

Meeting Minutes
Town of Indialantic
Regular Meeting of the Town Council
Council Chamber, 216 Fifth Avenue, Indialantic, FL 32903
Wednesday, January 11, 2023, at 7:00 p.m.

A. Call to Order:

A regular meeting of the Indialantic Town Council was called to order by Mayor McDermott at 7:00 p.m. with the following members present:

Honorable Mark McDermott, Mayor
Honorable Stu Glass, Deputy Mayor
Honorable Doug Wright, Councilmember
Honorable Loren Strand, Councilmember

Also present:

Michael Casey, Town Manager
Paul Gougelman, Town Attorney
Rebekah Raddon, Town Clerk
Michael Connor, Chief of Police
Sgt. Dovel, Police Dept.
Sgt. Weber, Police Dept.
Officer Sweeney, Police Dept.
Capt. Burnett, Fire Dept.
David Murtha, Fire Dept.

Mayor McDermott led the Pledge of Allegiance followed by a moment of silence to reflect on the recent passing of Vincent Benevente, who served on the town council for 14 years as well as several town boards and committees.

Police Chief Connor introduced Indialantic's newest police officer, Kevin Sweeney. Officer Sweeney served in the US Army for 20 years before working for the West Melbourne Police Department. Officers Sweeney and Dovel departed the meeting.

1. Mayor McDermott suggested changes to the order of items on the agenda: he would like to read public announcements and discuss New Business Item #7 Manatee Hustle 5K prior to the Flock Safety automated license plate reader presentation.
2. Mayor McDermott read the following Public Announcements:
 - There are openings on the following boards and committees: Board of Adjustment; Budget and Finance; Civil Service; and the Fifth Avenue Study Committee

- Town Hall will be closed on Monday, Jan. 16, in observance of Martin Luther King Jr. Day
- Annual beach parking permits for 2023 are available at Town Hall; bring current vehicle registration and \$40. Residency is not required to purchase.

Agenda item New Business #7. Approve/Designate Special Event Manatee Hustle 5k:

Discussion ensued; concerns were raised over the potential for traffic issues and short notice provided by race organizers. Paul Gougelman advised that the certificate of insurance is a meaningless document and the only way to ensure coverage is to obtain a copy of the full policy showing the Town as additional insured.

Motion by Councilmember Wright, seconded by Councilmember Strand to designate and approve the special event Manatee Hustle 5K.

Motion carried 3-1; nay vote by Deputy Mayor Glass.

Agenda item A. 1. Presentations: Automated License Plate Readers by Flock Safety:

Police Chief Connor advised that four license plate reading cameras were installed in Town recently to aid in solving crime. He invited Flock Safety representative Laura Holland to speak.

Ms. Holland gave a Powerpoint¹ presentation and spoke at length regarding automated license plate readers and answered numerous questions from the councilmembers and residents. In summary, the Automated License Plate Readers (ALPRs) take a still image of the back of each vehicle and record the plate information, vehicle type, body, and color. No biometric information is captured. The data is not used for traffic enforcement, and is automatically deleted in 30 days. Data is never sold or shared, and there is no third party. When information is accessed by law enforcement, the user name and reason for accessing the information is recorded for transparency and accountability. Ms. Holland noted the importance of Chief Connor's written policy² for use of the ALPR system. She gave real-life examples of how the ALPR system has solved crimes such as car-jacking, murder, and child abduction.

Councilmembers held lengthy discussion; in summary, they raised concerns regarding the struggle for laws to keep up with technology; the possibility of opting out of the program and the legislation necessary to do so; cyber security and the potential for hacking, and the potential for information to be used for other purposes. Chief Connor explained his policies and procedures for how the system would be utilized and advised that in Indian River County, it will be particularly helpful for solving vehicle and residential burglaries. He advised that his policy is more stringent than FDLE's policy and he gave examples of crimes that were solved here utilizing data from the ALPR's.

Public Comments:

Kevin McMahon, 440 First Avenue, is not opposed to the use of ALPR's but expressed concerns regarding where the data lives and how it will move between agencies. He feels AWS is not secure.

John Greco, 418 Seventh Avenue, inquired how one would opt out of the program after data has already been collected. He feels that is just giving people false hope. He inquired about worst-case scenarios happening as a result of using ALPRs.

Marquita Fuchs, Tampa Avenue, worries about crime in other areas and inquired about how the data is coordinated between jurisdictions as she has been accosted in other cities.

Lee Guthrie, 201 Melbourne Avenue, received confirmation that other cities have or will soon have ALPR's, and that they are in use currently in Indialantic. She inquired if it is necessary to have ALPR's in Indialantic since other cities have them, and suggested information be posted online.

Mayor McDermott asked to have Flock Safety's transparency portal added to the Town's website.

Vinnie Taranto, 330 Tenth Terrace, inquired about blurring out portions of images to maintain privacy. He inquired about portal or back-end access, and advised that all devices have IP addresses.

Loren Goldfarb, 320 DeLand Avenue asked for clarification regarding images; he inquired if they are kept for 30 days or if the Town owns them; if the town owns them then the Town sets the policy for how long they are kept.

Ms. Holland answered the questions posed during public comment and council discussion resumed, in particular regarding "opting out". One individual noted that "opting out" is meaningless unless the person never leaves Indialantic, since other jurisdictions have them in place.

Dick Dunn, 330 Tampa Avenue, noted that information regarding the license plate will have to be collected in order to opt out.

Dave Berkman, 225 Eighth Avenue, inquired about what owning the data means because the data is shared between agencies.

Brett Miller, 220 Cocoa Avenue, inquired if the technology is capable of doing facial recognition, and noted that it is a slippery slope as contracts can be amended.

B. Consent Agenda:

1. Approve Council Meeting Minutes 12-7-2022

2. Approve/designate special event Craft Fair (TNT Events, Inc) in Nance Park from 10 a.m. – 5 p.m., Feb. 25-26; authorize park closure
3. Approve Res. 01-2023 Supporting the Florida League of Cities Legislative Platform (Glass)
4. Approve \$7,675.20 firefighter assistance grant for thermal imaging camera

Motion by Deputy Mayor Glass to approve the consent agenda. Councilmember Strand requested item #4 firefighter assistance grant be pulled for discussion.

Deputy Mayor Glass amended his motion, approving consent agenda items 1-3. Councilmember Wright seconded the amended motion which passed unanimously, 4-0.

Councilmember Strand inquired if the firefighter grant required matching funds; Mr. Casey advised that it did not.

Motion by Councilmember Strand, seconded by Deputy Mayor Glass, and vote unanimous to approve Consent Agenda item #4 Firefighter assistance grant for thermal imaging camera. Motion carried 4-0.

C. Ordinances and Public Hearings: (None)

D. Unfinished Business: (None)

E. New Business:

1. Automated License Plate Reading – Flock Safety

Town Attorney Gougelman spoke regarding legal aspects of ALRPs and advised that the law would likely look favorably on ALRPs since photos are taken in the public domain on a public street. Lengthy discussion ensued. Councilmembers expressed concerns, in particular regarding being left out of the process as the item was not discussed in a council meeting. It was noted that the funds to pay for the ALRPs and operate them for one year were paid for by an anonymous donation. It was also noted that not all purchases go before council for approval. There was discussion regarding allowing the town manager the discretion to do his job while providing accountability and checks and balances. Mr. Gougelman described purchasing pencils as entering into a legal contract, and advised the council that they can set parameters for the manager and also for him with regard to how much legal review they would like.

Public Comments:

Dick Dunn, 330 Tampa Avenue, commented that this item should have been brought to the town council because it affects residents. It is different than replacing windows or fire rescue equipment. Guidance from town council should be sought for anything affecting residents and the manager should consult the attorney if there is uncertainty.

Loren Goldfarb, 320 DeLand Avenue, has no issues with the cameras but is concerned that this wasn't put on an agenda. For comparison, he pointed out that the firefighter assistance grant for a thermal imaging camera was on tonight's agenda for council's approval. He feels residents deserve open debate and commented that even repetitive, annual purchases such as lawn maintenance are put on the agenda, so a binding contractual agreement for ALPR's should be.

Carrie Foy, 235 Wayne Avenue, inquired if someone "opts out" and their car is stolen, then what happens? She advised that she has cameras on her property and anyone going to Publix is recorded and she keeps that data forever, and can share with law enforcement if she wishes. She noted that anyone outside in public should assume they are being seen and recorded. She supports the use of ALPRs. She feels the unintended consequences of requiring council to review and approve everything is that people may be less likely to donate funds to the town. She trusts the town manager and department heads to make decisions that are in the best interest of the town. She feels some posts on social media written by an elected official promoted controversy on the topic.

Brett Miller, 220 Cocoa Avenue, feels that everyone involved had good intentions but installing ALPRs is a policy decision which must be brought to the town council. Anything affecting residents' constitutional rights is a policy decision, not a managerial decision.

Dick Dunn, 330 Tampa Avenue, inquired about the location of the cameras and confirmed that the cameras cannot be used to perform a traffic study.

Vinnie Taranto, 330 Tenth Terrace, advised that purchases over \$5,000, anything affecting civil liberties, and/or additional functions of the police department should be brought to town council for approval.

Jim Vaidic, 110 Melbourne Avenue, received confirmation that the donation provided funding for installation and a year of service, and future years would be budgeted unless the donor decides to continue funding it.

Anita Mueller, 610 S Miramar, is a new resident and safety is very important to her. She would hate to see something like the Idaho murders take place here and not have the ability to solve crimes. She noted that the vehicle was the biggest piece of evidence in that case and it took 6 weeks to find it.

Chief Connor read a portion of an affidavit regarding that case, noting that the vehicle was spotted via an ALPR in California.

Town Manager Casey advised that in hindsight, knowing the town's reaction, he would have put this item on the agenda even though he's not legally obligated too.

There was consensus about writing a policy; Mr. Gougelman indicated he would like to collaborate individually with the mayor and Councilmember Wright on a draft. Councilmember Strand would like to see the “opt out” addressed.

2. Request for Rectangular Rapid Flashing Beacon (RRFB) at S. Miramar Ave. and Eleventh Ave.
Mr. Casey advised that this topic needs to be researched more and will be on a future agenda.
3. Promotion/utilization of the Everbridge Emergency Alert Notification System
Councilmember Strand would like to increase the number of residents signed up for the emergency notification system as only 30% have opted to receive alerts. Most people don’t know about it and he would like to do more outreach.

Lengthy discussion ensued regarding ways the town keeps residents informed which includes such as social media, mailers and newsletters, the website, and Benchmark emails. Deputy Mayor Glass urged the council to watch the Florida League of Cities webinars. He would like to have the town’s Social Media policy reviewed next month as it ties into the topic.

Motion by Councilmember Strand, seconded by Councilmember Wright, to authorize the town manager to develop a strategy and action plan to improve awareness of the alert system to residents, provide for direct discussion with residents who are not subscribed about the benefits, how to subscribe and, if needed, direct assistance subscribing, improve the timeliness, type and content of messages sent from the alert system, and provide adequate cross training and documentation of the alert system.

Public Comments:

Gabrielle Strand, 120 Ormond Drive, spoke regarding outreach to residents. People are familiar with the county system but don’t know about our local notification system.

Loren Goldfarb, 320 DeLand Avenue, urged everyone to look at best practices. We are a small enough town that we can go door to door. No one reads the newsletter, emails aren’t effective, and social media is full of nonsense. He encouraged a texting based notification system. He feels people won’t mind receiving texts.

It was noted that Everbridge is for disseminating emergency information.

Lee Guthrie, 201 Melbourne Avenue, suggested a tab on the home page titled “How to get information...” She prefers to receive information by text and likes to have numerous reminders.

Motion carried unanimously, 4-0.

4. Benchmark email mailing lists

Mayor McDermott suggested separate email distribution lists for Council Agendas, Council Meeting Minutes, Town Manager notes, and a Mayor's Update. No consensus was reached.

5. Beach Parking Permits for Town Employees

Deputy Mayor Glass received a request from town staff that they be allotted two beach parking permits at no charge. Staff are currently allotted one free pass per year whereas elected officials and board/committee members are allotted two free passes. Employees are good stewards of the beaches and this would be an additional benefit for them and their families.

Motion by Deputy Mayor Glass, seconded by Councilmember Wright, and vote unanimous to approve two beach parking decals for town employees. Motion carried 4-0.

6. Regular town council meeting schedule

Brief discussion ensued regarding the unusual town meeting schedule which currently has the town council meeting on the "Wednesday preceding the second Thursday of each month." Town Clerk Raddon noted that it is confusing for residents to try to remember and changing it to the second Wednesday of the month would be much simpler. She added that changing the meeting time to 6:00 p.m. would also be beneficial. She advised that most municipalities in Brevard County have earlier starting times for their council meetings.

Motion by Mayor McDermott, seconded by Councilmember Strand, and vote unanimous to approve drafting an ordinance changing the town council meeting schedule. Motion carried 4-0.

It was noted the time of the meetings could be adopted by resolution. [Drafter's note: It was determined later that both the date and time will be adopted by ordinance].

7. Approve/Designate Special Event: Manatee Hustle 5K – This item was discussed after Public Announcements.

F. Public Comments, Non-Agenda Items:

Vinnie Taranto, 330 Tenth Terrace, Sustainable Community and Resiliency Committee Chairman, spoke regarding projects the committee is working on which include a sustainability plan and a swale ordinance.

G. Administrative Reports:

1. Town Attorney - None

2. Town Manager – Mr. Casey commended the police and fire department for their response in providing aid to a construction worker who was electrocuted.

H. Council Reports:

Councilmember Strand asked Town Clerk Raddon to include the ACLU report³ he distributed as an attachment to the meeting minutes. He inquired about sending flowers to Vincent Benevente's family and offered to pay for them. He spoke briefly regarding the Space Coast League of Cities dinner he attended. He read a tribute in remembrance of Todd Moore, a long-time resident who recently passed away.

I. Adjournment:

There being no further discussion, Mayor McDermott adjourned the meeting at 10:14 p.m.

Mark McDermott, Mayor, Signature on file.

Attested by: Rebekah Raddon, CMC, Town Clerk. Signature on file.

Attachments:

1. Flock Safety Presentation
2. Indialantic Procedure/Policy for ALPR System
3. ACLU Report



flock safety

+ Indialantic PD

Leverage the future of policing, *now*



flock safety

Our Mission

Eliminate Crime & Shape a **Safer Future, Together**





flock safety

Why Flock Safety?



What we observe: **the current reality**

- Police headcount is on the decline
- 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 tech work?

flock safety

When you get Flock you get:

objective, real-time and investigative leads

- Vehicle Fingerprint™ = license plate plus
- **Indiscriminate evidence** from fixed locations
- No people, no facial recognition, no traffic enforcement



Plate
TX LGS2639



Last Visit
3:15 PM EDT



Make
Toyota



Seen
3 OF 30 DAYS




Color
Gray



What is this tech?

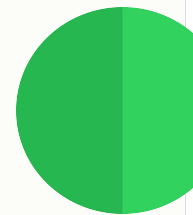
- License plate recognition
- Gathers objective evidence and facts about vehicles, not people
- Alerts police of wanted vehicles
- Used to solve crime
- Adheres to all state laws

What ISN'T this tech?

- Not facial recognition
 - Not tied to PII
 - 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 act as a deterrent






flock safety

Transparency & Accountability



Protecting Privacy

- Footage owned by Agency/City and will never be 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 personal information is identifiable in Flock
 - NOT used for traffic enforcement
 - Not connected to registration data or 3rd party databases (Carfax, DMV)
 - Transparency Portal
- 

Your ALPR Policy

- **Purpose**

- Allowed uses
- Sharing policy
- Hotlist verification

- **Protections**

- Data retention
- Audit procedures
- Misuse policy
- Training

I. POLICY

The Reno Police Department has been authorized by the Reno City Council to utilize Automated License Plate Readers (ALPR) to assist in providing safety to the residents of the City of Reno. This policy establishes the use of ALPR technology.

II. PURPOSE

The primary purpose of the Reno Police Department Automated License Plate Readers (ALPR) system is to provide a tool for use by Patrol and Criminal Investigations personnel. This tool assists in the detection and apprehension of vehicles and/or persons traveling through the jurisdiction of the Reno Police Department in a vehicle that has license plates that have been entered either into the National Crime Index Computer or on the Reno Police Department ALPR Hotlist. The ALPR system can also be utilized by RPD Detectives to assist in the development of leads that can eventually identify suspects who have committed crimes within the City.

Transparency + Insights

Measure ROI and promote the ethical use of public safety technology

Transparency Portal

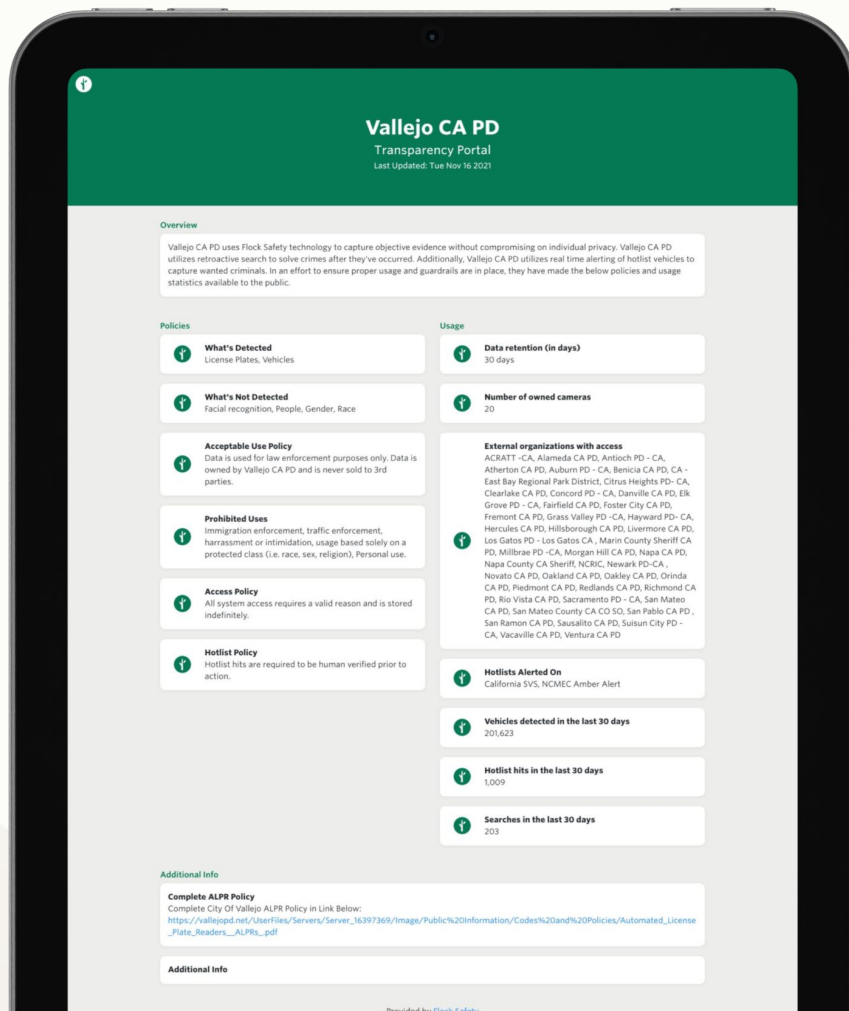
- Customizable for each agency
- Display technology policies
- Publish usage metrics
- Share downloadable Search audits

Insights Dashboard

- Measure crime patterns and ROI
- Audit Search history

Examples

- Click here for [Indialantic PD](#)



**It actually solves and prevents
crime**



CASE STUDY *Amber Alert*



CPD



Chamblee, Georgia



Stranger on Stranger Abduction
August 28, 2020

When every second matters, Flock Safety's Machine Vision is Critical

- 12:33 PM ● Amber Alert Issued
- 1:01 PM ● Search Conducted with Flock Safety
- 2:30 PM ● Suspect Vehicle Located
- 5:03 PM ● Felony Stop + Arrest
- 6:00 PM ● Baby Reunited with Mother

Flock ALPR



Savannah PD



Savannah, GA

- In Florida, elderly woman attacked and carjacked.
- Flock's ALPR identified the stolen car license plate in Savannah and alerted Savannah PD.
- Savannah PD found the vehicle, questioned the two occupants, and arrested one of the individuals as a suspect in the Florida woman's assault.
- From [Fox28 News](#)



“[Flock is] very effective. This is a force multiplier for areas where you might not have an officer that can be everywhere when things are happening. So, this technology gives the ability to expand that,” said Major Gavin, SPD Patrol Division.”

Flock ALPR



St. Petersburg PD
Tampa PD



St. Petersburg, FL
Tampa, FL

- **Two murders in overnight hours in South St. Petersburg**
- With **license plate evidence from Flock's ALPR**, Tampa officers arrested an individual with an outstanding warrant for aggravated battery with a deadly weapon, felon in possession of a firearm, resisting an officer without violence, and trafficking cocaine.
- They then learned this individual was also a **suspect in the St. Petersburg murders.**

Person of interest in custody following deadly South St. Pete shootings

By FOX 13 news staff | Published April 14, 2022 | Updated April 15, 2022 | St. Petersburg | FOX 13 News



Flock ALPR



River Rouge PD



Tampa, FL
Detroit, MI

- Suspect robbed SunTrust outside of Tampa, FL on January 14th
- **Flock camera caught a picture of the vehicle and license plate.**
- FBI had reason to believe he was headed to Michigan.
- Before the FBI could alert Michigan PDs, **Flock's system alerted River Rouge PD the suspect's license plate** was hit in the area.
- River Rouge and Ecorse PD found, pursued, and arrested the suspect, who had several prior arrests.

NEWS / BREAKING NEWS

Man robbed Carrollwood SunTrust bank, Hillsborough sheriff says

Detectives are looking for a suspect who pointed a gun at a bank teller.

Florida bank robbery suspect arrested after police pursuit, crash in Ecorse

By FOX 2 Staff | Published January 20, 2022 | Crime and Public Safety | FOX 2 Detroit

Flock ALPR



Chesterfield PD



Chesterfield, MO

- **Police received a “Check the Welfare” call** within our city limits for an adult female who had not been in contact with her family for several hours.
- Investigating officers were able to identify **the vehicle including the license plate** and ran the plate through the Flock system.
- They identified a hit on one of the cameras and searched the parking lots and located the vehicle.
- **The individual was found alive** inside the vehicle and in need of medical attention.



“Flock Safety helped save a life. Without the Flock camera system, we would not have been able to locate the person in need so quickly.”

- Lt. Teresa Koebbe

CASE STUDY: Long Term Results



Gwinnett County PD - Central Precinct



Gwinnett County, GA

Central Crime Statistics Comparisons 2020 to 2021

Crime Type	2020	2021	Difference	+/- Percentage
Homicide:	17	10	-7	-41%
Robbery:	135	109	-26	-19%
Aggravated Assault:	259	229	-30	-12%
Aggravated Battery	26	16	-10	-38%
Residential Burglary:	226	204	-22	-10%
Commercial Burglary	190	120	-70	-37%
Entering Autos:	1097	947	-150	-14%
Motor Vehicle Theft:	375	345	-30	-8%

“2021 is the first time in six years that they have had under 1,000 entering autos.”



Resources

1. **Educate council and create buy in:**
 - a. What is ALPR? - [click here](#)
 - b. ALPR FAQs - [click here](#)
 - a. Crime stats - [click here](#)
2. **Educate the community, and listen to concerns:**
 - a. Press release template - [click here](#)
 - b. Images of ALPRs - [click here](#)
3. **Transparently communicate:**
 - a. PIO Toolkit - [click here](#)
 - b. Model ALPR policies
 - i. Option 1 - [click here](#)
 - ii. Option 2 - [click here](#)
 - iii. Option 3 - [click here](#)
 - c. Examples of the Transparency Portal - [click here](#)

Thank You





Indialantic Police Department

Michael A. Connor, Chief of Police

POLICY/PROCEDURE

400.56 Automated License Plate Recognition (ALPR) System

Number Series: 400 – Operational LE

Approved Date: October 25, 2022

Rescinds: N/A

Revision Log:

Review Frequency: 3-Year

CFA Standard: 32.04(A-D)

Michael A. Connor
Michael A. Connor, Chief of Police

PURPOSE

The purpose of this policy is to provide members with guidelines on the proper use of an Automated License Plate Recognition (ALPR) system, also known as license plate reader systems.

POLICY

It is the policy of the Indialantic Police Department that the ALPR system, and any data gathered as a result of system operation, will be used for criminal justice purposes only. Personnel utilizing and maintaining ALPR equipment will be trained to preserve system integrity and to ensure that inaccurate or dated information is properly purged. The technology should be used in a manner that protects the civil rights and civil liberties of citizens, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments of the United States Constitution.

DEFINITIONS

Automated License Plate Recognition (ALPR) System – a system of one or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data.

Fixed ALPR System - ALPR equipment that is permanently affixed to a structure, such as a pole, traffic barrier, or bridge.

Mobile ALPR System - ALPR equipment that is affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

Hot List - data provided that includes license plate numbers of stolen vehicles, stolen license plates, wanted person(s) with a license plate associated with those records, and suspended or revoked registrations. This term also includes, but is not limited to, national data (i.e. NCIC) for similar categories, license plates associated with AMBER Alerts or Missing Persons/Vulnerable Adult Alerts, and includes manually entered license plate information associated with crimes that have occurred in any local jurisdiction or other investigative targets.

Alert - an audible, visual, or documented response that is triggered when the ALPR system receives a potential "hit" on a license tag.

Policy/Procedure

400.56 – Automated License Plate Recognition (ALPR) System

Page 1 of 4

Hit - an alert matched from a vehicle tag to either the "hot list" or a manually registered vehicle tag by a user for further investigation. This requires visual verification that the ALPR correctly deciphered the vehicle tag.

Verified Hit - a hit by the ALPR system that has been deemed valid after the ALPR user has conducted a live query transaction in FCIC/NCIC.

Personal Identifying Information (PII) - information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII includes names, gender, race, date of birth, photographs, addresses, social security numbers, driver's license numbers, or biometric data.

PROCEDURE

400.56.1 ALPR System Management

1. The ALPR system, associated equipment, and data generated by the ALPR shall be used for criminal justice purposes only.
2. An ALPR is used to scan vehicle license plates that are affixed in public view (i.e. plates of vehicles traveling or parked on any street or highway or other public property, or visible from a place or location at which a law enforcement officer is lawfully present).
3. ALPR system use shall be authorized by the Chief of Police or designee. Authorization may be given for repeated or continuous deployment of an ALPR (i.e. mounting the device on a particular law enforcement vehicle or positioning the ALPR at a specific stationary location), in which case the authorization will remain in force and effect unless and until rescinded or modified by the Chief of Police or designee.
 - a. Requests for placement of fixed location ALPR cameras will be forwarded to the Administrative Sergeant or designee.
 - b. Requests for placement of mobile ALPR cameras will be forwarded to the Chief of Police or designee.
4. Regular maintenance, support, upgrades, calibration and refreshes of the ALPR system will be conducted to ensure that it functions properly.
 - a. Designated personnel shall periodically inspect equipment to ensure functionality and camera alignment.
 - b. Any equipment failures need to be reported immediately to the Administrative Sergeant or Chief of Police.
 - c. Any system maintenance will be performed approved vendors.
5. Members may access or use ALPR stored data only if they are a designated authorized user and have received training on the proper use of ALPR data.
6. Members are guided by 200.10 Criminal Justice Information Security to safeguard against unauthorized persons viewing CJIS and PII displayed information.
7. Misuse of ALPR equipment, associated databases, and/or data generated by the ALPR system will subject the user to disciplinary action up to and including termination.

400.56.2 Officers authorized to use the ALPR system will receive training which may include, but is not limited to, the following:

1. Setup procedures
2. Proper use guidelines
3. Legal issues involved with the use of the ALPR system
4. Other issues as deemed necessary

400.56.3 ALPR System Overview

1. The ALPR system scans, captures, and compares optical license plate information to vehicles

- associated with crimes and criminals, comparing them against a Hot List.
- 2. ALPR can store the digital image of the license plate, the time, date, location of the image captured, and the capturing camera information.
- 3. Stored ALPR data does not include PII of individuals associated with the license plate. Obtaining persons associated with license plate information requires a separate, legally authorized inquiry to another restricted-access database, such as DAVID and/or New World.
- 4. The Hot List is downloaded on a daily basis with the most current wanted vehicle information available at that time from FCIC/NCIC.
- 5. The ALPR system does not conduct a live check against FCIC/NCIC databases.
- 6. The ALPR system is capable of conducting various types of queries against the Hot List that may include, but are not limited to, wanted checks, stolen vehicles, stolen tags, registered sexual offenders, AMBER/SILVER alerts, BOLOs, person checks, etc.
- 7. Members using the ALPR system shall enter additional vehicles of interest to the Hot List for criminal justice purposes only. Examples of possible scenarios where manual entry of a vehicle's tag include, but are not limited to, BOLOs, attempts to locate, investigative targets, child abductions, missing persons, and wanted persons.

400.56.4 Criteria for activation of the ALPR includes license plate canvasses in relation to any criminal investigation, violation of law, or incident concerning the safety of the public.

- 1. The ALPR system will assist members in the detection, identification and recovery of stolen vehicles, wanted persons, missing and/or endangered children/adults, and persons who have committed serious and violent crimes.
- 2. ALPR data can help members develop and pursue leads in criminal investigations by assisting in locating suspects, witnesses, and victims by identifying vehicles in the vicinity at the time of the crime.

400.56.5 Fixed ALPR Procedure

- 1. Upon alert notification and prior to taking action on a potential hit of the fixed ALPR system, the ALPR user will:
 - a. Verify the ALPR system correctly "read" the license plate characters and verify the state of issue of the license plate.
 - b. Verify the record that triggered the alert is still active in FCIC/NCIC.
 - c. Confirm with dispatch that the hit is still active.
- 2. ALPR users will be notified of potential hits in real time according to the method the user selected in the program (email, text, etc.)
 - a. Following a verified hit, and upon developing probable cause, an officer(s) will initiate a stop in accordance with Department guidelines, depending on the type of violation.
 - b. Recognizing that the driver of the vehicle may not be the registered owner, verification that the driver is the subject of the hit prior to the stop should be made. This does not apply to a verified stolen vehicle hit.

400.56.6 Vehicle-Based ALPR Procedure*

- 1. Vehicle-based ALPR equipment will be inspected prior to use to ensure that the cameras are properly affixed and operating. Any damages to the ALPR camera or supporting equipment will be reported to the officer's supervisor.
- 2. At the start of each shift, users must ensure the ALPR system has been updated with the most current Hot List available.
- 3. Upon alert notification and prior to initiating a stop based on a tentative hit, the user will conduct the following:
 - a. Verify the ALPR system correctly "read" the license plate characters and verify the state of issue of the license plate.
 - b. Verify the record that triggered the alert is still active by querying the plate in FCIC/NCIC.
 - c. Confirm with dispatch that the hit is still active.

- d. Following a verified hit, the officer will initiate a stop in accordance with Department guidelines, depending on the type of violation.
- e. Recognizing that the driver of the vehicle may not be the registered owner, verification that the driver is the subject of the hit prior to the stop should be made. This does not apply to a verified stolen vehicle hit.

400.56.7 A non-verified hit on either a mobile or fixed ALPR will not be used as the sole reason for a stop or enforcement contact unless:

1. the officer has independent probable cause/reasonable suspicion to make a stop
2. the officer has exigent circumstances
3. officer safety issues exist

400.56.8 Security Access and Storage of Data

1. Access to ALPR data shall be secured and controlled by a user login/password accessible ALPR database, capable of documenting who accessed the information by date and time. Access to hot lists are restricted to members who have received CJIS Awareness Training.
2. The Administrative Sergeant will ensure that all data returned from the mobile* ALPR system is properly stored and retained in accordance with FSS Chapter 119. Fixed ALPR data is stored on the vendor's cloud based system in accordance with their procedures.
3. Images and/or data containing or providing PII obtained through the use of a ALPR system is confidential and exempt from FSS 119.07(1) in accordance with FSS 316.0777.
4. Information obtained through the use of an ALPR system may only be disclosed in accordance with FSS 316.0777.
 - a. Any such information may be disclosed by or to a criminal justice agency in the performance of the criminal justice agency's official duties.
 - b. Any such information relating to a license plate registered to an individual may be disclosed to the individual, unless such information constitutes active criminal intelligence or investigative information.

400.56.9 Retention

1. ALPR data shall be retained in accordance with FSS 316.0778.
2. ALPR data that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion may be retained for no longer than 3 anniversary years.
3. Access to ALPR data for criminal investigation or intelligence purposes is limited to authorized Criminal Justice Agency personnel for no longer than 3 anniversary years and requires an agency case number or case name and logging of access.
4. Data captured, stored, generated, or otherwise produced shall be accessible in the ALPR system for 30 days for tactical use.

REFERENCES

State/Federal Regulations:

316.0777 – Automated license plate recognition systems; public records exemption
 316.0778 – Automated license plate recognition systems; records retention
 Chapter 119 – Public Records

Forms:

N/A

Other Policy/Procedure References:

N/A

*The agency does not own/deploy vehicle-based ALPRs at the time of this policy publication. Vehicle-based language included for future use.



Fast-Growing Company Flock is Building a New AI-Driven Mass-Surveillance System

By Jay Stanley
March 3, 2022

A new and rapidly growing surveillance company called Flock Safety is building a form of mass surveillance unlike any seen before in American life. The company has so far focused on selling automatic license plate recognition (ALPR) cameras to homeowner associations and other private parties, as well as to police departments. But it has done so through a business model that effectively enlists its customers into a giant centralized government surveillance network — and the company is aiming to expand its offerings beyond ALPR to traditional video surveillance, while also expanding its AI machine vision capabilities.

In this paper, we look at this company's products, business model, and future aims, and how those embody some of the more worrisome trends in surveillance technology today. Flock is not the only company engaging in mass collection of ALPR data; Motorola Solutions and the company it acquired, Vigilant Solutions, also run a giant nationwide ALPR database, and have recently [made a bid](#) to compete with Flock's strategy. But we focus here on Flock because it is a new, up-and-coming company that industry analysts say is poised for major expansion both geographically and in the kinds of technology it provides.

A public/private license-scanning network

A startup founded in 2017, Flock has grown rapidly, riding two [major trends](#) in the security camera industry: a move to cloud services, and video analytics. The company recently attracted \$300 million in [venture capital investments](#), which industry analysts [say](#) is “unparalleled in the video surveillance industry” and will put the company “in a position to expand aggressively over the next few years.” The company makes grandiose claims about its mission, which it says is to “eliminate nonviolent crime across the United States.”

Flock [says](#) its fixed cameras have been installed in 1,400 cities across the U.S. and [photograph](#) more than a billion vehicles every month, and its [ambition](#) is to expand to “every single city in America.” Flock also has a [partnership with](#) the body camera company Axon to provide mobile ALPR devices for police vehicles. Flock’s cameras allow private customers like homeowner associations as well as police customers to create a record of the comings and goings of every vehicle that passes in front of the cameras. But the service goes well beyond that; it feeds that data into a centralized database run by Flock. As the company [tells](#) police:

If you know the specific license plate in question, use FlockOS to get a detailed report of the suspect vehicle’s history over a given timeframe.

Use FlockOS’s local and national search network to find the suspect vehicle across state lines, including up to 1 billion monthly plate reads. All this is included, for FREE, for any Flock Safety customer.

Flock not only allows private camera owners to create their own “hot lists” that will generate alarms when listed plates are spotted, but also runs all plates against state police watchlists and the FBI’s primary criminal database, the National Crime Information Center (NCIC). When a camera scores a hit against one of those databases, law enforcement receives an immediate notification. As Flock CEO Garrett Langley [explained](#) in 2020:

We have a partnership through the FBI that we monitor all of the cameras for about a quarter of a million vehicles that are known wanted — either stolen, it’s a warrant, it’s an amber alert. And so at any given time — about 20 times an hour — we will notify local authorities. ... In January we reported just over 67,000 wanted vehicles across the country.

This giant surveillance network might also be used by immigration authorities to deport people, as is [Motorola’s](#) private ALPR [database](#). [Asked](#) by Vice News whether Flock could be used for such purposes, Langley said, “Yes, if it was legal in a state, we would not be in a position to stop them,” adding, “We give our customers the tools to decide and let them go from there.”

All of this means that those who purchase Flock cameras are effectively buying and installing surveillance devices not just for themselves, but for the authorities as well, adding their cameras to a nationwide network searchable by the police. The closest thing to this model we have seen before is the doorbell camera company Ring, which also raises many [troubling issues](#). But Flock is working (and enlisting its customers to work) directly as an agent of law enforcement even more than Ring. It says it is “working with” over 700 law enforcement agencies and, [according](#) to Langley,

At the end of the day, we view the police department as our actual end-user. They’re the only ones that can make an arrest. So neighborhoods, apartment complexes, motels, hotels, malls, hospitals — they might pay for the camera, but more often than not the only ones that are actually looking at it are the police. ... Most of our software is actually running in the patrol vehicles. So if there’s a crime, or there’s a stolen car that drives by,

we're notifying the nearest officer, typically within a few seconds from when that happens, and they can turn on the blue lights and go get 'em.

As with Ring, police departments appear to be coordinating with Flock in ways that are unseemly for agencies serving the public. Vice [reported](#) that it obtained emails showing that "Flock works closely with police to try and generate positive media coverage, improve their PR strategy, and ... 'bring more private cameras into the area.'" Flock has also helped write police press releases, Vice found, and officers appear in Flock [promotional videos](#). Emails obtained by the video surveillance industry research group IPVM [show](#) local Texas police referring homeowners associations and other neighborhood groups to Flock, advocating for the company at community meetings, providing the company with neighborhood contact lists, and introducing other police chiefs to company sales managers. In 2020, Langley [told](#) a police audience,

When you partner with Flock ... you're also getting a new ability to do public outreach. ... Every single day we're working with our chiefs and their command staff to host community events, to build awareness, and more importantly, build a common trust and relationship between your constituents and the police department. And the end result is more cameras at no cost to you.

The company has run into [trouble](#) for pushing police departments to embrace its technology without getting the approval of the communities those departments serve. It has also [created conflict](#) in some communities where its cameras have been proposed or adopted, and sparked well-founded concerns that the technology might have a [disproportionate](#) effect on communities of color and other vulnerable communities.

Centralization of data

When a neighborhood association buys a Flock camera, it is basically contributing a piece of equipment to a new nationwide law enforcement surveillance infrastructure that, as Slate [put it](#), means even "small-town police departments can suddenly afford to conduct surveillance at a massive scale."

Flock can gather the information captured by its cameras around the country into its own centralized database because it is a cloud-based service provider rather than a mere seller of hardware. That database is available to more than [500 U.S. police departments](#). As a business matter, this allows the company to benefit from self-reinforcing [network effects](#). But if Flock cameras become as widespread and densely placed as the company hopes, law enforcement will gain the ability to know the detailed movements of virtually any vehicle for as far into the past as that data is held. That would create enormous risks of privacy violations and other abuses and would have significant legal implications as well.

And the risk of abuse by government is all too real. Unfortunately, this country has a [long tradition](#), extending up to the [present](#), of law enforcement targeting people not because they're suspected of criminal activity but because of their political or religious beliefs or race. That includes quasi-private surveillance. There are also many [documented instances](#) of individual officers abusing police databases, including ALPR databases.

We have long had concerns about the dangers posed by hybrid [public-private surveillance](#) practices — but Flock threatens to take that to a new level. In the past we have [noted](#) that distributed private surveillance cameras are less of a threat to civil liberties than centralized surveillance networks — [but also](#) warned that if all those private cameras were connected to a cloud, the effect would be to re-centralize them. By pulling all the data recorded by its customers — including its police customers — into its own centralized servers, Flock not only creates an enormously powerful private-public machine sweeping up data on Americans’ activities, but puts itself at that machine’s center. It’s bad enough when law enforcement engages in such mass surveillance, but to have such data flowing through a private company creates an additional set of incentives for abuse.

For one thing, there are no checks and balances on the use of this database. The lack of proper checks on the behavior of law enforcement is well established — and studies [suggest](#) improper use of ALPR in particular may be widespread. Nor are there adequate checks on Flock. The company says it only keeps ALPR data for 30 days, but no laws require them to honor that promise. The company controls an enormous data set that could probably be monetized in various ways — and while the company is growing fast now, boom times never last forever. What will future managers do if the company hits tough times, the spotlight has moved on from their controversial role, and they’re tempted to reach for revenue they’re flushing out of their database every 30 days? How might they use their tool against competitors, or against workers, say, if they find themselves fighting a union battle?

We’ve already had a glimpse of what can go wrong with cloud surveillance providers in the case of the company Verkada, which was hacked and found to be [secretly tapping into its customers’ cameras](#). Indeed, think what present or future leaders or employees at Flock could do with that power — or what they could be pressured or forced into doing by unscrupulous government officials. We know that Ring gave workers [access to every Ring camera](#) in the world, together with customer details. Other companies offering cloud services have also run into controversy from granting such access, including [Google](#), [Microsoft](#), [Apple](#), and [Facebook](#). Those companies accessed people’s data to improve their AI models, which are always hungry for real-world data. Flock likewise [says](#) that its cloud architecture “allows us to continue to improve the software and deploy enhancements out to our cameras in real-time.”

Of course, the authorities and the company are not the only possible sources of abuse; there are [plenty of reasons](#) to worry about nosy homeowner association board members and the like using this tool to snoop on the comings and goings of their neighbors (and their neighbors’ friends, family, lovers, etc.). Neighborhood administrators are not subject to even such training and oversight as is applied to the police, and don’t generally know how to impose access restrictions, if they even think of doing so.

It is true that all vehicles are required to display license plates, and in our [past work on ALPRs](#) we have written that license plate readers would pose few civil liberties risks if they only checked plates against legitimate hot lists and these hot lists were implemented soundly. But we also noted that a proliferation of cameras and widespread sharing allow for the creation of intrusive records of our comings and goings, create chilling effects, and open the door to abusive

tracking. And the scale of what Flock is doing goes far beyond what was contemplated when ALPRs first arrived on the scene.

Accuracy problems

ALPR is also bedeviled by accuracy problems. In tests, IPVM [found](#) that Flock's ALPR worked well overall compared to other products — but nothing is perfect, and even a low error rate can produce tragic consequences given the scale of Flock's operations. In particular, IPVM found that Flock's system misidentified a license plate's state about 10 percent of the time. Given that state misidentification errors [have](#) led to innocent people being terrorized by the police as presumed dangerous criminals, that is a real problem.

The FBI's NCIC database that Flock checks plates against is notoriously [inaccurate](#), and people have been [badly harmed](#) by inaccuracies in that database, [including](#) through ALPR cameras. Federal law requires that government agencies maintain records used to make “any determination about any individual” with “such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” That doesn't seem like too much to ask — but when it comes to its NCIC database, the FBI felt compelled to [exempt itself](#) from that law.

One detective also [told](#) colleagues [on LinkedIn](#) that “today we almost did a felony stop on a stolen vehicle that wasn't actually stolen,” and reminded them that when dealing with stolen cars they must “remember to remove the vehicle if it's recovered.” A system dependent on busy and sometimes sloppy officers to remember to carry out such follow through is also a recipe for trouble.

Another source of potential error is that Flock's cameras download fresh hit lists from the NCIC only [twice a day](#), which creates the possibility that the removal of a plate from the hotlist will cause out-of-date alerts to be sent to law enforcement for up to 12 hours until the next update.

The accuracy problems with ALPRs have led to [many incidents](#) in which [people](#) have been subject to [traumatic treatment](#) by law enforcement because of errors. And when law enforcement comes running on high alert because technology has raised an alarm, those most likely to be subject to such treatment — or worse — are Black people and members of other vulnerable communities for whom even the most casual encounter with law enforcement can turn deadly.

When the only people running plates were police officers doing so manually and only when they personally witnessed a suspicious vehicle, errors in law enforcement databases like the NCIC occasionally had bad effects. But when plates are being run 500 million times a month, the consequences of errors in those databases become greatly magnified. (For more on the problems ALPR devices present see the ACLU's 2013 [report](#) and this 2017 Electronic Frontier Foundation [page](#) on the technology.)

Beyond license plates

Flock does not plan to remain limited to ALPR cameras. Langley, its CEO, [told](#) IPVM that the company is working on ideas for traditional camera products and sees “a ton of opportunity in the traditional [surveillance] market.”

Already, the photos taken by Flock’s ALPR cameras capture more than just license plates; the photos are used to create what the company [calls](#) a searchable “Vehicle Fingerprint.” Using a “proprietary machine learning algorithm,” the company [says](#), it gathers “vehicle make, type, color, license plate, state of the license plate, covered plates, missing plates, and unique features like roof racks and bumper stickers.” Presumably that would allow searches for all vehicles that include a particular political bumper sticker, enabling people to be targeted based on the exercise of their First Amendment-protected free expression rights.

If Flock applies its public-private business model and its camera technology to ordinary surveillance cameras, it will be super-charging the spread of centralized police camera networks and helping transform video surveillance from sporadic collections of cameras into truly powerful dragnet surveillance tools.

The spread of such systems has been slow because of the expense involved — but Flock could end that. In October 2021, I attended a security conference where security industry analyst and publisher John Honovich of IPVM told attendees that Flock represents a new, disruptive business model in the surveillance video industry. Outdoor cameras have always been orders of magnitude more expensive than indoor cameras, he said, because they are so difficult to install; running power and data lines to outdoor cameras is no easy feat, and they require costly maintenance contracts.

Flock is focused on solving what has been a very hard problem of outdoor installations with a new model based on three technologies that are rapidly improving: solar power, wireless connectivity, and artificial intelligence. The [rapid decline](#) in the cost of solar power has made solar cameras more economical, and wireless connectivity continues to improve as well. Most significantly, perhaps, improving AI computer vision allows cameras to constantly monitor a scene and only send data off the camera when the AI has determined that something of significance has appeared. In the case of ALPR, that would be a vehicle driving by — but it could be anything. Sending still photos or short clips of scenes identified as significant by AI algorithms allows for the installation of large numbers of cameras without the strain on bandwidth and storage capacities that full-motion video cameras often bring.

According to Honovich, “it’s clear that Flock will get much bigger,” and the company is “a threat to any incumbent doing city-wide systems.” One officer says in a company [promotional video](#) that police have even started using the company’s name as a verb — as in, “Have you Flocked that tag yet?”

Expanding analytics

In addition to looking at a move toward full-motion surveillance, Flock's ambitions include expanding its analytics offerings beyond ALPR. Already, for example, its system can carry out what it calls "[convoy analysis](#)," which involves doing proximity analyses to identify vehicles that are near to each other at crucial times and therefore presumably associated with each other. And in a sales video seen by [Vice](#) (apparently since removed from YouTube), the company said it can detect people, cars, animals, and bicycles, a further indication of the company's interest in expanded video analytics.

The company has also announced a troubling expansion of its ALPR devices into audio recording and analytics, [unveiling](#) an augmented version of its ALPR cameras called "Raven" that purports to provide audio gunshot and "crime detection" as cloud services. This service will use AI to attempt to identify the sounds of gunshots, screeching tires, breaking glass, and sawing metal (to try to detect catalytic converter theft).

The Raven product raises questions about Flock's direction as AI and machine vision continue to improve. Today the company reads license plates and bumper stickers; tomorrow that could expand to t-shirts and tattoos. And how long before it offers products claiming to be able to visually detect guns, fighting, muggings, "[aggression](#)," or "anomalous" behavior? All of these and many more capabilities are currently being worked on by computer scientists. We discussed this trend in more detail in our 2019 [report](#) on video analytics, but the long-term threat is that millions of cameras will be turned into ever-watchful digital officers, never sleeping or distracted but highly biased and error-prone, monitoring us constantly and ready to report us to our neighbors or the authorities. Indeed, one of Flock's [marketing slogans](#) makes this analogy explicit, saying that its cameras "see like a detective."

Flock has another product called "[Wing](#)" that allows police to scan through thousands of hours of footage to extract vehicle "fingerprints" for searching — an extremely powerful new surveillance capability. It can thus transform existing third-party cameras owned by police departments into cameras that the company says can — yes — "see like a detective." The power of cloud AI analytics is that they're not tied to any particular hardware.

Even more so than license plate recognition, other forms of AI are also notoriously [brittle](#) and unreliable. It's highly questionable how effective Flock's Raven audio analytics service will be, for example. The gunshot detection company ShotSpotter similarly [uses](#) microphones distributed across a city to listen for gunshots, but mostly relies on human analysts to try to differentiate between gunshots and other loud bangs — and even so, questions have been [raised](#) about ShotSpotter's false alarm rate and overall effectiveness. The number of false alarms triggered by Raven will likely prove to be significant and perhaps dysfunctional.

And of course, Flock will want to access its customers' cloud data in order to improve its AI, as it says it is already doing with ALPR data. If and when the company moves into collecting live video and other increasingly sensitive data, it will create a significant privacy issue as well. Raven also raises significant legal issues due to wiretapping laws (see below).

Flock is already building an unprecedented, public-private, distributed-yet-centralized surveillance machine. All the risks posed by such a machine will only grow if the company expands its offerings from ALPR to traditional surveillance cameras and to advanced new forms of behavioral analytics.

Privacy practices

Flock constantly [claims](#) to be “privacy friendly” to try to disarm one of the primary obstacles to its acceptance by communities. It says it doesn’t do face recognition, which is good (though that wouldn’t stop an end-user police department from doing so once it had downloaded an image of a person). For auditing purposes, it includes a data field in which police enter the reason for a search, which is good. It also says it doesn’t sell or share ALPR data with third parties (other than through its database service, which is part of what it is selling with its products), and only retains plate data for 30 days. “With built-in 30-day data retention, everyone’s comfortable,” Langley [claims](#).

Everyone is not comfortable. An even shorter retention period would be better, but this system would be far worse than it is if the retention period were longer. Still, given the scale of this system, 30 days is a long enough window that it poses real privacy risks, especially if Flock cameras continue to grow, providing an ever-more-detailed record of people’s movements. People can engage in a lot of perfectly legal yet private behavior within 30 days — movements that would reveal things about their political, financial, sexual, religious, or medical lives that nobody in the police or in a company like Flock has a right to track. As discussed below, a majority on the Supreme Court has [explained](#) that tracking a vehicle with GPS constitutes a “search” for Fourth Amendment purposes even when the tracking only lasts 28 days. And the court later held that obtaining seven days of location information about a person was a Fourth Amendment “search,” too.

Whenever questioned about privacy, Flock executives mention these policies, as if that’s the end of it. But it’s not the end of it; there are many other privacy implications of license plate recognition in general, and Flock’s system in particular, that communities need to consider. Flock may not sell its data but the company itself holds it. And as IPVM aptly [put it](#), if the company achieves its growth targets, “it will effectively become a gigantic private entity that is performing public policing work.” The privacy protections Flock likes to tout are necessary but not sufficient in a system playing that role at such a scale, and Flock’s products raise many privacy issues that aren’t addressed by the privacy practices that they cite. And again, we have no way of knowing whether Flock is following its stated policies, and it could change those policies at any time.

A system of mass surveillance

Altogether, Flock’s ALPR network adds up to a system of mass surveillance — a system that seems poised to expand beyond just license plate recognition. Mass surveillance systems have long been feared by people who value open, democratic societies, and for good reason. The ability to access a record of all our activities — even if just when we’re in public spaces —

conveys the power to learn an enormous amount about our social, political, sexual, medical, and religious lives. Mass surveillance simply gives too much power to those who control it. Such power lends itself too easily to abuse, chilling people who might want to protest those in power or otherwise exercise their freedom of expression, and generally casting a pall over people's freedom to live their lives without being watched.

Surveillance systems also tend to have a disproportionate impact on Black and Brown and other historically disadvantaged communities. Often police departments [install them disproportionately](#) in communities of color. The NYPD [used](#) ALPR devices to abusively [surveil mosques](#) in the 2000s. And systems such as Flock's enable the continuation and intensification of patterns of policing such as those uncovered by the Department of Justice in Ferguson, Mo. There, the DOJ found in a [comprehensive report](#) that the police department aggressively over-enforced low-level, nonviolent "offenses" in communities of color (a [pattern](#) that has been found across the nation, including in [New York City](#), [Minneapolis](#), [Chicago](#), [North Carolina](#), [Philadelphia](#), and [Boston](#)). In Ferguson and some other jurisdictions, low-level arrests were intentionally used to extract payments to fill municipal coffers. This practice draws poor people who can't pay fines or who miss court dates into an escalating cycle of fees, fines, police stops, and general entanglement with the criminal justice system, amplifying petty offenses into ruined lives in a truly Dickensian dynamic. Many of those stops and fines involve automobiles, and a dragnet ALPR surveillance system [lends itself very naturally](#) to supporting that kind of policing.

Legal analysis

The system that Flock has built and is building could have many bad effects, but does it violate the law or Constitution?

The first question is whether the fact that people and/or their license plates are being photographed in public means that there can't be any legal violation of privacy. That claim does not appear to be winning acceptance in the courts.

In a pair of cases involving police use of digital-age technologies to track or aggregate peoples' locations and movements, the Supreme Court has [explained](#) that "individuals have a reasonable expectation of privacy in the whole of their physical movements" because of the "privacies of life" those movements can reveal. In *United States v. Jones*, a majority of the court wrote that using a GPS tracker to follow a car's movements for 28 days constitutes a Fourth Amendment search, observing that the ability to "secretly monitor and catalogue every single movement of an individual's car for a very long period" raised serious concerns. More recently, the court held in *Carpenter v. United States* that when police request seven days or more of a person's historical cell phone location information from a cellular service provider, a warrant is required. That's because of the "deeply revealing nature" of these digital location records, their "depth, breadth, and comprehensive reach," and the "inescapable and automatic nature of [their] collection." These rulings expressly rejected the argument that the public nature of the targets' movements meant they had no legally significant expectation of privacy.

Automated license plate readers raise the same concerns the court addressed in *Jones* and *Carpenter*: they facilitate detailed, pervasive, cheap, and efficient tracking of millions of

Americans in previously unthinkable ways. ALPR data can reveal private and sensitive details about a person's life — details that individuals reasonably expect to remain private — and searches of ALPR databases by law enforcement to find evidence of criminal activity should require a warrant. As the Massachusetts Supreme Judicial Court [recently observed](#), “With enough cameras in enough locations, the historic location data from an ALPR system ... would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes.”

And what holds for ALPR cameras should also hold for any future mass-surveillance camera systems that can track people in equivalent ways — for example, by using a centralized network of public and private cameras combined with face recognition or other forms of video analytics or biometrics.

The second question is whether Flock's status as a private company affects this analysis — after all, only the government is constrained by the Fourth Amendment. And in fact, in many contexts, private actors have a right to take photographs that is *protected* by the Constitution's First Amendment. That right is not absolute, however; lawmakers, if they so choose, do have the authority to regulate photography that interferes with Americans' reasonable expectations of privacy, such as in private spaces like restrooms or people's homes. The deployment by private parties of surveillance systems such as camera networks that track people across space and time implicate similarly pressing privacy concerns.

But if lawmakers fail to enact such privacy protections, does the Constitution have anything to say about a private company like Flock engaging in such surveillance? It might, if Flock were acting in concert with police departments to the extent that courts would consider it a “[state actor](#).” In past cases, the Supreme Court has found private parties to be state actors (and therefore subject to the Constitution and other laws that apply to the government) where:

- Private parties perform public functions that have traditionally and exclusively been performed by the government.
- The government influences and encourages the performance of private actions.
- The government and a private actor enter into a “joint enterprise” or “symbiotic relationship” or become “pervasively entwined” with each other.

This body of law prevents the government from evading its constitutional responsibilities by delegating power to and hiding behind private entities. In the ACLU's recent [successful challenge](#) to the City of Baltimore's persistent aerial surveillance program, the City did not even dispute that the third party surveillance vendor conducting its surveillance operations was a state actor under the relevant law. Given Flock's actual entanglement and symbiotic relationship with law enforcement, there would at a minimum be a plausible case that Flock fits this definition and that its ALPR services — and potentially other mass-surveillance services such as a Raven audio recording network or other future offerings — are therefore constrained by constitutional privacy rights.

State laws are also relevant in assessing the legality of ALPR deployments. [Sixteen states](#) have passed statutes regulating ALPR devices. A few state laws regulate or ban certain private uses of

ALPR, which would of course directly affect the legality of Flock’s business model in those states. But most of the state laws regulate how law enforcement uses ALPR. California, for example, bans state police departments from sharing ALPR data with out-of-state and federal agencies, but a number of departments are [violating the law](#). (The ACLU of Northern California is [suing](#) over this violation.)

State constitutions, many of which have stronger privacy protections than the federal Constitution, may also impose limits on private surveillance business models such as Flock’s. Some state constitutions, such as [California’s](#), also place more limits on private actors.

A major question this raises is whether any police departments are using their reliance on this private company to do an end run around these laws. [Judges](#) in Virginia, for example, [ruled](#) that a Virginia privacy law (which says that personal information “shall not be collected” by state agencies “unless the need for it has been clearly established in advance”) bars police from collecting and storing ALPR data outside of a specific investigation. But if the State Police were accessing Flock’s ALPR database without considering themselves as “collecting” the data held by Flock, that would represent an evasive end-run around the intent of Virginia’s law.

Raven

Aside from threatening to expand daily surveillance in American life [from video to audio monitoring](#), Flock’s Raven gunshot detection product also raises significant legal questions. While the United States has millions of video cameras in public places, very few of them include microphones, and there’s a good reason for that. It’s not because mics are expensive or difficult to install, but because our wiretapping laws make it legally problematic to audio record people in public places. Laws in all the states and federal law make it illegal to record a conversation where the recording party is not a participant — and some state laws require the permission of all participants in a conversation. ShotSpotter’s microphones have survived scrutiny on this score partly because most of its mics are placed high above street level, where they can better hear gunshots and be shielded from everyday sounds. Those mics are also very narrowly targeted toward listening for gunshots, and there is no important privacy interest when it comes to the sound of gunshots in a city. Even so, we and other privacy advocates have been [very wary](#) about ShotSpotter’s product on that score.

But Flock’s audio sensors, which come packaged with the license plate readers, are placed close to the ground so the ALPR can see vehicles, and are therefore much more likely to pick up conversations. They also extend their monitoring beyond loud percussive noises to other noises that are much more likely to be a regular part of human life. By listening for a broader variety of more ambiguous sounds, Raven is more likely to accidentally record conversations. And in the rich and complicated lives we lead, people might have good reasons to break glass, or saw metal, or make screeching sounds — not to mention other noises that might be mistaken for those sounds by the AI — and shouldn’t have to worry about police arriving on the scene every time they do so.

Just recently my neighbor was bringing home groceries and dropped and shattered a glass bottle in her driveway. I found myself thinking about Flock’s product and how glad I was she didn’t

have to worry about the police showing up — something that, again, poses particular dangers for people of color.

Recommendations for Public-Private Surveillance Systems

Our nation should not permit the construction of any mass-surveillance systems, including through private-public law enforcement systems such as that being built by Flock. Legislators should enact rules governing ALPR along the lines of the [recommendations](#) we laid out in our 2013 report, and extend them to private actors working closely with law enforcement. Policymakers should include the following updates to account for the changing landscape:

- Given the increasing regional and national reach of ALPR systems, any non-hit data they collect should be permitted to be held only for very short periods. New Hampshire [state law](#) is a good model; it requires that where there is a hit, ALPR data “shall not be recorded or transmitted anywhere and shall be purged from the system within 3 minutes of their capture.” That policy allows the devices to be used to search for wanted vehicles but prevents the creation of dragnet location tracking databases. Retention periods of 30 days are too long for surveillance systems with a breadth and scope of any significance.
- No hot lists should be used unless they are certified by independent auditors as meeting the highest standards of due process (allowing people a meaningful way to have themselves or their vehicles removed including through adjudication by a neutral arbiter), legitimacy (being based only on individualized suspicion, and not being based on First Amendment-protected activity, for example), and reliability (including those standards imposed by the Privacy Act of 1974, a standard that the NCIC does not currently meet).
- Law enforcement agencies should not share license plate reader data with third parties that do not conform to the above principles and should be transparent regarding with whom license plate reader data is shared.
- Communities and their elected representatives should be especially hesitant to embrace networked surveillance cameras. Before investing in a partnership with Flock they should do some very careful legal analysis in light of the Supreme Court’s *Carpenter* decision.
- Communities that have not yet enacted a [CCOPS ordinance](#) should not permit the police that serve them to deploy surveillance devices without first receiving approval from the city council or other elected governing body. The decision-making process around whether to deploy surveillance technology should be transparent and open to public input and debate.

Businesses, community associations, and other private parties should consider the following when evaluating or deploying this technology:

- Private institutions should, at a minimum, think long and hard about whether they truly need ALPR or other dragnet surveillance devices, especially where vendors allow law enforcement — local and not — to search the data collected by any such devices.
- Private institutions should not use ALPR or other dragnet surveillance devices unless they disclose that fact to their customers, residents, or others subject to the surveillance.
- Housing and community associations that adopt such systems should ask sharp questions about their deployment such as: Who will have access to the data that is collected about you, your family, and friends or other visitors? Will there be any restrictions on the purposes for which data is accessed, or with whom it is shared, or can those with access browse through the data whenever they want? How will requests for access by residents, non-residents, those accused of wrongdoing, media outlets, or others be handled? Is there any logging of access to the data, or other mechanisms for enforcing rules about sharing and access?
- Any associations that create their own hotlists should do so only in conformance with the principles above that are applicable to government hot lists. They should also create and publish policies people driving throughout the community can read and understand.

Conclusion

Flock is pushing the adoption of surveillance devices by private parties and folding them into a larger, centralized network that is fast becoming a key policing infrastructure, all while pushing to expand beyond license plate recognition to other forms of AI machine vision and simultaneously making it much easier to install and connect outdoor cameras. If successful, the convergence of these trends — whether under the aegis of Flock or other companies — threatens to bring an entirely new level of surveillance to American communities, where it will further undermine Americans' privacy, disproportionately harm historically disadvantaged communities, and generally shift power to the government from the governed in our nation.

###