

Per Minnesota State Statutes, Automated License Plate Reader means 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 an existing law enforcement database for investigative purposes. The law enforcement database is updated by the state Bureau of Criminal Apprehension (BCA) twice daily. 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.

III. Operator's Responsibilities

A. Only officers trained in the proper use of the ALPR may operate it.

B. At the start of each shift the officer shall open the system and download the latest update to the database. The system can operate in the background allowing the officer to use the MDC in the normal course of duty.

C. When an officer receives a "hit" on the ALPR, the system will alert the officer visually and audibly to the match. The officer must then acknowledge the "hit" and verify the "hit" is current, by running the information through the state real-time data system prior to taking enforcement action.

D. Proper department procedures and safe police tactics should be followed when initiating a stop or investigation into a "hit" vehicle.

E. Any problems with the system should be immediately reported to the ALPR administrator or a supervisor.

IV. Data Collected by an ALPR must be limited to the following:

A. License plate numbers.

B. Date, time, and location data on vehicles.

C. Pictures of license plates, vehicles, and areas surrounding the vehicles.

D. Collection of any data not authorized above is prohibited.

E. Data collected by an ALPR may only be matched with data in the Minnesota license plate data file. Additional sources of data may be used for matching if the additional data relates to an active criminal investigation.

F. ALPR's must not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, or exigent circumstances justify the use without obtaining a warrant.

V. Data storage

A. Data collected by an ALPR that are not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection. This allows a sufficient time frame for retrieving data relevant to a violation or criminal investigation.

B. Preservation of data is required upon receipt of a written request from an individual who is the subject of a pending criminal charge or complaint, along with the case or complaint number and statement that the data may be used as exculpatory evidence. This data, otherwise subject to destruction after 60 days, must be preserved until the criminal charge or complaint is resolved or dismissed.

C. Destruction of data is required upon written request from a program participant of "Data Protection for Victims of Violence." ALPR data related to the program participant must be destroyed at the time of collection or upon receipt of the request, whichever occurs later, unless the data is classified as active criminal investigative data.

D. All data collected by an ALPR is classified according to Minnesota State Statute 13.82.

VI. Authorization to Access Data shall be permitted by the following

A. Shakopee Police Department personnel is granted access to ALPR data for legitimate, specified and documented law enforcement purposes.

B. Access to this ALPR data must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation and must include a record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.

i. Officers will document any queries of ALPR data in an associated ICR. This will include the factual basis for the query, what was queried and any complaint information.
ii. Associated ICR's shall either be through an active incident, such as a missing person, or an ADMINISTRATICR ICR may be created to document the query.
iii. All ALPR query ICR's shall be given a custom attribute of "LPR SEARCH".
iv. All supporting documents, such as KOPS Alerts, ATL's or a request from another agency, shall be attached to the ICR.

C. The ability of authorized individuals to enter, update or access ALPR data must be limited through the use of role-based access that corresponds to the official duties or training level of the individual and the statutory authorization that grants access for that purpose. All queries and responses, and all actions in which data is entered, updated, accessed, shared, or disseminated, must be recorded in a data audit trail or log.

VII. Sharing of Information among Law Enforcement Agencies

A. Historical data records date, time, plate number, GPS location, squad info and camera info for each read. Historical data is only searchable for legitimate law enforcement purposes, outlined above in paragraph VI.

B. Outside Law Enforcement requests for historical data shall be routed to the Chief of Police, or his/her designee.

C. If data collected by an ALPR are shared with another law enforcement agency under this Subdivision, the agency that receives the data must comply with all data classification, destruction and security requirements.

D. ALPR data that are not related to an active criminal investigation may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by state statute.

VIII. Log of Use

A. Log of use is required to record specific times of day the reader actively collected data.

B. Log of use is required to record the aggregate number of vehicles or license plates on which data are collected for each period of active use, and a list of all state and federal databases with which the data were compared, unless the existence of the database itself is not public.

C. Log of use is required to record the number of vehicles or license plates where the data identifies a vehicle or license plate that has been stolen, a warrant for the arrest of the owner of the vehicle or an owner with a suspended or revoked driver's license or similar category, or are active investigative data.

D. Log of use is required to record an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

E. A list of the current and previous locations, including dates at those locations, of any fixed APLR, or other surveillance device with ALPR capability, must be maintained. This list must be accessible to the public, unless it is determined that the data is security information.

IX. Biennial audit

A. It is required that records showing the date and time ALPR data was collected and the applicable classification of the data be maintained. An independent biennial audit of the records

is required to determine whether data currently in the records is classified, how the data is used, whether they are destroyed as required, and to verify compliance with the law.

B. A report summarizing the results of each audit must be provided to the commissioner of administration; to the chair and ranking minority member of the committees of the House of Representatives and the Senate with jurisdiction over data practices and public safety issues; and to the Legislative Commission on Data Practices and Personal Data Privacy, no later than 30 days following completion of the audit.

X. Notification to Bureau of Criminal Apprehension

A. Within ten days of the installation or current use of an ALPR, or the integration of ALPR technology into another surveillance device, the Bureau of Criminal Apprehension must be notified of that installation, or use, and any fixed location of a stationary ALPR.

XI. Discipline

A. Any person who willfully violates the provisions of this chapter, or any rules adopted under this chapter, or whose conduct constitutes the knowing unauthorized acquisition of non-public data, as defined in Section 13.055, Subdivision 1, is guilty of a misdemeanor.

B. Willful violation, including any action subject to a criminal penalty by any employee, constitutes just cause for suspension without pay or dismissal of the public employee. See Directive 82.

41.3.10 TWO FINGER RAPID IDENTIFICATION DEVICE (IBIS)

I. Definitions

Automated Fingerprint Identification System (AFIS) – The Minnesota Bureau of Criminal Apprehension's fingerprint system for identification of individuals in the criminal justice system.

Rapid Identification System – Also known as IBIS (Integrated Biometics Identification System), is a subsystem of the Automated Fingerprint Identification System (AFIS) that is capable of searching submitted index fingerprints and returning identification and/or criminal history data in a short period of time.

II. Policy

The rapid identification equipment is designed to aid police in the identification of individuals through the evaluation of fingerprints. Only employees who have received training in the use of the Rapid Identification System are authorized to use it.

Two finger based rapid identification data is only an aid to the identification of a person. Information received from the Rapid Identification System shall not be used as the sole grounds for establishing

provable cause for arrest. Police using the rapid identification equipment or accessing the rapid identification data shall ensure that 4th Amendment rights of the individual being tested are not violated and that civil rights, state law, policy and procedure are not violated.

The Minnesota Bureau of Criminal Apprehension requires a record of use be kept, and that record includes the name of the individual using the equipment, date and reason for use. Officers shall document the use in written report or on an Initial Complaint Report (ICR).

Those who use the Rapid Identification System in a manner inconsistent with the policies, state and federal law, will be subject to discipline.