CITY OF CORCORAN

Council Work Session Agenda
February 8, 2024 – 5:30 pm

HYBRID MEETING OPTION AVAILABLE

The public is invited to attend the regular Council meetings at City Hall.

Meeting Via Telephone/Other Electronic Means

Call-in Instructions:
+1 312 626 6799 US
Enter Meeting ID: 893 9035 3069

Video Link and Instructions:
https://us02web.zoom.us/j/89390353069 or visit http://www.zoom.us and enter **Meeting ID: 893 9035 3069**

*Please note in-person comments will be taken at the scheduled meeting where noted. Comments received via email to City Clerk Friedrich at mfriedrich@corcoranmn.gov or via public comment cards will also be accepted. All email and public comment cards must be received by the Wednesday prior to scheduled Council meeting.

For more information on options to provide public comment visit:
www.corcoranmn.gov

1. **Call to Order / Roll Call**
2. **LPR Cameras***
3. **Unscheduled Items**
4. **Adjournment**

***Includes Materials -** *Materials relating to these agenda items can be found in the house agenda packet book located by the Council Chambers entrance, or online at the City's website at www.corcoranmn.gov.*

CITY OF CORCORAN
8200 County Road 116 · Corcoran, MN 55340
763-420-2288 · www.corcoranmn.gov

MEMO

Meeting Date: February 8, 2024

To: City Council

From: Peter Ekenberg, Sergeant
Tim Spellacy, Detective

Re: ALPR

In 2023 the council identified a goal to deploy automatic license plate readers (ALPR) for use by Police/Public Safety. The council reaffirmed the goal in 2024 while staff was conducting research into ALPR cameras.

ALPR cameras read license plates in real time and alerts directly to officers that are working. These alerts could be for stolen vehicles, registered owners with warrants, revoked driver's license status, attempt to locate, Amber alerts, and more.

Staff met with vendors, attended demonstrations, and met with neighboring agencies who currently use ALPR cameras. While researching vendors, staff reviewed features such as security of the information obtained by ALPR cameras, leasing versus buying ALPR cameras, IT related issues with set up and use of the cameras, and the remote nature of where some of the cameras would be located. Staff also learned that some vendors sell information acquired by ALPR cameras, which was not desirable.

Staff identified nine potential locations to deploy ALPR cameras for the initial deployment.

The proposed locations are:

1. Co Rd 30 near Co Rd 101 – Westbound traffic
2. Co Rd 10 near Brockton – Westbound traffic
3. Co Rd 116 near Hackamore Rd – Northbound traffic
4. Co Rd 116 near Co Rd 117 - Southbound traffic
5. Co Rd 50 near Co Rd 19 - Eastbound traffic
6. Co Rd 30 near Co Rd 19 - Eastbound traffic

7. Co Rd 19 near St Hwy 55 - Northbound traffic
8. Co Rd 19 near Co Rd 117 – Southbound Traff
9. Co Rd 10 near Co Rd 19 – Eastbound traffic

Staff wanted the ability to extend the ALPR network by allowing HOA's or private businesses to deploy their own ALPR cameras with the option to integrate police department access.

Staff determined that leasing cameras would be the most beneficial as it would not require costly IT involvement and maintenance. Additionally, the vendor would be responsible for updating the hardware.

Based on the needs that were outlined, staff identified Flock Safey as the vendor that could best meet all of the concerns and requirements staff identified. The Flock program is being utilized by more than 32 agencies in Minnesota, including Medina, Maple Grove, West Hennepin, and Plymouth.

Flock charges an annual flat rate lease per camera of $3,000 per camera, which is wireless, free of infrastructure setup, and has the option for solar or direct power. They also include a warranty, Criminal Justice Information Services (CJIS) compliant cloud-based hosting, unlimited user licenses, ongoing software enhancements, camera setup, mounting, shipping, handling and a cellular connection. The Flock lease program prevents the city from being burdened with maintaining costly equipment at the end of the agreement, which could require replacement.

Financial/Budget:
Each camera is $3,000 a year with a set-up fee of $150 (city pole) or $650 (installed by Flock). Staff is recommending that the first two years' cost be paid using the State of Minnesota's Public Safety money that was disbursed to cities on December 26, 2023. If private entities elect to allow police department access to their information, there is no additional charge.

If Council elects to proceed, staff will incorporate council feedback into the policy and camera locations. Staff will bring final policy and hardware information to council for final approval.

Attachments
a. Automatic license place reader memo
b. Staff slide show
c. Flock information FAQ
d. Flock Privacy and Ethics
e. Minnesota State Statute 13.824
f. Sample Policy ALPR Orono
g. Sample Policy Robbinsdale
h. Sample Policy Rochester
i. Flock Reduce Crime document
j. Sample Policy West Hennepin Public Safety

CITY OF CORCORAN

ALPR CAMERAS

SERGEANT PETER EKENBERG

DETECTIVE TIM SPELLACY

FLOCK COMMUNITY ENGAGEMENT MANAGER KRISTEN MACLEOD

SUMMARY

- IN 2023 THE COUNCIL IDENTIFIED GOALS FOR THE YEAR. ROADSIDE AUTOMATED LICENSE PLATE READERS (ALPR) WERE ONE OF THE ITEMS DISCUSSED IN THE HIGH PRIORITY CATEGORY
- IN 2024 COUNCIL REAFFIRMED THAT GOAL
- STAFF CONDUCTED RESEARCH, ATTENDED DEMONSTRATIONS, AND MET WITH OTHER DEPARTMENTS USING ALPR TECHNOLOGY

CONSIDERATIONS

- BASED ON FEEDBACK FROM THE COUNCIL AND COMMUNITY MEMBERS, STAFF PRIORITIZED SEEKING A SOLUTION THAT APPROPRIATELY INTEGRATES SAFEGUARDS FOR THE PROTECTION AND PRIVACY OF COMMUNITY MEMBERS
- STAFF REVIEWED SEVERAL COMPANIES AND IDENTIFIED FLOCK SAFETY AS A PREFERRED VENDOR FOR OUR NEEDS

GOALS

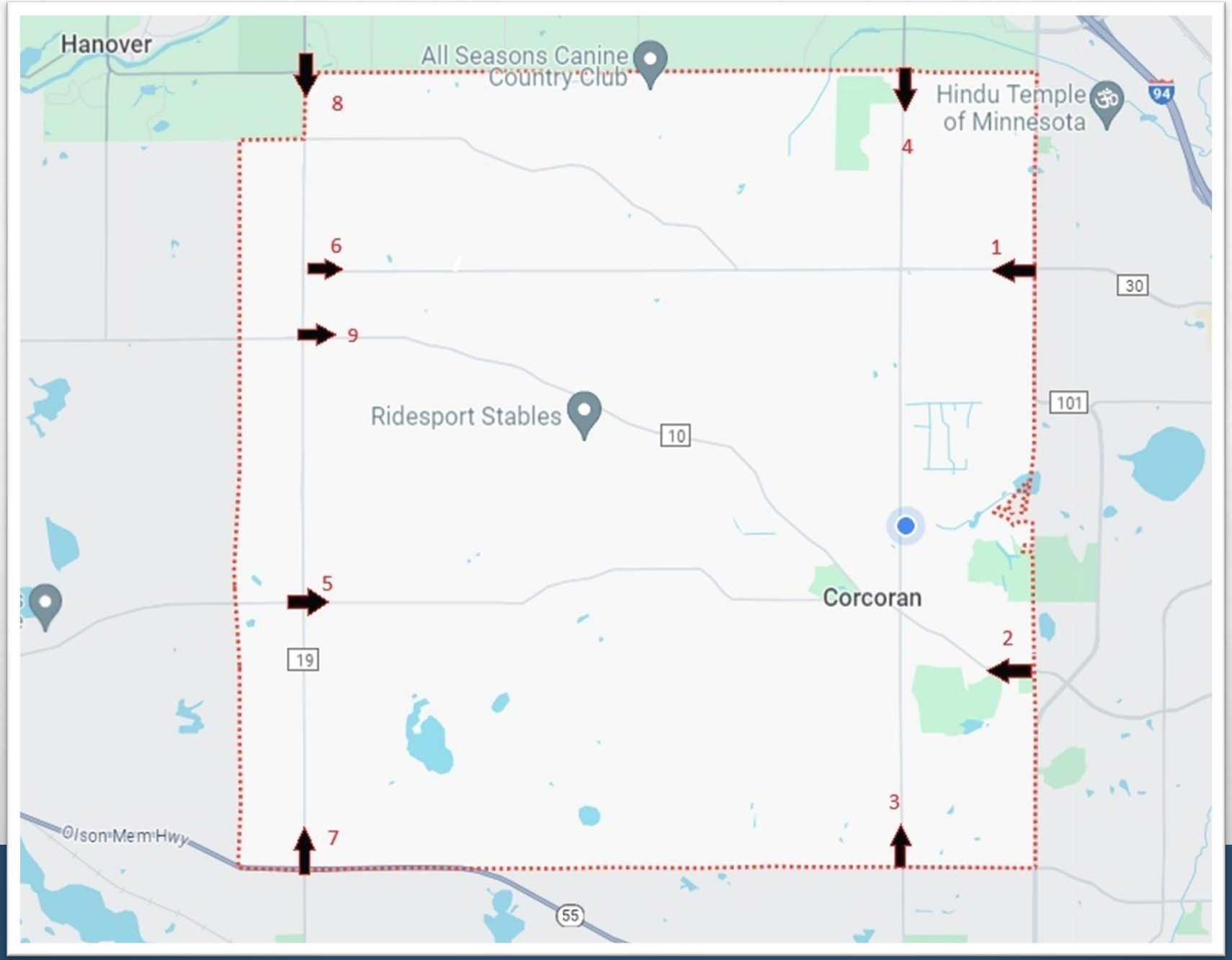
- CREATE A NETWORK OF ALPR CAMERAS AS A FORCE MULTIPLIER FOR PUBLIC SAFETY
- CREATE A FRAMEWORK FOR PARTICIPATION BY HOME OWNERS ASSOCIATIONS AND PRIVATE BUSINESSES
- IMPLEMENT POLICIES TO PROTECT INFORMATION OBTAINED BY ALPR CAMERAS
- PREVENT CRIME BEFORE IT CAN OCCUR
- SOLVE CRIMES MORE EFFICIENTLY

APPLICATIONS FOR ALPR CAMERAS

- ALPR CAMERAS CAN BE USED TO HELP IDENTIFY STOLEN VEHICLES, MISSING PEOPLE, AMBER ALERTS, AND REVOKED DRIVERS TRAVELING INTO CORCORAN.
- TRAFFIC MANAGEMENT AND PATTERNS
- ALPR CAN AID IN INVESTIGATION INTO CRIMES
  - GOLF COURSE THEFTS
  - CATALYTIC CONVERTER THEFTS
  - STOLEN VEHICLE IN RAVINIA
  - CONSTRUCTION SITE THEFTS
  - BUSINESS DISTRICT THEFTS

PROPOSED LOCATIONS

1. CO RD 30 NEAR CO RD 101 – WESTBOUND TRAFFIC
2. CO RD 10 NEAR BROCKTON – WESTBOUND TRAFFIC
3. CO RD 116 NEAR HACKAMORE RD – NORTHBOUND TRAFFIC
4. CO RD 116 NEAR CO RD 117 - SOUTHBOUND TRAFFIC
5. CO RD 50 NEAR CO RD 19 - EASTBOUND TRAFFIC
6. CO RD 30 NEAR CO RD 19 - EASTBOUND TRAFFIC
7. CO RD 19 NEAR ST HWY 55 - NORTHBOUND TRAFFIC
8. CO RD 19 NEAR CO RD 117 – SOUTHBOUND TRAFFIC
9. CO RD 10 NEAR CO RD 19 – EASTBOUND TRAFFIC


Hanover
All Seasons Canine Country Club
Hindu Temple of Minnesota
94
8
4
6
1
30
9
Ridesport Stables
10
101
5
Corcoran
19
2
3
7
Olson Mem Hwy
55

COST

- LEASE PROGRAM - $3,000 A YEAR / CAMERA WITH 650.00 SETUP FEE.
- 1 YEAR/2 YEAR OPTION, CAN INCREASE OR DECREASE CAMERAS.
- PUBLIC SAFETY GRANT MONEY CAN BE USED FOR INITIAL SET-UP AND FIRST YEARS.

SUCCESS STORIES

- WEST HENNEPIN PUBLIC SAFETY REPORTED THEY HAVE BEEN ABLE TO LOCATE MANY DRIVERS WHO ARE SUSPENDED, REVOKED, ETC. HAVE LOCATED SEVERAL STOLEN CARS/PLATES. THEY ALSO USE THE INFORMATION SEVERAL TIMES A WEEK FOR INVESTIGATIONS. MOST RECENTLY, A BUSINESS IN A NEARBY CITY WAS BURGLARIZED. THEY PROVIDED A LIST OF CARS THAT WERE LEAVING THE AREA AROUND THE TIME OF THE BURGLARY.
- ORONO POLICE PROVIDED A RECENT INVESTIGATION THAT LED TO A STOLEN TRAILER BEING LOCATED. ALONG WITH THE TRAILER, OVER $25,000 IN STOLEN PROPERTY WAS ALSO RECOVERED WITH MORE STILL COMING.

FLOCK IN NEIGHBORING COMMUNITIES

- FLOCK SAFETY IS RAPIDLY GROWING IN MINNESOTA AGENCIES
  - NEARBY AGENCIES RECENTLY USING FLOCK
    - ROGERS POLICE, MAPLE GROVE POLICE, PLYMOUTH POLICE, MEDINA POLICE, AND WEST HENNEPIN PUBLIC SAFETY
    - BY CHOOSING FLOCK, WE JOIN WITH ALL OTHER FLOCK AGENCIES INCREASING OUR INVESTIGATIVE SCOPE

CREATE A FRAMEWORK FOR PARTICIPATION BY HOME OWNERS ASSOCIATIONS AND PRIVATE BUSINESSES

FLOCK SAFETY

- LEASED CAMERAS
- WILL SET-UP AND MAINTAIN CAMERAS
- PROCESS FOR COMPANIES/ HOA'S TO GET ALPRS WE CAN ACCESS (WITH PERMISSION)
- REAL-TIME ALERTS
- CAN INTEGRATE WITH OTHER CITES SYSTEM
- SECURE SYSTEM
- DOES NOT SELL INFORMATION

INFORMATION FROM FLOCK

flock safety

+ Corcoran, MN

Eliminate crime and shape a safer future, **together**.

flock safety

Why Flock Safety?

flock safety

flock safety

What we observe:
the current reality

- Limited Police Resources
- Crime is on the rise
- Trust is needed more than ever

What we believe:
the opportunity

- Technology multiplies the force
- Capture and distribute objective evidence to the right user
- Engage community to support and grow

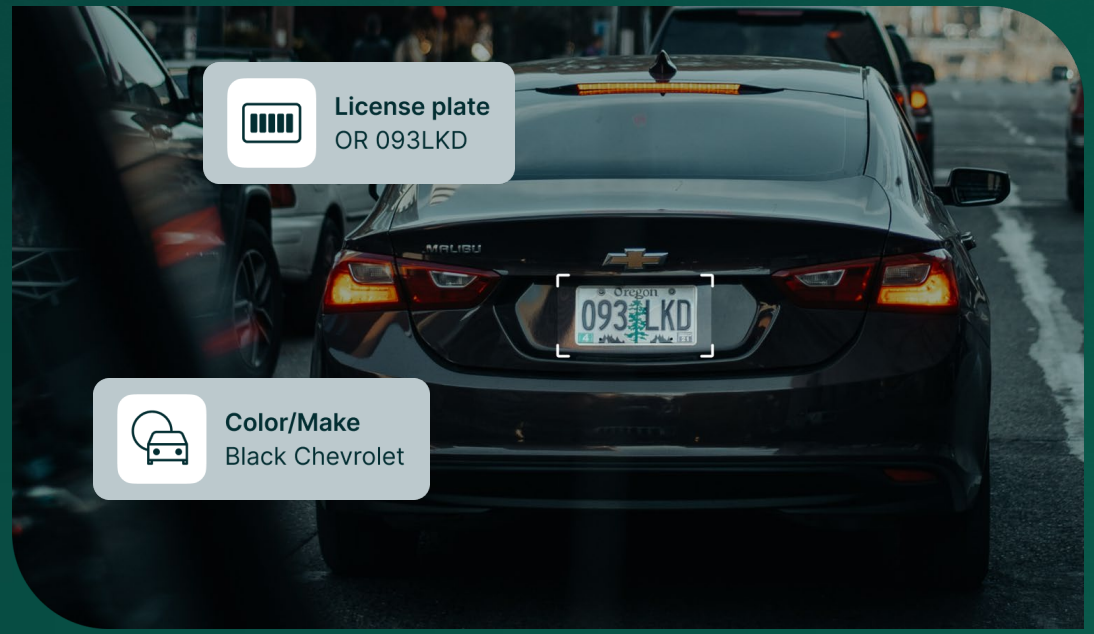
How does the technology work?

flock safety

flock safety

When you get Flock you get:

Flock Safety provides your police department with indiscriminate evidence from fixed locations. We provide all of the maintenance so that your police department and city staff can focus on keeping your city safe and prosperous.



INFRASTRUCTURE-FREE

Reduce time to value and utility costs with full-service deployment.

24/7 COVERAGE

Capture objective vehicle data around the clock to multiply your force.

REAL-TIME ALERTS

- NCIC
- NCMEC (Amber Alert)
- Custom Hot Lists

Ethically Made

- No people
- No facial recognition
- No traffic enforcement
- Indiscriminate evidence

flock safety

What this IS

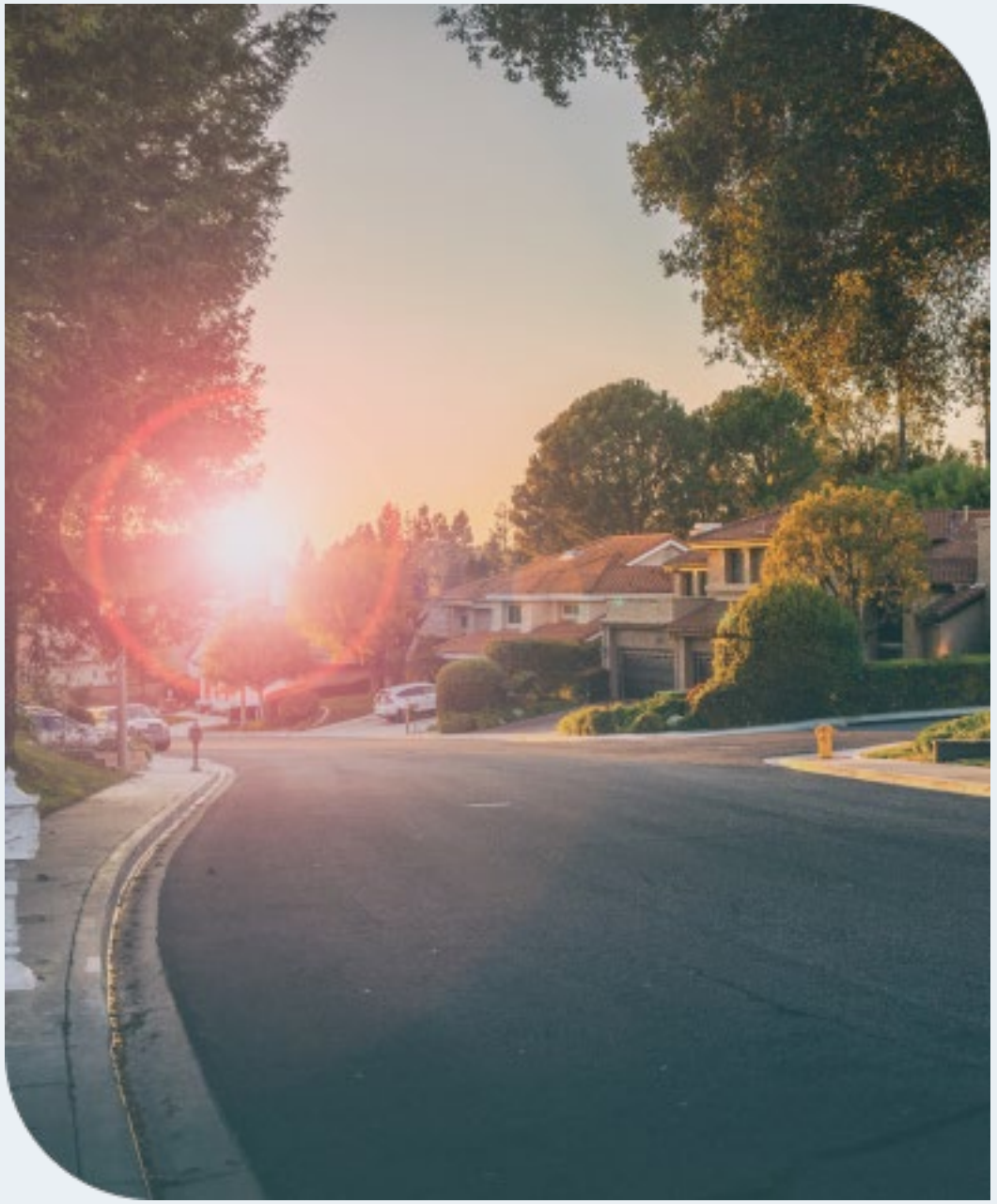
- **License plate recognition**
- **Gathers objective evidence and facts about vehicles, not people**
- **Alerts police of wanted vehicles**
- **Used to solve crime**
- **Adheres to all state laws**

What this is NOT

- Not facial recognition
- **Not tied to Personal Identifiable Information**
- Not used for traffic enforcement
- **Data not stored beyond 30 days → *automatically deletes every 30 days***

How does this technology prevent and eliminate crime?

- **Proactive:** Real time Alerts when stolen or wanted vehicles enter your city
- **Investigative:** As clearance Rates increase, crime rates decrease
- Flock cameras serve as a **deterrent**



flock safety

Mitigating Risk

flock safety

flock safety

Protecting Privacy

- **Footage owned by Agency/City and will never by sold or shared by Flock**
- 30 day data retention, then deleted
- Short retention period ensures that all data not associated with a crime is automatically deleted & unrecoverable
- **Takes human bias out of crime-solving by detecting objective data, and detecting events that are objectively illegal (ex. Stolen vehicles)**

- **All data is stored securely in the AWS Cloud, and end to end encryption of all data**
- **Search reason is required for audit trail**
- NOT facial recognition software
- NOT predictive policing
- NO PII is contained in Flock
- **NOT used for traffic enforcement**
- Not connected to registration data or 3rd party databases (Carfax, DMV)
- Transparency Portal (optional)

flock safety

Transparency + Insights

Measure ROI and promote the ethical use of public safety technology

Transparency Portal

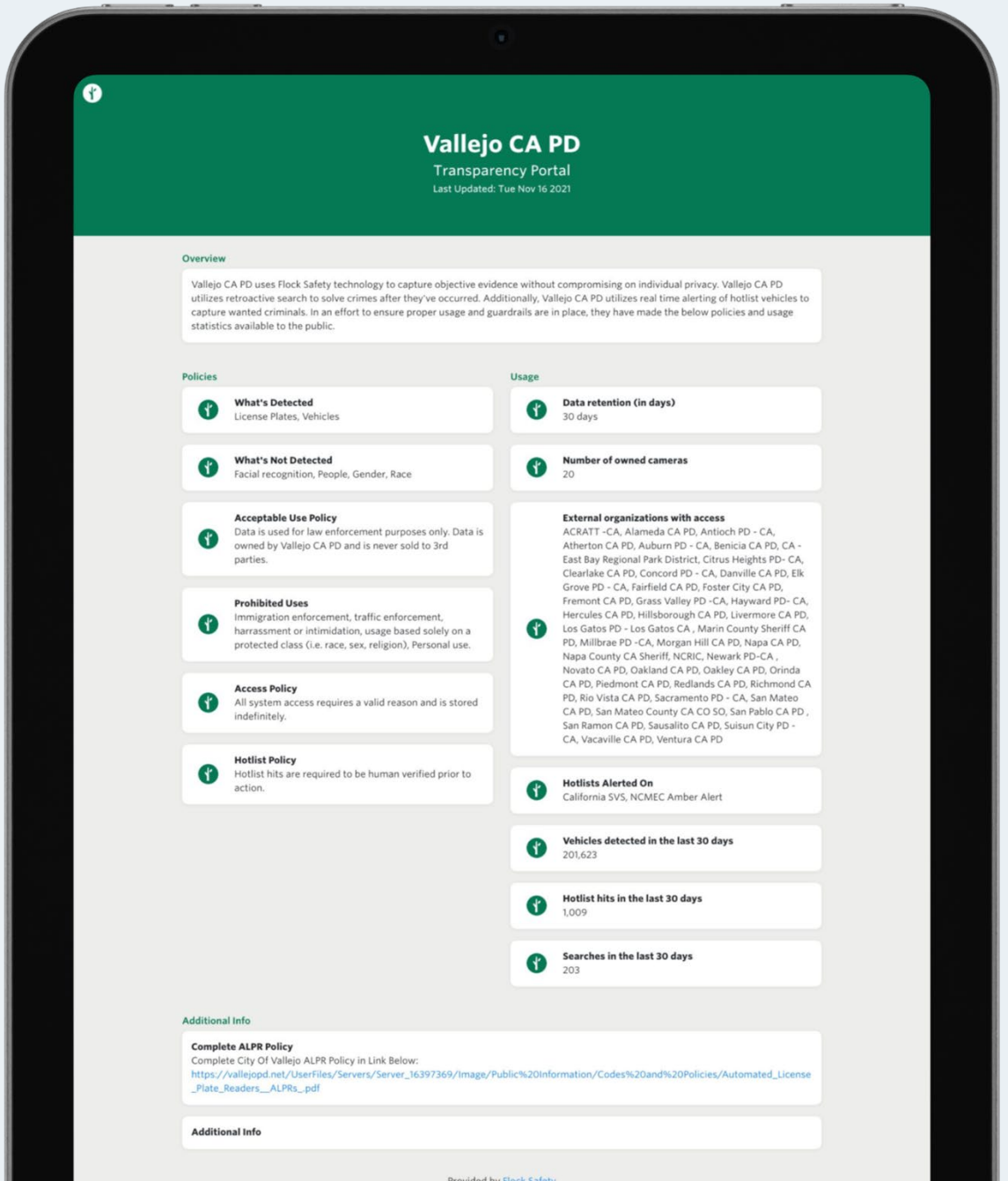
- Customizable for each agency
- Display technology policies
- Publish usage metrics
- Share downloadable Search audits

Insights Dashboard

- Measure crime patterns and ROI
- Audit Search history

Examples

- Click here for Morgan Hill PD
- Click here for Vallejo PD



Already solving and preventing crime

flock safety

Flock Safety In Minnesota

Plus, many more commercial and private customers

Orono PD

West Hennepin DPS

Wayzata PD

Coon Rapids PD

Roseville PD

St. Louis Park PD

Minnetonka PD

Edina PD

Champlin PD

Plymouth PD

S. Lake Minnetonka PD

Robbinsdale PD

Hopkins PD

Ramsey Co SO

Richfield PD

Anoka County SO

Anoka PD

Hudson (WI) PD

Woodbury PD

St. Mary's Point

University of Minnesota PD

Maple Grove PD

St. Louis County SO

Three Rivers Park Dist. Public Safety

Brooklyn Center PD

Paul Bunyan Task Force

Belle Plaine PD

Fridley PD

Mounds View PD

Sartell PD

Fairbault PD

Blaine PD

Medina PD

Willmar PD

Solving Violent Crimes in Wisconsin

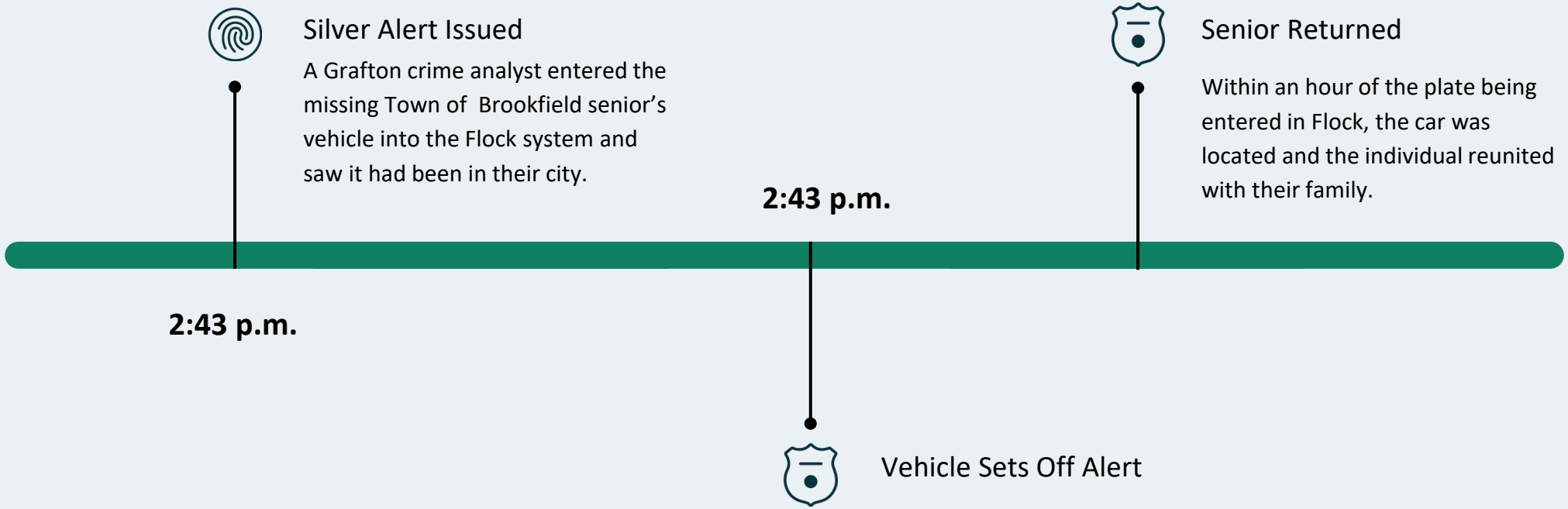
West Allis PD - West Allis, WI

- **Armed robbery:** West Allis officers received an alert that a Kia SUV wanted in connection with an armed robbery in Milwaukee was in the area. Officers initiated a traffic stop but the suspects fled, kicking off a high-speed pursuit that ended in a crash. The three suspects, two of whom had several felony warrants, were arrested.

- **Homicide**: Another alert on a stolen Hyundai sedan came in connection to a Milwaukee homicide. Officers quickly responded but the suspects fled. The chase concluded in Milwaukee where the suspects were arrested.

Missing, Endangered Senior Found in 15 Minutes

Port Washington PD - Port Washington, WI



flock safety

flock safety

Case Study: Smash and Grab Robbery

San Bruno, PD

San Bruno, CA

- January 2022 - Five suspects attempt a Smash & Grab at a Jewelry store but are chased off by the owner
- **But here's what didn't make the news…**
- Suspect vehicle identified using Flock
- SBPD thought the suspects would try again, potentially more violently
- **Vehicle placed on a custom hotlist**
- SBPD receives a real time alert that the suspects are returning
- **Officers locate the vehicle within seconds preventing another attempt**

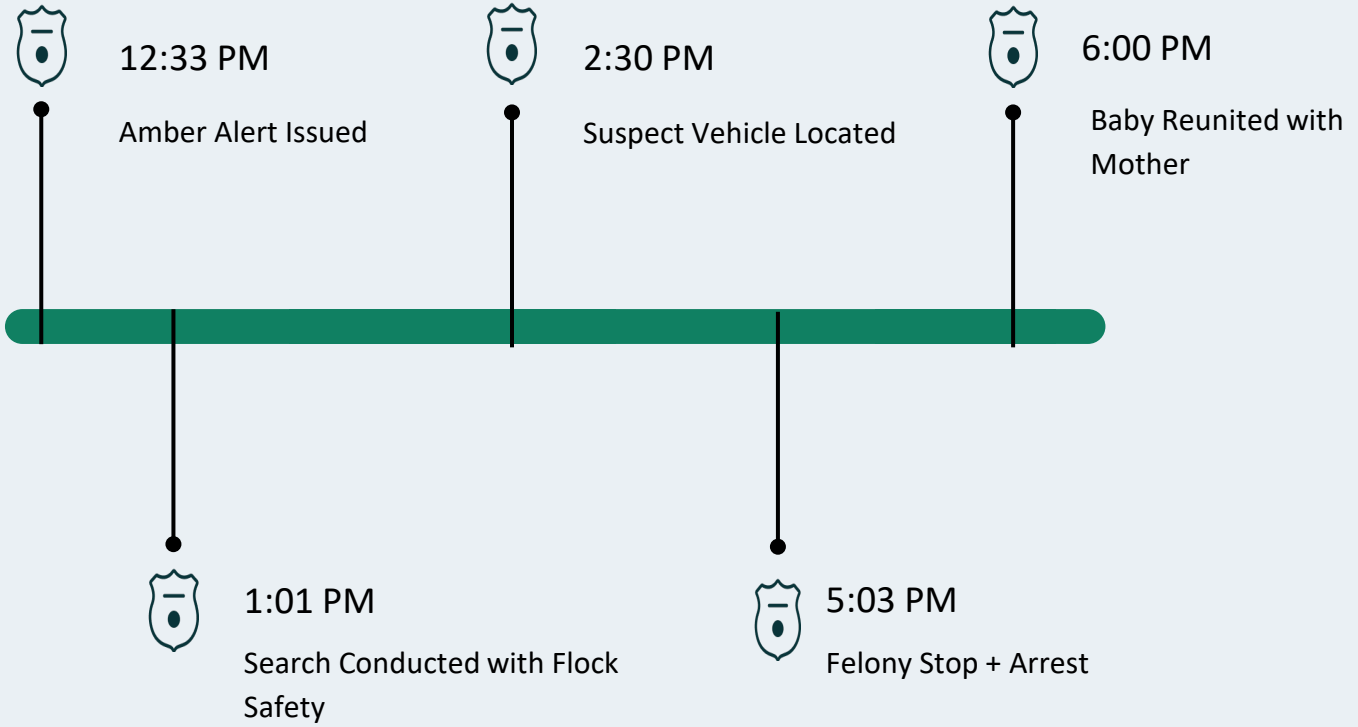
San Bruno jewelry store owner stops attempted smash-and-grab robbery

- ABC 7 News - Bay Area

When Every Second Matters: Child Abduction

Chamblee PD - Chamblee, GA

Stranger on Stranger Abduction
August 28, 2020



QUESTIONS AND FEEDBACK

flock safety™
Let's defeat crime together.™

About Automatic License Plate Readers (ALPR)

The Problem: Violent Crime Is Not Going Away

Nationwide, cities are experiencing a disturbing rise in homicides and violence. The FBI's 2020 Crime Report shows a 30% increase in homicides from 2019 to 2020, the largest single-year increase recorded.

Over two-thirds of the country's most populous cities saw even more homicides in 2021.

One Solution: Technology that Detects Objective Evidence to Clear More Cases

Automated License Plate Readers (ALPR) capture computer-readable images of license plates and vehicles, allowing officers to compare plate numbers against those of stolen cars or wanted individuals on a crime database like the NCIC.

ALPR devices assist law enforcement in solving crime in two ways:

- Proactive - ALPR devices provide real-time alerts when a vehicle that is stolen or associated with a known suspect is detected.
- Investigative - ALPR cameras help determine whether and which vehicle(s) were at the scene of a crime.

Is ALPR effective ?

According to the National Conference of State Legislatures, when employed ethically and objectively, ALPRs are an effective tool for law enforcement, cutting down on the time required for investigations and acting as a force multiplier. In 2011, a study by the Police Executive Research Forum concluded that ALPRs used by the Mesa, Ariz., Police Department resulted in "nearly 3 times as many 'hits' for stolen vehicles, and twice as many vehicle recoveries."

Communities with ALPR systems report crime reductions of up to 70 percent. In some areas, that included a 60 percent reduction in non-residential burglaries, 80 percent reduction in residential burglary, and a 40 percent reduction in robberies.

ALPR Provides Objective Evidence While Protecting Privacy

ALPR does not include facial recognition capabilities and does not capture personally identifiable information (PII). While eyewitnesses and individual officers are subject to inherent human bias, ALPR cameras capture wholly-objective images of vehicles and license plates, providing a clear and actionable investigative lead.

ALPR Use Cases Include:

- AMBER Alerts: License plate readers in metro Atlanta were able to find a vehicle containing a kidnapped one-year-old, who had been taken from his mother at random off the street. The child was recovered unharmed. Some ALPR systems integrate directly with the National Center for Missing and Exploited Children's AMBER Alert system, sending real-time alerts to officers in seconds. [New information released about 1-year-old's kidnapping]

- Silver Alerts: Knoxville Police were able to locate a missing elderly man who suffers from dementia after he drove away in a family vehicle. ALPR technology has helped solve hundreds of Silver Alerts across the country. [Missing man with dementia found using Flock camera]

- Firearm violence: The Las Vegas Trail, a high-crime area in Fort Worth, TX, saw violent crime decrease by 22% in 2021 compared with the first nine months of 2019. Fort Worth Police attributed this drop partially to the license plate reader system implemented in the neighborhood during the same period of time. [Crime is down 22% in Fort Worth's Las Vegas Trail. How neighbors and police made it safer]

- Organized theft: Grafton, a growing village with a bustling retail district, is dealing with increased organized retail theft — Two-thirds of all the crimes reported to Grafton police in 2020 were retail thefts. Grafton Police have implemented a license plate reader system to identify vehicles that have been involved in thefts or have been stolen themselves. In one week alone, they recovered three stolen vehicles with drivers planning to engage in retail theft. [Losses mount as retailers fight theft rings, accuse online storefronts of doing little to stop resale of stolen goods]

flock safety™
Let's defeat crime together.™

About Flock Safety ALPR

Privacy and Ethics Factsheet

How does Flock Safety keep devices and data secure?

Flock Safety holds itself to the highest level of security. We have implemented the following security policies and features:

- Flock Safety data and footage is encrypted throughout its entire lifecycle. All data is securely stored with AES256 encryption with our cloud provider, Amazon Web Services.
- On-device, data is only stored temporarily for a short time until it is uploaded to the cloud, at which point it is removed automatically from the local device. This means the data is secure from when it is on the Flock Safety device to when it is transferred to the cloud, using a secure connection to Flock Safety servers. While stored in the cloud, all data (both footage and metadata) is fully encrypted at rest.
- Flock Safety defaults to permanently deleting all data after 30 days on a rolling basis, setting a new standard in the industry.

Who has access to data collected by Flock Safety devices?

- Flock Safety's customers own 100% of their data and determine who has access. Flock Safety will never share or sell the data, per our privacy policy.
- With explicit written permission from the customer, Flock Safety does have the ability to grant law enforcement access to specific footage for a short period (24 hours, 48 hours, or however long the customer desires) in the event of an investigation following a crime. Access can only be granted through the approval of the customer.
- Flock Safety has maintenance software in place to measure device performance and image capture quality. This is used to diagnose issues preemptively and schedule service calls in the event of a device malfunction or emergency.

flock safety™
Let's defeat crime together.™

About Flock Safety ALPR

Privacy and Ethics Factsheet

How long does Flock Safety keep data?

- Flock Safety stores footage for only 30 days on a rolling basis by default, after which the footage is automatically hard deleted. The only exception to this is if a democratically-elected governing body or official legislates a different data retention period.

What features do Flock Safety devices have that enable audits and oversight?

- While searching for footage or other evidence on the Flock Safety platform, law enforcement agencies must enter reason codes to verify the legitimacy of the search and create an audit trail.
- Authorized users go through training to properly use our system and communicate with their dispatch teams.
- Flock Safety customers commit not to use the data collected to work with third-party repossession companies, traffic enforcement, revenue collection, unpaid fines, or towing companies. We do not use facial recognition or capture any personally identifiable information such as name, phone number, or address, and we do not work with federal government agencies for immigration enforcement purposes.
- Flock Safety's ALPR Transparency Portal, an optional free feature for all law enforcement customers, is the first public-facing dashboard for law enforcement agencies, city leaders, and local government officials to share policies, usage, and public safety outcomes related to ALPR technology. The ALPR Transparency Portal helps promote transparency and accountability in the use of policing technology in order to build community trust while creating a safer, more equitable society.

13.824 AUTOMATED LICENSE PLATE READERS.

Subdivision 1. **Definition.** As used in this section, "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 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.

Subd. 2. **Data collection; classification; use restrictions.** (a) Data collected by an automated license plate reader must be limited to the following:

(1) license plate numbers;

(2) date, time, and location data on vehicles; and

(3) pictures of license plates, vehicles, and areas surrounding the vehicles.

Collection of any data not authorized by this paragraph is prohibited.

(b) All data collected by an automated license plate reader are private data on individuals or nonpublic data unless the data are public under section 13.82, subdivision 2, 3, or 6, or are active criminal investigative data under section 13.82, subdivision 7.

(c) Data collected by an automated license plate reader may only be matched with data in the Minnesota license plate data file, provided that a law enforcement agency may use additional sources of data for matching if the additional data relate to an active criminal investigation. A central state repository of automated license plate reader data is prohibited unless explicitly authorized by law.

(d) Automated license plate readers must not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probable cause, or exigent circumstances justify the use without obtaining a warrant.

Subd. 3. **Destruction of data required.** (a) Notwithstanding section 138.17, and except as otherwise provided in this subdivision, data collected by an automated license plate reader that are not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection.

(b) Upon written request from an individual who is the subject of a pending criminal charge or complaint, along with the case or complaint number and a statement that the data may be used as exculpatory evidence, data otherwise subject to destruction under paragraph (a) must be preserved by the law enforcement agency until the criminal charge or complaint is resolved or dismissed.

(c) Upon written request from a program participant under chapter 5B, automated license plate reader 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 are active criminal investigative data. The existence of a request submitted under this paragraph is private data on individuals.

(d) Data that are inactive criminal investigative data are subject to destruction according to the retention schedule for the data established under section 138.17.

Subd. 4. **Sharing among law enforcement agencies.** (a) Automated license plate reader data that are not related to an active criminal investigation may only be shared with, or disseminated to, another law enforcement agency upon meeting the standards for requesting access to data as provided in subdivision 7.

(b) If data collected by an automated license plate reader 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 of this section.

(c) Automated license plate reader 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 this subdivision or other law.

Subd. 5. **Log of use required.** (a) A law enforcement agency that installs or uses an automated license plate reader must maintain a public log of its use, including but not limited to:

(1) specific times of day that the reader actively collected data;

(2) 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;

(3) for each period of active use, the number of vehicles or license plates in each of the following categories where the data identify 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; and

(4) for a reader at a stationary or fixed location, the location at which the reader actively collected data and is installed and used.

(b) The law enforcement agency must maintain a list of the current and previous locations, including dates at those locations, of any fixed stationary automated license plate readers or other surveillance devices with automated license plate reader capability used by the agency. The agency's list must be accessible to the public, unless the agency determines that the data are security information as provided in section 13.37, subdivision 2. A determination that these data are security information is subject to in-camera judicial review as provided in section 13.08, subdivision 4.

Subd. 6. **Biennial audit.** (a) In addition to the log required under subdivision 5, the law enforcement agency must maintain records showing the date and time automated license plate reader data were collected and the applicable classification of the data. The law enforcement agency shall arrange for an independent, biennial audit of the records to determine whether data currently in the records are classified, how the data are used, whether they are destroyed as required under this section, and to verify compliance with subdivision 7. If the commissioner of administration believes that a law enforcement agency is not complying with this section or other applicable law, the commissioner may order a law enforcement agency to arrange for additional independent audits. Data in the records required under this paragraph are classified as provided in subdivision 2.

(b) The results of the audit are public. The commissioner of administration shall review the results of the audit. If the commissioner determines that there is a pattern of substantial noncompliance with this section by the law enforcement agency, the agency must immediately suspend operation of all automated license plate reader devices until the commissioner has authorized the agency to reinstate their use. An order of suspension under this paragraph may be issued by the commissioner, upon review of the results of the audit, review of the applicable provisions of this chapter, and after providing the agency a reasonable opportunity to respond to the audit's findings.

(c) A report summarizing the results of each audit must be provided to the commissioner of administration, to the chairs and ranking minority members 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.

Subd. 7. **Authorization to access data.** (a) A law enforcement agency must comply with sections 13.05, subdivision 5, and 13.055 in the operation of automated license plate readers, and in maintaining automated license plate reader data.

(b) The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the data only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to data collected by an automated license plate reader for a legitimate, specified, and documented law enforcement purpose. Consistent with the requirements of paragraph (c), each access must be based on a reasonable suspicion that the data are 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.

(c) The ability of authorized individuals to enter, update, or access automated license plate reader 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 are entered, updated, accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail are public, to the extent that the data are not otherwise classified by law.

Subd. 8. **Notification to Bureau of Criminal Apprehension.** (a) Within ten days of the installation or current use of an automated license plate reader or the integration of automated license plate reader technology into another surveillance device, a law enforcement agency must notify the Bureau of Criminal Apprehension of that installation or use and of any fixed location of a stationary automated license plate reader.

(b) The Bureau of Criminal Apprehension must maintain a list of law enforcement agencies using automated license plate readers or other surveillance devices with automated license plate reader capability, including locations of any fixed stationary automated license plate readers or other devices. Except to the extent that the law enforcement agency determines that the location of a specific reader or other device is security information, as defined in section 13.37, this list is accessible to the public and must be available on the bureau's website. A determination that the location of a reader or other device is security information is subject to in-camera judicial review, as provided in section 13.08, subdivision 4.

History: *2015 c 67 s 3; 1Sp2021 c 11 art 3 s 4*

ORONO POLICE DEPARTMENT

"Dedicated to fairness, service, pride and quality"

POLICY: **3059.0**

EFFECTIVE DATE: **July 9, 2020**

REVIEW DATE:

APPROVED BY:

Title: Automated License Plate Recognition System (ALPR)

Distribution: Sworn Personnel

Purpose: The purpose of this policy is to provide guidance on the access, storage and review of the Automated License Plate Recognition System (ALPR) and the use of data collected by the reader as well as the required system audits in accordance with Minn. Stat. 13.824.

3059.01 Policy:

The Orono Police Department recognizes the use of the ALPR as an effective tool to identify vehicles and vehicle owners who are associate with criminal activity and missing and endangered persons.

3059.02 Definitions:

Minnesota State Statute 13.824 defines an ALPR 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. The law enforcement database is updated by the Minnesota 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.

3059.03 Operator's Responsibilities:

1. Use of LPR system shall adhere to department policy 4009.0 (Professional Conduct of Officers).
2. Only officers trained in the proper use of the ALPR may operate it with their own unique login.
3. When an officer receives a "Hit" on the ALPR, the system will alert the officer visually and audibly to the match. The officer must acknowledge that the ALPR read the license plate correctly and verify the "Hit" is current by running the information through the state real-time data system via MDC or dispatch.

4. Prior to taking enforcement action, the officer shall verify that the vehicle description matches that given for the "Hit" vehicle. When a "Hit" is based on the status of the registered owner (i.e., license status, want or warrant) the officer shall also verify that the driver of the vehicle reasonably fits the physical descriptors given for the subject of the "Hit".
5. Proper department procedures and safe police tactics should be followed when initiating a stop or investigation into a "Hit" vehicle.
6. Any issues / problems with the ALPR system should be reported immediately to the ALPR administrator or a supervisor.
7. Any member who willfully violates Minn. Statute 13.09 through the unauthorized acquisition or use of ALPR data may face discipline up to and including termination of employment as well as possible criminal prosecution. (MN Statute 626.8472)

3059.04 Data Collected by an ALPR Must be Limited to the Following:

1. License plate numbers
2. Date, time and location data on vehicles
3. Pictures of license plates, vehicles and areas surrounding the vehicles
4. Collection of any data not authorized above is prohibited
5. Data collected by an automated license plate reader may only be matched with data in the Minnesota license plate data file, provided that a law enforcement agency may use additional sources of data for matching if the additional data relate to an active criminal investigation. A central state repository of automated license plate reader data is prohibited unless explicitly authorized by law.
6. Automated license plate readers must not be used to monitor or track an individual who is the subject of an active criminal investigation unless authorized by a warrant, issued upon probably cause, or exigent circumstances justify the use without obtaining a warrant.

3059.05 Data Storage:

1. 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.
2. 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.

3. 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.

.

3059.06 Authorization to Access Data Shall be Permitted by the Following:

1. The Orono Police Department's written procedure ensures that law enforcement personnel have access to ALPR data if authorized in writing by the Chief of Police, or his/her designee. This access to data collected by an ALPR must be for a legitimate, specified and documented law enforcement purpose.
2. 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.
3. 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, responses and all actions in which data is entered, updated, accessed, shared or disseminated must be recorded in a data audit trail or log.

3059.07 Sharing of Information Among Law Enforcement Agencies:

1. Historical data records date, time, license plate number, GPS location, squad and camera information for each read. Historical data is only searchable for legitimate law enforcement purposes, outlined in above paragraph 3059.06
2. Outside law enforcement requests for historical data shall be routed to the Chief of Police or his/her designee.
3. ALPR data is classified as private, with specific exceptions per Minn. Stat. 13.821.
4. If data collected by an ALPR are shared with another law enforcement agency under this subdivision, the agency that received the data must comply with all data classification, destruction and security requirements.
5. 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.

3059.08 Log of Use

1. Log of use is required to record specific times of day the reader actively collected data.
2. 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.
3. Log of use is required to record the number of vehicles or license plates where 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.
4. 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.
5. A list of the current and previous locations, including dates at those locations, of any fixed ALPR 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.

3059.09 Manual Hot List Content and Use:

1. The ALPR is capable of alerting to license plates entered by the law enforcement agency in the ALPR system and not listed in the Minnesota License Plate Data File. Entries into the ALPR system shall comply with the following procedures and Minn. Stat. 13.824:
    a. A license plate number or partial license plate number shall only be entered in the Orono Police Department's Manual Hot List when there is a legitimate and specific law enforcement reason related to an active criminal investigation to identify or locate that particular vehicle or any person reasonably associated with that vehicle.
    b. Manual Hot List entries may only be made or edited by an ALPR administrator or supervisor.
    c. A Manual Hot List entry shall be removed as soon as practicable if there is no longer a justification for the entry.
    d. If an officer receives an alert based on a Manual Hot List entry, they must follow 3059.03 and confirm that current legal justification exists to take action on the alert.
    e. A Manual Hot List entry may not be used as a substitute for an entry into any other databases such as Minnesota or FBI Hot Files, Nation Crime Information Center (NCIC), or Keeping Our Police Safe (KOPS) files, if appropriate.

3059.10 Biennial Audit

1. 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.
2. 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.

3059.11 Data Requests:

1. Orono Police Department ALPR data that has been collected is classified as private unless access is permitted by law. Citizens can contact the Orono Police Department Records Department to obtain ALPR data on their registered vehicles. This request is reviewed by the Records Manager to ensure that it is consistent with the ALPR Statute 13.824 and Minnesota Data Practices Act, Minnesota Statues, Chapter 13.

3059.12 Notification to the Bureau of Criminal Apprehension:

1. Within 10 days of the installation or current use of an ALPR, or the integration of ALPR technology into another surveillance device, the Minnesota Bureau of Criminal Apprehension must be notified of that installation, or use and any fixed location of a stationary ALPR.

****

Automated License Plate Readers (ALPR)

427.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology (Minn. Stat. § 626.8472).

427.2 POLICY

The policy of the Robbinsdale Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

427.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Robbinsdale Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Captain. The Administration Captain will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

427.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not necessary before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the Minnesota Justice Information Services (MNJIS) and National Law Enforcement Telecommunications System (NLETS) databases before taking enforcement action that is based solely upon an ALPR alert.

427.4.1 RESTRICTIONS, NOTIFICATIONS AND AUDITS

The Robbinsdale Police Department will observe the following guidelines regarding ALPR use (Minn. Stat. § 13.824):

(a) Data collected by an ALPR will be limited to:

1. License plate numbers.
2. Date, time and location of data captured.
3. Pictures of license plates, vehicles and areas surrounding the vehicle captured.

(b) ALPR data may only be matched with the Minnesota license plate data file, unless additional sources are needed for an active criminal investigation.

(c) ALPRs shall not be used to monitor or track an individual unless done so under a search warrant or because of exigent circumstances.

(d) The Bureau of Criminal Apprehension shall be notified within 10 days of any installation or use and of any fixed location of an ALPR.

427.5 DATA COLLECTION AND RETENTION

The Administration Captain is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles and pole-mounted ALPRs to the designated storage in accordance with department procedures.

ALPR data received from another agency shall be maintained securely and released in the same manner as ALPR data collected by this department (Minn. Stat. § 13.824).

ALPR data not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection with the following exceptions (Minn. Stat. § 13.824):

(a) Exculpatory evidence - Data must be retained until a criminal matter is resolved if a written request is made from a person who is the subject of a criminal investigation asserting that ALPR data may be used as exculpatory evidence.

(b) Address Confidentiality Program - Data related to a participant of the Address Confidentiality Program must be destroyed upon the written request of the participant. ALPR data already collected at the time of the request shall be destroyed and future related ALPR data must be destroyed at the time of collection. Destruction can be deferred if it relates to an active criminal investigation.

All other ALPR data should be retained in accordance with the established records retention schedule.

427.5.1 LOG OF USE

A public log of ALPR use will be maintained that includes (Minn. Stat. § 13.824):

(a) Specific times of day that the ALPR collected data.

(b) 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 public databases with which the data were compared.

(c) For each period of active use, the number of vehicles or license plates related to:

1. A vehicle or license plate that has been stolen.
2. A warrant for the arrest of the owner of the vehicle.
3. An owner with a suspended or revoked driver's license or similar category.
4. Active investigative data.

(d) For an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

A publicly accessible list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance devices with ALPR capability shall be maintained. The list may be kept from the public if the data is security information as provided in Minn. Stat. § 13.37, Subd. 2.

427.6 ACCOUNTABILITY

All saved data will be closely safeguarded and protected by both procedural and technological means. The Robbinsdale Police Department will observe the following safeguards regarding access to and use of stored data (Minn. Stat. § 13.824; Minn. Stat. § 13.05):

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) Biennial audits and reports shall be completed pursuant to Minn. Stat. § 13.824, Subd. 6.

(d) Breaches of personal data are addressed as set forth in the Protected Information Policy (Minn. Stat. § 13.055).

(e) All queries and responses, and all actions, in which data are entered, updated, accessed, shared or disseminated, must be recorded in a data audit trail.

(f) Any member who violates Minn. Stat. § 13.09 through the unauthorized acquisition or use of ALPR data will face discipline and possible criminal prosecution (Minn. Stat. § 626.8472).

427.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures (Minn. Stat. § 13.824):

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.
4. A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
5. A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.

(b) The request is reviewed by the Administration Captain or the authorized designee and approved before the request is fulfilled.

1. A release must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.

Automated License Plate Readers (ALPR)

427.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology (Minn. Stat. § 626.8472).

427.2 POLICY

The policy of the Rochester Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

427.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the Rochester Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Services Captain in coordination with the Intelligence and Crime Analysis Unit (Intel).The Intel Lieutenant will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

System administrators shall:

(a) Provide or oversee the training of all officers and civilian employees who are authorized to operate an ALPR or to access or use ALPR stored data.

(b) Review and approve requests to access and use stored ALPR data.

(c) Ensure compliance with this directive and all state and federal laws.

427.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official law enforcement business and in accordance with the law.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not necessary before using an ALPR.

(c) An ALPR may be used to canvass license plates around major crime scenes or an area of repeated minor offenses. Captured data can be analyzed and utilized in any active criminal investigation.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) An officer shall verify an ALPR response through the Minnesota Justice Information Services (MNJIS) and National Law Enforcement Telecommunications System (NLETS) databases before taking enforcement action that is based solely upon an ALPR alert.

427.4.1 RESTRICTIONS, NOTIFICATIONS AND AUDITS

The Rochester Police Department will observe the following guidelines regarding ALPR use (Minn. Stat. § 13.824):

(a) Data collected by an ALPR will be limited to:

1. License plate numbers.
2. Date, time and location of data captured.
3. Pictures of license plates, vehicles and areas surrounding the vehicle captured.

(b) ALPR data may only be matched with the Minnesota license plate data file, unless additional sources are needed for an active criminal investigation.

(c) ALPRs shall not be used to monitor or track an individual unless done so under a search warrant or because of exigent circumstances.

(d) The Bureau of Criminal Apprehension shall be notified within 10 days of any installation or use and of any fixed location of an ALPR.

427.5 DATA COLLECTION AND RETENTION

The Services Captain, in conjunction with the Intelligence and Crime Analysis (Intel) Lieutenant, are responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

ALPR data received from another agency shall be maintained securely and released in the same manner as ALPR data collected by this department (Minn. Stat. § 13.824).

ALPR data not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection with the following exceptions (Minn. Stat. § 13.824):

(a) Exculpatory evidence - Data must be retained until a criminal matter is resolved if a written request is made from a person who is the subject of a criminal investigation asserting that ALPR data may be used as exculpatory evidence.

(b) Address Confidentiality Program - Data related to a participant of the Address Confidentiality Program, such as the Safe at Home program, must be destroyed upon

the written request of the participant. ALPR data already collected at the time of the request shall be destroyed and future related ALPR data must be destroyed at the time of collection. Destruction can be deferred if it relates to an active criminal investigation.

All other ALPR data should be retained in accordance with the established records retention schedule.

427.5.1 LOG OF USE

A public log of ALPR use will be maintained that includes (Minn. Stat. § 13.824):

(a) Specific times of day that the ALPR collected data.

(b) 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 public databases with which the data were compared.

(c) For each period of active use, the number of vehicles or license plates related to:

1. A vehicle or license plate that has been stolen.
2. A warrant for the arrest of the owner of the vehicle.
3. An owner with a suspended or revoked driver’s license or similar category.
4. Active investigative data.

(d) For an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

A publicly accessible list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance devices with ALPR capability shall be maintained. The list may be kept from the public if the data is security information as provided in Minn. Stat. § 13.37, Subd. 2.

427.5.2 ALPR HOTLISTS

A hotlist record may be created when a determination is made by the Rochester Police Department or another law enforcement agency there is a legitimate and specific law enforcement purpose to identify or locate a particular vehicle related to an active criminal investigation.

For purpose of the ALPR, a Hot list may be maintained that consists of a compilation of one or more license plates, or partial license plates, of a vehicle or vehicles for which a BOLO situation exists. A Hotlist may be programed into an ALPR so that the device will alert if it captures the image of a license plate that matches a BOLO list entry.

Hotlists shall only be comprised of license plates that are associated with specific vehicles or persons for which or whom there is a legitimate and documented law enforcement reason to identify and locate, or for which there is a legitimate and documented law enforcement reason to determine the subject vehicle's past location(s) through the analysis of stored ALPR data. The legitimate law enforcement purpose will be affirmed with the use an ICR number.

Examples of legitimate and specific reasons for adding a license plate or partial license plate to a BOLO list include, but are not limited to:

(a) Persons who are subject to an outstanding arrest warrant

(b) Missing persons

(c) Amber or Silver Alerts

(d) Stolen vehicles

(e) Vehicles that are reasonably believed to be involved in the commission of a crime

(f) Vehicles that are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list

(g) Persons who are subject to a restraining order or curfew issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements

(h) Persons wanted by a law enforcement agency who are of interest in a specific investigation, whether or not such persons are themselves suspected of criminal activity

(i) Persons who are on any watch list issued by a State or federal agency responsible for homeland security

Hotlist information may be downloaded in batch form from other databases, including but not limited to the National Crime Information Center (NCIC), National Insurance Crime Bureau, United States Department of Homeland Security, and Motor Vehicle Commission database.

A Hot list may be revised at any time necessitating frequent updates. For a mobile ALPR, updates to the Hotlist shall be made at the start of each shift. A stationary ALPR positioned at a fixed location shall be updated as frequently as practicable, but no less than on a daily basis.

Officers alerted to the fact that an observed motor vehicle's license plate is on the Hot list may be required to make a reasonable effort to determine if a lawful basis to stop the vehicle exists. An officer reacting to an alert shall consult the database to determine the reason why the vehicle had been placed on the Hot list and whether the alert has been designated as a non-encounter alert. In the event of a non-encounter alert, the officer shall follow any instructions included in the alert for notifying the law enforcement or homeland security agency that had put out the BOLO.

See attachment: ALPR Procedure.pdf

427.6 ACCOUNTABILITY

All saved data will be closely safeguarded and protected by both procedural and technological means. The Rochester Police Department will observe the following safeguards regarding access to and use of stored data (Minn. Stat. § 13.824; Minn. Stat. § 13.05):

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data

relate to a specific criminal investigation or department-related civil or administrative action.

(c) Biennial audits and reports shall be completed pursuant to Minn. Stat. § 13.824, Subd. 6.

(d) Breaches of personal data are addressed as set forth in the Protected Information Policy (Minn. Stat. § 13.055).

(e) All queries and responses, and all actions, in which data are entered, updated, accessed, shared or disseminated, must be recorded in a data audit trail.

(f) Any member who violates Minn. Stat. § 13.09 through the unauthorized acquisition or use of ALPR data will face discipline and possible criminal prosecution (Minn. Stat. § 626.8472).

427.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures (Minn. Stat. § 13.824):

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.
4. A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
5. A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.

(b) The request is reviewed by the Services Captain or the authorized designee and approved before the request is fulfilled.

1. A release must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy. All data collected by ALPR’s is classified as private data on individuals, until it is determined that the data should be classified as public data by the Minnesota Government Data Practices Act.

Attachments

ALPR Procedure.pdf

427.5.2 ROCHESTER POLICE DEPARTMENT ALPR HOTLIST PROCEDURE

A. This procedure has been established to ensure proper accountability of the RPD ALPR Hotlist.

B. All Officers/Staff using ALPR must complete policy acknowledgement and training prior to use.

C. All Officers are able to make additions/deletions to the RPD ALPR Hotlist. It is imperative that the RPD ALPR Hotlist only contain valid and current records.

D. Procedure for ALPR list entry:

1. Officer/Staff determine if they have proper vehicle information available and have satisfied the established ALPR Hotlist entry criteria.
2. Officers/Staff shall inform their supervisor of their intention to include a record on the RPD ALPR hotlist.
3. Officers/Staff enter license plate record using the evidence.com hotlist records management.
4. Officers/Staff include the associated ICR# along with the subject and reason for entry in the "NOTE" box when creating a new record.
   Example: 2023-99999999 John Jacob Doe DOB 4/4/88 PC arrest for Domestic Assault.
5. All RPD ALPR Hotlist entries shall be properly categorized and receive "HIGH" priority.
6. Officers/Staff shall inform all Police Sworn Officers of the entry to the ALPR Hotlist via email using the special information bulletin email template.

E. Procedure for BOLO list removal and documentation:

1. Officers/Staff delete license plate records using evidence.com hotlist records management.
2. An Officer that takes action after being alerted by an ALPR hit is required to ensure that the record is deleted once it is no longer valid.
3. Officers/Staff shall convert the ALPR Hit record to evidence in evidence.com.

F. An ALPR Records search may be executed by all department personnel that have the appropriate evidence.com access and a valid law enforcement purpose. Associated RPD ICR#'s are required for each search.

G. Procedure for ALPR Records search.

1. Enter full/partial license plate information in the plate number field of evidence.com.
2. Include appropriate search criteria.
3. Include RPD (or appropriate agency) ICR# in the search reason box.

H. All Officers are required to ensure that records included on the hotlists (RPD and NCIC) are valid prior to taking enforcement action.

I. The RPD APLR Hotlist is managed managed by the RPD Intelligence and Crime Analysis Unit. In addition, Patrol Supervisors shall ensure that the RPD ALPR Hotlist is valid and current on a daily basis.

flock safety

Let's defeat crime together

Help your city reduce crime with cameras that see like a detective

"Flock Safety made my job easy. The system was up and running in just a few weeks, and has proven to help our police department find the evidence to solve more crime."

City Manager in Ohio

Flock Safety provides an affordable, infrastructure-free automatic license plate reading (ALPR) camera system for cities who want to reduce crime within a principled framework. Unlike traditional ALPR, Flock uses Vehicle Fingerprint™ technology to transform hours of footage into a searchable database to find the single piece of evidence needed, even when a license plate isn't visible.

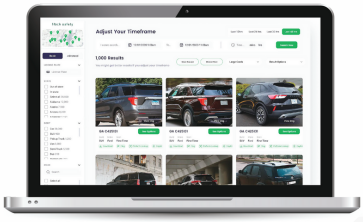
Not your average security cameras

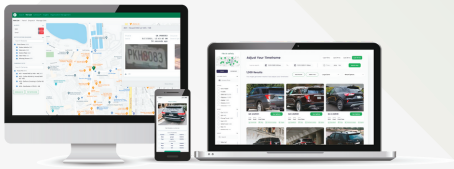
Infrastructure-Free and Discreet Design
With solar power and LTE connectivity, we can install the devices almost anywhere. And the beautiful design means it will blend in with your city's aesthetic.

Safety-as-a-Service
We install and maintain the devices, so you can focus on running the city. That means we will support you from procurement, through permitting, and even preparing you to present this project to the city council.

Vehicle Fingerprint Technology
Your officers can find vehicle evidence by vehicle type, make, color, license plate state, missing and covered plates, and other unique features like bumper stickers, decals, and roof racks.

Join 2500+ cities using Flock Safety to eliminate crime





Detect

objective evidence your police need to solve crime

Decode

footage with machine learning so your police can investigate

Deliver

real-time alerts to police if a wanted or stolen vehicle drives by

Public Safety Technology Built with Principles

You own the footage
We won't share it or sell it. It's 100% yours for your law enforcement to use to solve crime.

Protect resident privacy
All data automatically deletes by default every 30 days on a rolling basis and is encrypted with AES-256 encryption.

Promote transparency and accountability
Flock provides a transparency portal to share data with your community about how the devices work on an ongoing basis. Flock requires an investigative reason to search and proactively provides an audit report to city leadership.

Clear pricing and infrastructure free
$2500 per camera / year. All the footage is stored in the cloud at no additional fee and there are no hidden costs.

Protect the Whole Community
It takes all community members working together to eliminate crime, which is why we created a public-private partnership that enables businesses, neighborhoods, schools, and others to partner with your city and police department to build your network.

Learn More:

"Flock Safety continues to enhance and help our police department capture these vehicles and return the assets to their owners."

-Council member Josh McCurn of Lexington, KY

Automated License Plate Readers (ALPR)

425.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology (Minn. Stat. § 626.8472).

425.2 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the West Hennepin Public Safety to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Administration Sergeant. The Administration Sergeant will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

425.3 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose.

(a) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not necessary before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) No ALPR operator may access confidential department, state or federal data unless authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the Minnesota Justice Information Services (MNJIS) and National Law Enforcement Telecommunications System (NLETS) databases before taking enforcement action that is based solely upon an ALPR alert.

425.3.1 RESTRICTIONS, NOTIFICATIONS AND AUDITS

The West Hennepin Public Safety will observe the following guidelines regarding ALPR use (Minn. Stat. § 13.824):

(a) Data collected by an ALPR will be limited to:

1. License plate numbers.
2. Date, time and location of data captured.
3. Pictures of license plates, vehicles and areas surrounding the vehicle captured.

(b) ALPR data may only be matched with the Minnesota license plate data file, unless additional sources are needed for an active criminal investigation.

(c) ALPRs shall not be used to monitor or track an individual unless done so under a search warrant or because of exigent circumstances.

(d) The Bureau of Criminal Apprehension shall be notified within 10 days of any installation or use and of any fixed location of an ALPR.

425.4 DATA COLLECTION AND RETENTION

The Administration Sergeant is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

ALPR data received from another agency shall be maintained securely and released in the same manner as ALPR data collected by this department (Minn. Stat. § 13.824).

ALPR data not related to an active criminal investigation must be destroyed no later than 60 days from the date of collection with the following exceptions (Minn. Stat. § 13.824):

(a) Exculpatory evidence - Data must be retained until a criminal matter is resolved if a written request is made from a person who is the subject of a criminal investigation asserting that ALPR data may be used as exculpatory evidence.

(b) Address Confidentiality Program - Data related to a participant of the Address Confidentiality Program must be destroyed upon the written request of the participant. ALPR data already collected at the time of the request shall be destroyed and future related ALPR data must be destroyed at the time of collection. Destruction can be deferred if it relates to an active criminal investigation.

All other ALPR data should be retained in accordance with the established records retention schedule.

425.4.1 LOG OF USE

A public log of ALPR use will be maintained that includes (Minn. Stat. § 13.824):

(a) Specific times of day that the ALPR collected data.

(b) 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 public databases with which the data were compared.

(c) For each period of active use, the number of vehicles or license plates related to:

1. A vehicle or license plate that has been stolen.
2. A warrant for the arrest of the owner of the vehicle.
3. An owner with a suspended or revoked driver's license or similar category.
4. Active investigative data.

(d) For an ALPR at a stationary or fixed location, the location at which the ALPR actively collected data and is installed and used.

A publicly accessible list of the current and previous locations, including dates at those locations, of any fixed ALPR or other surveillance devices with ALPR capability shall be maintained. The list may be kept from the public if the data is security information as provided in Minn. Stat. § 13.37, Subd. 2.

425.5 ACCOUNTABILITY

All saved data will be closely safeguarded and protected by both procedural and technological means. The West Hennepin Public Safety will observe the following safeguards regarding access to and use of stored data (Minn. Stat. § 13.824; Minn. Stat. § 13.05):

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time.

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) Biennial audits and reports shall be completed pursuant to Minn. Stat. § 13.824, Subd. 6.

(d) Breaches of personal data are addressed as set forth in the Protected Information Policy (Minn. Stat. § 13.055).

(e) All queries and responses, and all actions, in which data are entered, updated, accessed, shared or disseminated, must be recorded in a data audit trail.

(f) Any member who violates Minn. Stat. § 13.09 through the unauthorized acquisition or use of ALPR data will face discipline and possible criminal prosecution (Minn. Stat. § 626.8472).

425.6 POLICY

The policy of the West Hennepin Public Safety is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

425.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures (Minn. Stat. § 13.824):

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.
4. A record of the factual basis for the access and any associated case number, complaint or incident that is the basis for the access.
5. A statement that the request is authorized by the head of the requesting law enforcement agency or his/her designee.

(b) The request is reviewed by the Administration Sergeant or the authorized designee and approved before the request is fulfilled.

1. A release must be based on a reasonable suspicion that the data is pertinent to an active criminal investigation.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy.