



**Minutes of Meeting
Board of County Commissioners
St. Johns County, Florida
Special Meeting
County Administration Building
500 San Sebastian View
St. Augustine, Florida 32084
September 15, 2026 - 5:01 p.m.**

CALL TO ORDER

Commissioner Murphy called the special meeting to order at 5:01 p.m.

Present: Clay Murphy, District 3, Chair
Ann Taylor, District 5, Vice Chair
Christian Whitehurst, District 1
Sarah Arnold, District 2
Krista Joseph, District 4

Staff Present: Joy Andrews, County Administrator
Brad Bradley, Deputy County Administrator
Jesse Dunn, Deputy County Administrator
Rich Komando, County Attorney
Kealey West, Deputy County Attorney
Crystal Smith, Deputy Clerk

ROLL CALL

The clerk called the roll.

INVOCATION

Chaplin Deon Johnson, St. Johns County Sheriff's Office, gave the invocation.

PLEDGE OF ALLEGIANCE

Director Jason Caban, St. Johns County Sheriff's Office, led the Pledge of Allegiance.

DELETIONS TO THE SPECIAL AGENDA

Murphy requested that discussion on funding for the Black History Museum be added as Regular Agenda Item No. 2.

Motion by Joseph, seconded by Taylor, carried 5/0, to approve the Special Meeting Agenda, as amended.

Yea: Joseph, Taylor, Murphy, Whitehurst, Arnold

Nay: None

1. Public Hearing - 5:01 p.m. Public Hearing - St. Johns County Board of County Commissioners Adoption of Final Millage Rates and Budget for FY 2027. In accordance with sections 129.03 and 200.065 of the Florida Statutes, the Board of County Commissioners (BCC) is required hold public hearings to adopt its millage rates and budget for the next Fiscal Year (FY). Such hearings must be held after 5:00 p.m. if scheduled on a day other than Saturday. The September 15, 2026, 5:01 p.m. hearing date has been advertised in the St. Augustine Record. The Florida Statutes further prescribe the specific order for consideration of substantive issues to be discussed during the required public hearings. The first substantive issue of discussion must be the percentage increase in the County's aggregate millage rate over the rolled-back rate necessary to fund the budget. The rolled-back rate is defined as the aggregate millage rate that would generate the same level of prior year tax revenues less certain defined allowances (such as new construction). During such discussion, the general public shall be allowed to speak and ask questions prior to the adoption of any measures by the BCC. The BCC shall adopt by resolution its final millage rates prior to adopting its final budget for FY 2027

Wade Schroeder, Director of the Office of Management and Budget, presented details of the Fiscal Year 2027 Final Millage Rates and Budget, including the meaning of FTEs (Full-Time Equivalent), debt proceeds, the increase in the fire district millage rate, the decrease in the general fund millage rate, and the percentage increase for the rollback rate. Neil Shinkre, Director for the Utility Department, explained the utility aspects of the budget.

Public Comment:

Shawn Morrison expressed concerns about using taxpayers' dollars to fund Flock cameras.

Kayliegh Masters expressed concerns about the budget funding Flock cameras and displayed a photo of herself with Sheriff Robert Hardwick after a missing child was found (Exhibit A).

Don Campbell expressed concerns about Flock cameras.

Sean Carpenter commended Sheriff Hardwick for his work with the homeless population in the County and expressed concerns about Flock cameras.

Mike Gill spoke against automated license plate readers and Flock cameras.

Forrest Parham expressed concerns about Flock cameras.

Joseph Miller questioned the different millage rates and spoke against Flock cameras (Exhibit B).

Jason Davis expressed concerns about Flock cameras.

Alexei Davis expressed concerns about Flock cameras and privacy.

Melissa Davis spoke against taxpayers funding Flock cameras and encouraged the County to remove the cameras.

Ryan Robinson spoke against taxpayers funding Flock cameras.

Sterling Seizert spoke against Flock cameras and explained his experience with surveillance cameras (Exhibit C).

Angela Foldi spoke about the 4-H youth program and funding.

Denver Cook referred to Schroeder's presentation and questioned the funding for Amendment 3 and the budget increase.

General Newsense sarcastically thanked public officials.

Deborah Campbell spoke against Flock cameras and highlighted a website known as *haveIbeenflocked.com*.

Kernel Earnest spoke against taxpayers funding Flock cameras.

Arnold raised concerns about Flock cameras and Artificial Intelligence (AI) capabilities. Discussion ensued on right-of-way permits for the cameras and funding for the St. Johns County Sheriff's Office.

Sheriff Robert Hardwick explained how the Flock system worked. Discussion ensued about the location of the Flock cameras, a workshop to address them, and state compliance.

Murphy *requested Board consensus to direct staff to bring back options for funding Flock cameras in County rights-of-way within the next few weeks.* **Consensus was given.**

Discussion ensued on a millage rate reduction.

Murphy made a motion to reduce the millage rate by 0.0469 percent below the flat rate. The motion failed for lack of a second.

Motion by Whitehurst, seconded by Joseph, carried 4/1, with Murphy dissenting, to adopt Resolution No. 2026-313, approving the Fiscal Year 2027 Final Millage Rates as set by the Board of County Commissioners of St. Johns County, Florida, for all property in St. Johns County, as of January 1, 2026.

Yea: Whitehurst, Joseph, Taylor, Arnold

Nay: Murphy

RESOLUTION NO. 2026 - 313

RESOLVED, that the following **FISCAL YEAR 2027 FINAL MILLAGE RATE** is hereby set by the Board of County Commissioners of St. Johns County, Florida, for all property in St. Johns County, as of January 1, 2026.

General Fund	4.4999
County Transportation Trust Fund	0.8444
County Health Unit Trust Fund	0.0160
Fire District, Countywide, <i>Except City of St. Augustine</i>	1.4700
St. Augustine South Street Lighting District	0.1268
Vilano Street Lighting District	0.0303
Summerhaven M.S.T.U.	7.3392
Coastal Highway M.S.T.U.	0.5000
South Ponte Vedra Beach Dune & Beach Restoration M.S.T.U.	2.0000
Serenata Beach Dune & Beach Restoration M.S.T.U.	0.5500
Ponte Vedra Beach Dune & Beach Restoration M.S.T.U.	0.0000
AGGREGATE MILLAGE RATE	6.7559
Aggregate Rolled-back Rate	6.6143
<i>Percentage increase in Property Taxes from rolled-back rate:</i>	<i>2.14%</i>

Motion by Whitehurst, seconded by Taylor, carried 4/1, with Murphy dissenting, to adopt Resolution No. 2026-314, approving the Fiscal Year 2027 Final Budget of the Board of County Commissioners of St. Johns County, Florida, using the certified taxable value of \$63,056,698,242, generating an estimated \$426,006,002 in taxes, and resulting in a total budget of \$1,939,752,566.

Yea: Whitehurst, Taylor, Joseph, Arnold

Nay: Murphy

RESOLUTION NO. 2026 - 314

RESOLVED, that the following **FISCAL YEAR 2027 FINAL BUDGET** of the Board of County Commissioners of St. Johns County, Florida, developed using the certified taxable value of \$63,056,698,242, generating an estimated \$426,006,002 in taxes, is hereby adopted, resulting in a total budget of \$1,939,752,566 as follows:

General Fund	\$543,610,743
Special Revenue Funds	
- Transportation Trust	\$204,279,506

- Fire District	114,972,336
- Health Department	977,629
- Building Services	23,536,917
- Tourist Development	41,538,897
- Impact Fees - Public Buildings	36,991,488
- Impact Fees - Police Services	5,095,861
- Impact Fees - Fire Rescue	15,612,491
- Impact Fees - Conservation	357,460
- Impact Fees - Roads	105,173,601
- Impact Fees - Parks	23,246,749
- Beach Services	6,229,105
- County Pier	753,802
- Golf Course	5,482,433
- Alcohol & Drug Abuse Trust	242,209
- Community Based Care	14,604,947
- Transit System	9,537,951
- State Housing Initiative Partnership	6,832,453
- Tree Bank	2,390,125
- Sidewalk Mitigation	63,758
- E-911 Communications	2,828,817
- Law Enforcement Trust	13,022
- Crimes Prevention Trust	104,532
- Court Innovation	327,735
- Legal Aid	384,988
- Law Library	65,589
- Juvenile Alternative Programs	80,241
- Court Technology	10,922,150
- Communications Surcharge	786,359
- Florida Boating Improvement	560,367
- Northwest Tower	509,573
- Court Facilities Trust	482,235
- Driver's Safety Education	92,964
- American Recovery Plan	5,944,830
- Emergency Rental Assistance	273,039
- FEMA Emergency Disaster Relief	354,137
- FEMA Emergency Disaster Events	51,331,897
- Opioid Settlement Funds	493,879
- Equitable Sharing Justice	21,248
- Equitable Sharing Treasury	65,820
- Equitable Sharing Task Force	7,132
- West Augustine CRA	2,210,932
- Flagler Estates CRA	1,105,075
- Vilano CRA	1,048,097
- Vilano Street Lighting District	53,445
- Elkton Drainage District	176,334

Special Revenue Funds Continued

- St. Aug. South St. Lighting District	\$150,980
- Treasure Beach M.S.B.U.	229,997
- Summer Haven M.S.T.U.	1,156,505
- Durbin CTITF	584,015
- Coastal Hwy Dune & Beach M.S.T.U.	84,411
- SPV Blvd Dune & Beach M.S.T.U.	601,688
- Serenata Beach M.S.T.U.	52,292

Debt Service Funds

- Trane Capital Lease	\$120,781
- Public Facility Note	410,923
- 19 CBA Refunding Bond	1,449,750
- 20 Special Obligation Revenue Note	764,732
- 21 Taxable Special Obligation Bonds	5,016,360
- 22 Special Obligation Bonds	1,059,446
- 22A Special Obligation Note	311,970
- 24 HUD 108 Loan Note	424,073
- 24 Special Obligation Bonds	1,105,500
- 24A Special Obligation Bonds	8,616,500
- 25 Special Obligation Bonds	5,201,000

Capital Improvement Funds

- Beach Re-Nourishment Projects	\$5,121,893
- SR 207 CIG Developers Projects	2,839,926
- 2019 Capital Projects	3,193,237
- Coastal Hwy Dune & Beach Project	2,119,208
- PV Beach Dune & Beach Project	200,645
- SPV Beach Dune & Berm Project	235,986
- LAMP	5,566,750
- County Capital Improvement Projects	15,507,189
- Hastings Community Center & Library	2,580,452
- Porpoise Point Stabilization	1,536,588
- FY 25 Capital Improvement Projects	70,950,172

Enterprise Funds

- Solid Waste Management	\$68,452,804
- Utility Services	417,358,335

Internal Service Funds

- Worker Compensation Insurance	\$3,765,704
- Health Insurance	63,980,501

Trust & Agency Funds

- FSA-Medical	\$1,143,802
- FSA-Dependent	209,748
- OPEB Trust	5,873,805

2. Discussion on Black History Museum

Murphy spoke on a request for \$125,000 in funding for the Black History Museum. Discussion ensued on funding for the Black History Museum Foundation. Howard Holley, President and Chairman of the Foundation for the Museum of Black History, spoke on the need for funding for the museum.

Motion by Murphy, seconded by Arnold, carried 4/1, with Joseph dissenting, to waive Board Rule 4.304 regarding funding on a non-published agenda.

Yea: Murphy, Arnold, Whitehurst, Taylor

Nay: Joseph

Motion by Murphy, seconded by Arnold, carried 3/2, with Taylor and Joseph dissenting, to remove \$125,000 from the General Fund Revenue for the Black History Museum.

Yea: Murphy, Whitehurst, Arnold

Nay: Taylor, Joseph

COMMISSIONERS' REPORTS

No reports.

COUNTY ADMINISTRATOR'S REPORT

No report.

COUNTY ATTORNEY'S REPORT

No report.

REPORTS:

There were none.

CORRESPONDENCE:

There was none.

With there being no further business to come before the Board, the meeting adjourned at 7:18 p.m.

Approved _____, 2026

BOARD OF COUNTY COMMISSIONERS
OF ST. JOHNS COUNTY, FLORIDA

By: _____
Clay Murphy, Chair

ATTEST: BRANDON J. PATTY,
CLERK OF THE CIRCUIT COURT & COMPTROLLER

By: _____
Deputy Clerk

Draft



EXHIBIT A

BCC September 15, 2024
Agenda Item No. SPC01
Presenter: Kaleigh Masters

FY 2027 Final Millage Rates

SJC BCC Taxing Authority	FY 2026 Adopted	FY 2027 RBR	FY 2027 Final
General Fund	0.0000	0.0000	0.0000
County Governmental Services Fund	0.0444	0.0444	0.0444
County Health and Trust Fund	0.0160	0.0160	0.0160
Fire District, Countywide (adopted City of SA dog)	1.4990	1.4730	1.4730
St. Augustine South Street Lighting District	0.1268	0.1268	0.1268
Wabash Street Lighting District	0.0381	0.0381	0.0381
Summerhaze MSTU	7.3381	7.4675	7.4675
Coastal Ridge MSTU	0.5500	0.4800	0.4800
S. Dunbar Vedral House & Beach Restoration MSTU	0.0000	0.0000	0.0000
Savanna Beach MSTU	0.1100	0.1100	0.1100
Ponte Vedra 1 House & Beach MSTU	-	-	-
Ponte Vedra 2 House & Beach MSTU	-	-	-
Seaside Beach MSTU	-	-	-

EXHIBIT B

BCC September 15, 2026
 Agenda Item No. SPC01
 Presenter: Joseph Miller

The Flock / ALPR System in St. Johns County: A Risk Assessment

Packet for the Board of County Comm's's'oners, September 15, 2026

Submitted for the record by Sterling Seizert, Nocatee

EXHIBIT C

BCC September 15, 2024
Agenda Item No. SPC01
Presenter: Sterling Seizert

Contents

Tab	Document
Cover	Cover letter
1	Summary of Findings
2	One-Page Commissioner Handout
3	Professional Assessment: What This System Is, and Who Decides When It Grows
4	Contract Findings
5	Policy 41.35, News Release, and Order Form Findings
6	Wyden and Krishnamoorthi Letter to the FTC, November 3, 2025
7	Precedent Map
8	Florida Toll Road Surveillance
9	Documented ALPR Misuse Incidents (reference)
10	Flock Contract Cancellations by Agency, with Northeast Florida snapshot (reference)
11	Requested Outcome, Immediate Steps, and Fallback Conditions
Appendix	Primary documents (contents listed at the end of the packet)

Terms used 'n th's packet

The Flock / ALPR system. This packet's subject is the full package of license plate reader technology and infrastructure the Sheriff's Office operates through Flock Safety, not any one part of it. It consists of the fixed and portable cameras on county roads and property; the vendor-hosted archive of every scan, retained one year under Sheriff's Policy 41.35; the vendor's products that join those records to other data; the sharing relationships with outside agencies; and the contractual and technical means by which the vendor can change any of those after purchase. The packet asks the Board to evaluate that system as a whole, not the device on the pole, and it concludes that the county should not host it.

ALPR / LPR. Automated license plate reader. **Hot list.** A watch list of plates; a match produces a real-time alert. **Vehicle Fingerprint.** The vendor's search by make, model, color, decals, and damage. **National Lookup.** The vendor's cross-agency search network, available to agencies that share their own data. **Nova / OS Investigate.** Vendor products that join plate data to people-lookup records and analyze movement patterns. **MFA.** Multi-factor authentication. **CJIS.** The FBI's security policy for criminal justice data. **Pattern of life.** A person's routine movements, locations, and associations built from repeated observation. **s. 30.49 / s. 30.53, F.S.** The statutes governing the Board's role in the Sheriff's budget and the Sheriff's independence in purchasing. **Non-appropriation clause.** A contract term ending the agreement without penalty if funds are not appropriated.

Cover Letter

Sterling Seizert, Nocatee, Florida, sterling@patriotcapitalllc.com. September 15, 2026. St. Johns County Board of County Commissioners, 500 San Sebastian View, St. Augustine, Florida 32084.

Chair Murphy, Vice Chair Taylor, Commissioners Joseph, Arnold, and Whitehurst:

I am a St. Johns County resident and a former Army Special Forces intelligence sergeant who built pattern-of-life analysis for a living. I submit this risk assessment for the record with my public comment at the September 15, 2026 budget hearing. It concerns the full Flock license plate reader system the Sheriff's Office operates: a roughly 180-camera network across the county, a vendor-hosted archive of every scan, sharing with outside agencies, and a platform whose capabilities expand after purchase.

I am not alleging misconduct by the Sheriff or any deputy. My position is that this system should not exist in St. Johns County, and that removal, not regulation, is the durable remedy. The reasons are cumulative and each is documented in the tabs that follow:

1. The system records the plate, description, time, and location of passing vehicles and retains every scan for one year under the Sheriff's policy. The last figure given to the public was 30 days.
2. In a grant application approved September 11, 2025, the Sheriff's Office told the State that one year of storage "allows law enforcement to develop a pattern of life to potentially identify home and work locations," and committed to sharing the data with ICE and CBP.
3. The data sits on vendor infrastructure under an agreement granting the vendor perpetual rights that survive termination and permitting assignment without the Sheriff's Office's consent. The county does not host it, and I found no right in the agreement produced allowing the county to audit the vendor's use of it.
4. Congressional investigators documented stolen Flock customer credentials in criminal markets, accounts advertised on a Russian-language cybercrime forum, and federal agents using a local detective's login undetected. Safeguards added since are vendor-controlled.
5. Capability attaches to the system after purchase: retention went from 30 days to a year on an order form; a sharing setting was switched on in another city without the police department's knowledge; the vendor's newest products join plate data to identity records and analyze movement.
6. The program is not identified on the budget page the Board votes on: one line last year, \$103,058,446; one line this year, \$109,234,299.

Tab 3 explains why these facts describe a strategic vulnerability rather than manageable risks: the archive has intelligence value independent of its stated purpose, layering ordinary records on it builds a picture of a person, automation lowers the cost of doing so, and neither the capability nor the intent that will act on the data has to exist when it is collected. A useful tactical tool can still create a vulnerability the county should not accept.

The requested outcome, set out in Tab 11, is removal: readers off county-controlled rights-of-way and property, as St. Lucie County voted on September 1, and no cameras, archive, or vendor platform hosted with county support. The immediate steps, within the Board's authority as counsel confirms it: reduce the law enforcement transfer by \$481,000, the county-funded cost of the program by the Sheriff's own account, with a stated finding; and direct the County Attorney to define the Board's authority over county funds, county property, and the agreement's non-appropriation clause, reporting back at a workshop. Tab 11 lists fallback conditions only if the Board declines removal.

Do not build the surveillance architecture first and hope policy can contain what it becomes. Respectfully,
Sterling Seizert

Tab 1: Summary of Findings

Why this matters to the Board: These facts, from the Sheriff's Office's own documents and the vendor's own statements, are cumulative reasons why this system, the cameras, the archive, the vendor platform, and the sharing relationships, should not be hosted in this county. They show why rules written around today's configuration cannot by themselves eliminate the risks of future capability expansion.

Every finding below is drawn from a document in hand or a named published source. The source for each is identified in the Master Claims Register, which is available to any commissioner or staff member on request.

The program

The St. Johns County Sheriff's Office operates roughly 180 Flock Safety license plate readers, by its own count, and has used the technology since 2017. Each camera records the plate, the vehicle's make, model, and color, distinguishing features such as decals and damage, the time, and the location. Under Sheriff's Policy 41.35, section .30, all scanned data is retained for one year and purged automatically at the end of that period. Retention of up to three years is permitted under the state's General Records Schedule; one year is lawful, and the question presented is governance, not compliance. The vendor's platform supports cross-agency searches; whether the Sheriff's Office shares its data through the vendor's national network has been requested and not yet established.

The base record does not contain the registered owner's name. A deputy obtains the name through a separate authorized query of the state driver and vehicle databases. The vendor's Nova product, reported by 404 Media in May 2025 from internal company materials, joins plate data to roughly 20 third-party data sources so that a user can move from a plate to a person and to that person's relatives and associates. Whether the Sheriff's Office subscribes to Nova has been requested and not yet answered.

The retention record

In February 2023, a Sheriff's Office spokesman told First Coast News that the readers purge every 30 days. An order form effective October 1, 2023 extended retention to 365 days across 137 units for a 60-month term at a total of \$1,955,500. The policy amendment of June 7, 2024 codified one-year retention for all scanned data. The Sheriff's Office's 2026 news release does not state a retention period and says the cameras do not continuously track where someone travels. I have not identified a public notice announcing the change.

The Sheriff's Office's stated purpose

In its application to the State Board of Immigration Enforcement, application IG039, approved September 11, 2025 and posted in the Board's September 30, 2025 cabinet package on FDLE's website, the Sheriff's Office budgeted 23 Flock license plate readers at \$427,050 and nine LPR trailers, and wrote: "The LPR scan captures the date, time and location of passing vehicles and the data is stored for up to one year. We will share this data with federal agencies including ICE and CBP. If ICE or CBP is searching for a specific person (for example, someone with an outstanding deportation order), LPR data can be used to track where their vehicle has been spotted. This allows law enforcement to develop a pattern of life to potentially identify home and work locations and plan enforcement actions." The application adds that the trailers "can be deployed to various check points or areas with the county as intelligence dictates." The Chief Financial Officer's office announced the one million dollar award on October 21, 2025. The relevant pages are in the appendix. The 23 cameras and \$427,050 in the application match, to the unit and the dollar, the December 17, 2025 order form with 365-day retention produced under the records request.

The vendor's own benchmark

On August 13, 2026, Flock announced that its recommended default retention is now seven days, based on its analysis that more than 90 percent of searches without a full plate occur within one week, and introduced a feature to preserve specific records for active investigations. Existing customers keep their current retention unless they opt in. The vendor recommends seven days. The Sheriff's Office retains 365.

The executed agreement

The agreement produced under public records request R042893-082726 grants the vendor a perpetual, irrevocable license to use the Sheriff's Office's Agency Data as part of aggregated data, a perpetual license to improve "other Flock offerings," and a disclosure license that survives termination. The agreement also states that Flock shall not sell Agency Data. Section 10.2 permits the vendor to assign the agreement without the Sheriff's Office's consent. The data is hosted on vendor infrastructure and accessed by the Sheriff's Office through a web interface; the county does not host it. No CJIS Security Addendum appears in the 113 pages produced. The 2023 special terms include a non-appropriation clause under which the absence of appropriated funds renders the agreement null and void without penalty. The December 2025 order form references a "FLOCK-updated Law Enforcement Agreement" that has not been produced, so which terms govern that order is unresolved.

Security

On November 3, 2025, Senator Ron Wyden and Representative Raja Krishnamoorthi asked the Federal Trade Commission to investigate Flock. Congressional staff identified at least 35 Flock customer credentials stolen by malware, a researcher provided a screenshot of Flock accounts advertised on a Russian-language cybercrime forum, and Flock confirmed that it did not require multi-factor authentication. The letter states that by not requiring multi-factor authentication, the vendor "has needlessly exposed Americans' sensitive personal data captured by the company's surveillance cameras to theft by hackers and foreign spies," and that anyone who gains access to a customer account with national lookup enabled "can misuse it to track Americans across the country." In Palos Heights, Illinois, DEA task force agents routinely used a local detective's login without detection. Flock made multi-factor authentication mandatory in August 2026 and will require case codes and misuse detection for all law enforcement customers by the end of the year. Those safeguards are vendor-controlled and were added after deployment.

Vendor changes w'thout customer knowledge

In February 2026, the Mountain View, California police chief disabled all 30 of the city's cameras after a national sharing setting was found switched on without the department's knowledge. In February 2026, Flock revised its standard terms, removing the sentence "Flock does not own and shall not sell Customer Data" and adding a perpetual license that survives termination; Flock states the deletion was redundant. In August 2026, WIRED reconstructed Flock's next-generation investigative software from the company's own files and found prompts that identify witnesses and associates from movement patterns, fourteen of which require no plate, name, or description to begin. Flock says the product is in development with a small group of agencies.

Misuse

The Washington Post's August 19, 2026 investigation counted at least 69 police officials accused, charged, or convicted of misusing plate reader systems, and found that in at least 15 cases someone outside the department identified the misuse first. Sheriff's Policy 41.35 requires random audits and an annual program evaluation. Those documents were requested on August 27, 2026. The Sheriff's Office marked the request complete and fully released on September 3 without producing the audit logs.

The budget

In the county's published financial plan for fiscal year 2026, the law enforcement appropriation appears at the summary level as a single transfer of \$103,058,446. The county's FY2027 Recommended Budget page, captured September 15, 2026, shows the same structure: Sheriff, Law Enforcement, Transfer to Officers, \$109,234,299, with the FY2027 Requested column blank and the program not identified. The Sheriff's separate submission under s. 30.49 has been requested; whether it identifies the program or the vendor has not yet been verified. The Sheriff's text to commissioners, as published, states that \$908,000 was spent on the technology in fiscal year 2026, \$481,000 from his budget and the balance from grants. The program is not identified in the county's published financial plan.

The region and the state (corroboration; status verified through September 9, 2026)

Governor DeSantis publicly raised concerns about the expansion of automated plate readers, and on August 31, 2026 the Florida Department of Transportation revoked permits for plate readers in state rights-of-way and ordered their removal within 30 days. Local agencies then made their own decisions. Duval County discontinued use countywide. Clay, Nassau, Putnam, Baker, Bradford, Volusia, and others ended or suspended their programs. Flagler County's sheriff suspended Flock use while publicly defending the technology and calling for strong protections, which shows the regional response includes regulated-use positions as well as discontinuation. On September 1, 2026, the St. Lucie County Commission voted 3 to 2 to remove plate readers from county-controlled roads. The Sheriff's Office has said it will comply on state roads; the fate of the cameras on county roads has not been stated. The Sheriff's Office's public statement says it "supports the development of legislation which addresses concerns around LPR technology and establishes clear standards for its use." The workshop requested in this packet is a way for the Board to determine what authority it has to remove county support for the existing system rather than wait for future state legislation.

The vendor in Tallahassee

Florida's lobbyist registration records show four lobbyists registered for 2026 with Flock Safety as a principal, for both chambers of the Legislature; two of the registrations use the Tallahassee address and phone number of Ballard Partners. The Sheriff's text to commissioners states that he is in contact with legislators and that the Board "will be pleased with the outcome." These facts are consistent with a legislative effort in the coming session. They do not establish coordination, and none is alleged. Lawful lobbying establishes nothing about the merits of the program; it bears only on whether the county should wait for state rules.

Tab 2: One-Page Commissioner Handout

The Flock / ALPR system 'n St. Johns County

What it is. Roughly 180 cameras recording the plate, description, time, and location of vehicles passing them, retained one year under Policy 41.35 §.30.

The retention timeline

Date	Event	Source
Feb. 2023	Public told data “purges every 30 days”	First Coast News
Oct. 1, 2023	60-month order: 365-day retention, 137 units, \$1,955,500	Order form
Sept. 11, 2025	Grant application approved: one year “allows law enforcement to develop a pattern of life”	SJSO application IG039 (FDLE)
Aug. 13, 2026	Vendor cuts recommended default to 7 days	Flock announcement

What the Board saw: FY2026 adopted, one line: **Transfer to Officers, \$103,058,446.** FY2027 recommended, one line: **\$109,234,299.** The program appears on neither page.

The region (verified through Sept. 9, 2026)

Jurisdiction	Action
Duval County	Discontinued countywide
Clay County	Removing all readers from county roads
St. Lucie County	Commission voted 3 to 2 to remove from county roads
St. Johns County	Complying on state roads only; county roads unaddressed

The requested outcome: removal. The immediate step: a workshop.

1. **Removal of the system.** Readers off county-controlled rights-of-way and property, as St. Lucie County voted on Sept. 1; no cameras, archive, or vendor platform hosted with county support. Any future plate-reading use is a separate public decision.
2. **Tonight and the workshop.** Under s. 30.49(4), reduce the law enforcement transfer by \$481,000, the county-funded cost of the program by the Sheriff's own account, with a stated finding; then direct the County Attorney to define the Board's authority over funds, county property, and the non-appropriation clause, inventory every reader on county property, and report within 45 days.
3. **Fallback only if the Board declines removal.** Disclosure of surveillance technology as a condition of funding; a vote before any expansion; a retention ceiling set in public; audits published.

Why removal, not regulation: retention went from 30 to 365 days on an order form; a sharing setting changed elsewhere without the police department's knowledge; capability arrives as a product. A grid that is not there cannot be expanded, breached, or repurposed.

Tab 3: Professional Assessment

Why this matters to the Board: This is the assessment of what the system can become without another public decision, written by a resident who built pattern-of-life analysis for a living, and it concludes that the county should not host the system. The immediate steps are a budget reduction tied to the program on the record and a workshop with the Board's authority defined by counsel.

What Th's System Is, and Who Dec' des When It Grows

Annex to the St. Johns County Board of County Comm'ss'oners packet

Sterling Seizert, Nocatee, Florida. Former Army Special Forces Intelligence Sergeant (18F), 2nd Battalion, 10th Special Forces Group

1. Purpose of th's assessment

I served twelve years in Army Special Forces as an intelligence sergeant. From 2016 to 2021 I ran the exploitation of captured cell phones and drones downrange and trained SOCOM soldiers to do the same. I completed formal training in physical surveillance, technical surveillance, technical exploitation, and exploitation analysis, the discipline that converts collected data into targeting decisions in the find, fix, and finish cycle. I operated a program that applied hostile surveillance and foreign intelligence tactics against U.S. special operations units during training exercises in order to teach those units how they could be exploited. I also participated in Defense Threat Reduction Agency assessments of U.S. government facilities, evaluating security-in-depth postures for vulnerabilities that a hostile individual, organization, or foreign intelligence service could exploit. The core of that work was pattern-of-life analysis: taking repeated observations of a person, a vehicle, and a device and building a reliable picture of where that person sleeps, where he works, which routes he drives, whom he meets, and when he will be at a given place.

I am submitting this assessment because the public debate has focused on whether a camera on a pole is acceptable, and that is not the decision in front of the Board. The decision is whether this county should host this system at all, the cameras, the vendor-hosted archive, the sharing relationships, and the platform that grows around them, knowing what it is permitted to become, who is allowed to decide that, and whether anyone in this county would know when it happens. My assessment is that it should not.

I am not alleging misconduct by the Sheriff or by any deputy. I am identifying a structural problem. The Sheriff's Office answers to voters, has published a written policy, and has an audit obligation. Present leadership and present intentions do not constrain what the system can do next, and they do not constrain the vendor whose platform it runs on.

2. The Sher'ff's Office has already stated what one year of data 's for

There is no need to speculate about whether a year of license plate data supports pattern-of-life analysis, because the Sheriff's Office has stated in writing that it does.

In its application to the State Board of Immigration Enforcement, application IG039, approved September 11, 2025 and posted in the Board's September 30, 2025 cabinet package on the Florida Department of Law Enforcement's website, the Sheriff's Office budgeted 23 license plate readers and nine trailers and stated: "The LPR scan captures the date, time and location of passing vehicles and the data is stored for up to one year. We will share this data with federal agencies including ICE and CBP. If ICE or CBP is searching for a specific person (for example, someone with an outstanding deportation order), LPR data can be used to track

where their vehicle has been spotted. This allows law enforcement to develop a pattern of life to potentially identify home and work locations and plan enforcement actions.” It added that the trailers “can be deployed to various check points or areas with the county as intelligence dictates.” The award of \$1 million was announced on October 21, 2025. The pages are attached behind this annex.

That request describes using the capability against specific individuals in an immigration enforcement context. I agree that the data permits exactly that analysis. My concern is different. The system can produce that analysis retrospectively only because it first collects and retains, for a full year, the movements of people who were not subjects of any investigation when the data was collected. The subject of the analysis is chosen later. The collection happens first, on vehicles passing the network.

3. The State of Flor'da has already acted on the governance question

On August 31, 2026, the Florida Department of Transportation revoked all permits for automated license plate readers in state highway rights-of-way and ordered their removal within 30 days, citing privacy concerns, reports of misuse, and the rapid growth of surveillance technology. The Sheriff's Office has stated that it will comply on state roads while continuing to defend the value of the technology. The state's order does not reach county roads.

This is no longer a concern raised only by privacy advocates. The state concluded that the governance surrounding these systems on its own rights-of-way required intervention. The Board now has the opportunity to answer the same governance question for the portion of the Sheriff's Office's roughly 180-camera network located outside state rights-of-way.

4. What the system 's

The system has three layers. I describe them at the level of function only. I will not describe parts, methods, or configuration, and I would decline to do so if asked. The purpose of this section is not to speculate about what may someday be technically possible. Each of the three layers described below already exists as a deployment, a product, or a stated analytical purpose.

Layer 1: Observation. Each camera records the plate, the vehicle's make, model, and color, distinguishing features such as decals and damage, the time, and the location. Under the Sheriff's own Policy 41.35, section .30, all scanned data is retained for one year. This layer is fully deployed in St. Johns County.

Layer 2: Enrichment. Observations are joined to other data associated with the vehicle or the person: registration records, commercial data broker records, and records from other agencies. This layer is a product. In May 2025, 404 Media reported, from internal presentation slides, company chat messages, and meeting audio, that Flock's Nova product joins plate data to roughly 20 third-party data sources so that a user can “jump from LPR to person” and to that person's relatives and associates, and that the product was already in early access with law enforcement agencies. Flock publicly responded that Nova does not use data obtained from breaches. I note the company's response. The point stands: the vendor expanded from vehicle identification toward person-level investigation as a product decision, without any county-level public decision.

Layer 3: Correlation. Repeated observations are analyzed across time and location to establish routines, relationships, and patterns of life. This is the analysis my team performed by hand, on one subject at a time, over weeks, under a defined chain of authority, mission rules, and oversight. This capability is no longer theoretical. On August 19, 2026, WIRED reported that its reporters reconstructed Flock's next-generation investigative software from files served by the company's own login pages. The software, first called Nightshift and since renamed OS Investigate, ships with 69 prewritten prompts. Nineteen of them are built around patterns of movement, and fourteen require no plate, name, or physical description to begin. One prompt identifies likely witnesses by finding the vehicles most often seen in a neighborhood over the previous 14 days. Another surfaces a driver's “associates” from the cameras their vehicles pass together.

Because the software also reaches police case files, 911 dispatch logs, and commercial identity records, WIRED reported, plates can be turned into names, home addresses, and relatives. Flock told WIRED that the product remains in development and is being tested with a small group of law enforcement agencies. For years, the company's public materials stated that its technology "cannot recognize, identify, or track individuals." Separately, the Sheriff's Office has told the State of Florida that its one-year retention period is what enables pattern-of-life analysis.

Layer 1 is deployed here. Layer 2 exists as a Flock product. Layer 3 exists as a Flock product under development, and it is also the analytical purpose the Sheriff's Office itself has given for one-year retention. What I have not identified is a separate public process requiring approval when the system materially expands.

5. The vendor can change the system w'thout the county's knowledge

This is the concern I want the Board to take most seriously, because it is documented.

In February 2026, the Chief of Police in Mountain View, California ordered all 30 of the city's Flock cameras disabled after discovering that a national data-sharing setting had been switched on for one of the city's cameras, allegedly by the vendor, without the city's knowledge, in a state where that sharing is prohibited by statute. The chief stated that he continued to support license plate reader technology but no longer trusted the vendor.

In St. Johns County, the retention period changed from 30 days, as described to the public in February 2023, to one year fleet-wide seven months later. The change appears in an order form. I found no corresponding public Board vote. No allegation of misconduct is necessary to make the point: a material expansion in surveillance capability occurred without a separate public decision. That is the governance mechanism I am concerned about. Material changes to the system can occur through settings, order forms, and product updates without a separate public decision.

In February 2026, Flock revised its standard terms and conditions. According to the American Civil Liberties Union's review of those terms, the company removed the sentence "Flock does not own and shall not sell Customer Data," added a perpetual, irrevocable license to use customer data that survives termination of the contract, and granted itself "the exclusive right to determine and control the method, timing, format, and medium" of the customer's access to its own data. Flock has stated that it removed the no-sale sentence because it was redundant, that it does not sell customer data, and that customer ownership and control are unchanged. I am not characterizing the company's motives. I am noting that the standard terms Flock offers its public-sector customers changed, and that the change was made by the vendor.

The company has an economic incentive to expand the value and capability of its platform. It has demonstrated that expansion with Nova and with OS Investigate. It has demonstrated that settings can change without the customer's knowledge. It has demonstrated that its standard terms move over time. None of this requires bad faith. It requires only that a company do what companies do, inside a contract that permits it.

6. What the executed St. Johns County agreement perm'ts

The following provisions are quoted from the executed agreement between the Sheriff's Office and Flock Safety, produced under public records request R042893-082726. The relevant pages are attached behind this annex. These are the executed terms produced by the Sheriff's Office in response to my request. As discussed below, whether they govern the December 2025 order in whole or in part has not yet been established.

- Section 4.2 states that all right, title, and interest in Agency Data belongs to the Sheriff's Office, and in the same section grants Flock "a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify and distribute the Agency Data as a part of the Aggregated Data."

- Section 4.4 grants Flock a perpetual license to use Aggregated Data to improve the Services “and other Flock offerings.” The same agreement states that Flock shall not sell Agency Data.
- Section 4.1 grants Flock “a non-exclusive, worldwide, perpetual, royalty-free right and license (during and after the term hereof)” to disclose Agency Data for hot list monitoring and investigative search access. Section 6.6 provides that Section 4 survives termination.
- Section 10.2 permits Flock to assign the entire agreement without the Sheriff’s Office’s consent.

The agreement names the capabilities that exist. In my review of the 113 pages produced, I found no provision expressly stating that the vendor will not add new data types or capabilities to the platform serving this county, will not join the Sheriff’s Office’s Agency Data to commercial records, or will not add data sources. The agreement grants Flock specified perpetual licenses involving Agency Data and Aggregated Data, described above, and it permits transfer of the relationship to another company without the Sheriff’s Office’s consent.

One further point requires the County Attorney’s attention. The December 17, 2025 order form references a “FLOCK-updated Law Enforcement Agreement.” The terms produced to me are the 2022 agreement. Which terms govern the most recent order, and whether the February 2026 revisions apply to any part of the county’s relationship, has not been established.

7. Security, and what the vendor’s recent changes show

On November 3, 2025, Senator Ron Wyden and Representative Raja Krishnamoorthi asked the Federal Trade Commission to investigate Flock. Congressional staff found at least 35 Flock customer account passwords stolen by malware and circulating in criminal markets, a security researcher provided the offices with a screenshot of Flock accounts advertised on a Russian-language cybercrime forum, and Flock confirmed to Congress that it did not require multi-factor authentication. In Palos Heights, Illinois, agents on a DEA task force routinely used a local detective’s Flock login to run searches, and the system did not detect it.

On August 13, 2026, Flock announced that multi-factor authentication is now mandatory, that case codes and automated misuse detection will be required for all law enforcement customers by the end of 2026, and that accounts showing abnormal activity will be locked automatically. Those improvements are welcome. They also demonstrate the central point of this assessment. Every one of those safeguards is a feature controlled by the vendor and added after deployment. Vendor-controlled safeguards can also be revised unless they are independently fixed by contract, policy, or law.

In the same announcement, Flock reduced its recommended default retention period from 30 days to seven, stating that its own analysis shows more than 90 percent of searches conducted without a full plate number occur within one week, and introduced a feature to preserve specific records for active investigations beyond that period. Existing customers keep their current retention unless they choose to change it. The company that sells this system now recommends seven days. The Sheriff’s Office retains data for 365 days. The Sheriff’s Office has already told the state what the additional 358 days are for.

8. The strategic vulnerability is the infrastructure itself

The sections above describe what the system collects, what the Sheriff’s Office has said the collection is for, how the vendor can change the system, what the contract permits, and what the security record shows. This section explains why those facts add up to a strategic vulnerability rather than a list of manageable risks, and why the answer is architectural.

Movement data has intelligence value independent of the purpose for which it was collected. The same repeated observations that let law enforcement identify a subject’s home, workplace, routes, and patterns have the same value to a criminal organization, a hostile intelligence service, a stalker, or any other actor who obtains sufficient access. The value does not depend on who is holding the data or why it was gathered. It depends only on the data existing.

In my former work, turning that data into a picture of a person was called layering. A location layer tells you where and when a vehicle was; that is what this system produces, and the longer the history is retained, the more complete that layer becomes. An identity layer links the plate to an owner record; in Florida that can be done through an authorized query of the state driver and vehicle databases. A commercial layer can add addresses, phones, relatives, and associates from data brokers. Open-source information can add affiliations, interests, associations, and publicly expressed views. Each layer may look ordinary on its own. Stacked together, they become an intelligence picture of a person: identity, movements, routines, associations, and tendencies. The vendor has now begun building that kind of fusion into its own products, as Section 4 describes: Nova joins plate data to roughly 20 commercial sources, and OS Investigate reaches case files, dispatch logs, and identity records. The plate-derived location layer, the one that starts the process, is the one this county is helping create and retain.

Technology lowers the cost of every step in that process. Cameras lower the cost of collection, retention lowers the cost of retrospective search, networks lower the cost of sharing, and machine learning lowers the cost of correlation and analysis. Work that once required trained analysts, deliberate collection, and significant time can increasingly be performed by software at speed and scale. The vendor's own investigative software, reconstructed by WIRED in August 2026, identifies witnesses and associates from movement patterns with prompts that need no plate, name, or description to begin. Artificial intelligence does not create the surveillance. It lowers the cost of exploiting information already collected.

That has a consequence the Board should weigh carefully. The analytical capability does not have to exist at the time the observations are collected, and neither does the intent. A dataset retained under one administration, for one stated purpose, can remain available to a later administration, a different agency, or another authorized user operating under a different purpose. If the historical information still exists when a new capability or a new mission arrives, it can be applied to records collected under an earlier understanding of what the system could do and what it was for.

That is why the security question is larger than whether someone can breach the Sheriff's Office. Once historical movement data exists in a vendor-hosted and interconnected system, every authorized pathway to that data becomes part of the security boundary protecting it. The executed agreement places the data on vendor infrastructure. The Sheriff's Office has committed to sharing grant-related data with ICE and CBP. Congressional investigators have documented compromised Flock credentials and federal agents using another agency's credentials without detection. None of that establishes that St. Johns County data has been compromised. It establishes why the existence of the dataset matters, and why the perimeter around it is not one the county controls.

It also identifies who has the most to gain from that archive. The Department of Defense has warned that geolocation capabilities can expose the locations and routines of its personnel and create increased risk to the force and mission. For military personnel and their families who live in or travel through this county, that risk is not abstract. A year of a family's movements can reveal the home, the routine, a spouse's commute, a child's school, and the day the routine changes because someone deployed. That is the information a hostile service uses to select and pressure the people it wants, and building that picture was my job.

None of this concerns the intent of this Board or of the Sheriff. It concerns the parties whose intent no one here can know: whoever holds a compromised credential, whichever outside agency is authorized access through a sharing relationship, whichever future administration inherits the archive, and whichever vendor or acquirer holds the rights to it. Misuse of trusted access inside law enforcement is documented across agencies and jurisdictions; The Washington Post counted at least 69 officials accused, charged, or convicted of misusing these systems, and in at least 15 of those cases someone outside the agency found it first. And the archive records vehicles without regard to whose they are. Absent specific exclusions, the system has no inherent reason to treat the vehicles of deputies or their families differently from any other vehicle passing the network. The Sheriff's Office takes threats against its own people seriously, and it should. The residents of this county, including military and intelligence professionals and their families, have the same interest in preventing their movements from becoming exploitable intelligence.

The tactical benefits of the system are real, discrete, and measurable: a stolen vehicle recovered, a missing person located, a suspect identified. The strategic exposure is different in kind. It is cumulative. Every retained observation enlarges the archive, every new access path enlarges the security perimeter, and every new analytical capability increases what can be extracted from data already collected. Tactical value therefore does not answer the architectural question. A tool can produce useful individual outcomes while creating a system-level vulnerability that government should not accept.

This is why better passwords, better audits, and shorter retention do not resolve the structural concern. They can reduce particular risks. They do not eliminate the intelligence value of the collection infrastructure itself, and they do not guarantee what that infrastructure will become under future technology, vendors, leadership, or missions. The strategic risk is both the historical archive created today and the surveillance infrastructure left in place for tomorrow. The durable way to eliminate that vulnerability is to remove the infrastructure.

9. What the Board controls, and what I am asking for

The Sheriff is an independent constitutional officer, and Florida law expressly protects his independence concerning the purchase and procurement of equipment. The Board nevertheless holds substantial budgetary authority under section 30.49, Florida Statutes, including the authority to amend, modify, increase, or reduce items of expenditure in the Sheriff's proposed budget and to require relevant and pertinent expenditure information, and it holds authority over county property and county rights-of-way generally, subject to law. The precise boundary between those authorities is a legal question for the County Attorney. I am therefore asking the Board for one outcome and two immediate steps, within whatever authority counsel determines is available, with fallback conditions if the Board declines the outcome.

The requested outcome: removal of the system. Readers off county-controlled rights-of-way and property, as St. Lucie County voted on September 1, 2026, and no cameras, archive, or vendor platform hosted with county support. The reason is architectural. A retention period is a setting; this county's own history shows it can change on an order form. A sharing setting can change without the customer's knowledge; Mountain View shows it. Analytical capability arrives as a product; Nova and OS Investigate show it. Infrastructure that is not there cannot be reconfigured, expanded, breached, or repurposed. Whether any plate-reading technology should be used in this county in the future is a separate decision for the Board to make in public, with its authority defined, rather than a feature of a system that already exists and grows on its own.

The first immediate step: the budget. At the September 15, 2026 final budget hearing, under section 30.49(4), the Board may reduce the law enforcement transfer by \$481,000, the county-funded cost of the program in fiscal year 2026 by the Sheriff's own account, and state on the record that the reduction corresponds to the license plate reader program and that the Board does not intend county funds to support it. The Sheriff may appeal such a reduction, and because the Board does not appropriate line by line, a reduced total does not by itself prevent the program from being funded from what remains. The reduction places the Board's intent on the record; whether it constitutes an absence of appropriated funds under the agreement's non-appropriation provision is a question for counsel.

The second immediate step: a workshop. Direct the County Attorney to review the executed agreement, determine which terms govern the December 2025 order, identify the enforceable mechanisms available to the Board, including the agreement's non-appropriation provision and the assignment and termination provisions, advise on the boundary between the Board's authority and the Sheriff's under sections 30.49 and 30.53, and report back at a workshop within 45 days. Direct staff to inventory every reader on county rights-of-way and property, including portable units, so that the Board decides with the facts in front of it.

Fallback conditions, only if the Board declines removal. Disclosure of surveillance technology in the Sheriff's annual submission as a condition of funding, with the audits and annual evaluations the Sheriff's policy already requires provided to the Board and the public; no new data type, data source, analytical

capability, or retention extension on county-funded or county-hosted infrastructure without public notice, a written record, and a Board vote; and a retention limit set in public and treated as a ceiling that requires a Board vote to raise. These are mitigations for an infrastructure I believe should not exist. They are not the objective, and a shorter retention period should not be mistaken for my position.

A policy governs the conduct of the people who work under it. It does not govern what the system is permitted to become. Policies and contracts can reduce risk. The only way to eliminate the risks created by this infrastructure is to remove it.

The question before the Board is not whether this vendor is trustworthy. It is whether St. Johns County should host a system whose ability to reconstruct the movements and associations of its residents can grow through software updates, new data sources, and additional access relationships.

I built pattern-of-life analysis for a living, under a defined chain of authority, mission rules, and oversight. I know how little data it takes and how quickly the capability grows once the collection exists. I am asking this Board not to build the surveillance architecture first and hope that policy can contain everything it becomes later.

Sterling Seizert

This assessment describes capabilities at the level of function and public documentation. It intentionally omits any information that would assist in constructing such a system. Every factual statement is sourced in the accompanying Master Claims Register.

Tab 4: Contract Findings

Why this matters to the Board: The executed agreement determines what the vendor may do with the data, how the relationship can be transferred, what contractual exit mechanisms exist, and which, if any, the Board can lawfully invoke. The perpetual data rights and the assignment clause are reasons the system should not be hosted; the non-appropriation clause is a potential path out.

Note: quotations below were checked against a scanned production processed by optical character recognition. Verify each quoted clause against the page-numbered scans in the Appendix before relying on exact wording. The recital language describing capability to capture “audio, image, and recordings” describes the vendor’s product suite generally; no document produced establishes that the deployed units capture audio. This tab consolidates findings from both productions; where the second production resolved a question left open by the first, the consolidated finding is stated.

SJSO-Flock Contract Production: Findings Memo

Source: 113-page production (R042893-082726), OCR-reviewed August 31, 2026. The bundle contains the June 2022 master Government Agency Agreement plus order forms and additional services agreements from 2022 through December 2025, with duplicates. Page numbers below refer to the PDF.

1. The retention finding (the headline)

The master agreement recites that Flock deletes all Footage on a rolling 30-day basis, and Section 4.2 repeats the 30-day auto-delete. The order forms tell a different story:

- An early additional services order purchased “Extended data retention (Up to 1 Year)” for 20 units at \$300 each (\$6,000/yr), alongside 5 Falcon Flex cameras (pp. 1-4)
- Order of March 21, 2025: “Retention Period: 360 Days,” extended 1-year retention for 18 cameras, \$4,754.61/yr, 24-month term, \$9,509.22 total (pp. 29-35, signed Shari Shuman, CFO)
- Order of December 17, 2025: “Retention Period: 365 Days,” with all 23 new cameras on the order (18 LPR, 2 Solar Long-Range, 3 Flex) carrying extended 1-year retention line items (pp. 22-28, signed Howard Cole)
- By contrast, the December 3, 2024 order states “Retention Period: 30 Days” for its 18 units (pp. 11-17)

Consolidated finding (updated after the second production): the October 1, 2023 order form, produced with the policy batch, carries 365-day retention on 137 units for a 60-month term; the March 2025 order extended 18 units to 360 days and the December 2025 order carries 365 days on 23 units. Policy 41.35 §.30 applies one-year retention to all scanned data. One-year retention is therefore the fleet-wide condition under the Sheriff’s own policy, purchased annually since 2023. The December 2024 order’s 30-day entry for 18 units was superseded in March 2025.

Retention law, stated accurately: s. 316.0778 directs the Department of State, in consultation with FDLE, to establish the retention schedule. The General Records Schedule for law enforcement (GS2) permits ALPR records to be retained until obsolete, superseded, or no longer of administrative value, but no longer than three anniversary years unless another records series applies. One-year retention is therefore lawful under the schedule. The question this packet raises is not compliance; it is whether one year is necessary and appropriately governed. Also note Section 4.1: Flock “may store deleted Footage” to comply with legal obligations, retrievable with a court order, so even 30-day deletion is not absolute.

2. The December 17, 2025 commitment

The December 17, 2025 order (pp. 22-28) was signed with: a 60-month initial term (running to roughly late 2030), 24-month auto-renewals, \$427,050 total, 23 new cameras, 365-day retention. Timing matters: this five-year commitment was signed months after Flock's CBP pilot admission (August 2025), after the Texas abortion-search story (May 2025), and in the middle of the national cancellation wave. It also postdates the \$1M state immigration-enforcement funding for network expansion. Question for the Board: was a five-year, \$427,050 obligation presented to or approved by the BOCC in the budget process?

3. Contractual exit mechanisms

Section 6.2, Termination for Convenience: SJSO "may self-elect to terminate this Agreement for convenience" at any time, effective immediately, for a one-time fee of \$500 per Flock Hardware unit, with a prorated refund of prepaid fees for Falcon cameras. Flock removes hardware at its own cost at natural expiration (2.7.4). At 182 documented units, the convenience-termination fee would be roughly \$91,000 before prorated refunds, assuming section 6.2 applies to every unit. Which mechanism, if any, the Board itself can invoke is a question for the County Attorney.

4. Data rights and custody

- Ownership on paper: Section 4.2 states all right, title and interest in Agency Data belongs to SJSO. Then the same section grants Flock (a) a license to use Agency Data as necessary to provide services, and (b) "a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify and distribute the Agency Data as a part of the Aggregated Data."
- Section 4.4: Flock compiles de-identified Aggregated Data from Agency Data and holds a perpetual license to use and distribute it to improve the Services "and other Flock offerings." The Falcon itself is described in the order forms as proprietary machine learning software; SJSO captures feed the product. Precision note: this is a de-identified aggregate license, not the "retain data for any purpose" language the LAPD IG found in that agency's agreements. Section 2.5's "any purpose in Flock's sole discretion" clause applies to Flock IP, not Agency Data. Quote it accurately.
- Section 4.4 also states Flock shall not sell Agency Data or Aggregated Data. Note it honestly.
- Section 4.1: SJSO "expressly grants Flock a non-exclusive, worldwide, perpetual, royalty-free right and license (during and after the term hereof)" to disclose Agency Data including Footage for law enforcement hotlist monitoring and investigative search access. Per Section 6.6, all of Section 4 survives termination. The disclosure license outlives the contract.
- Section 4.1 further allows Flock to access, use, preserve, or disclose Footage to law enforcement, government officials, or third parties on Flock's own good-faith belief that it is reasonably necessary for legal process, enforcing the agreement, security issues, or protecting the rights, property, or safety of Flock, its users, a third party, or the public. The clause gives Flock specified discretion based on its good-faith determination.
- Section 9.1 inverts custody: SJSO agrees to preserve and securely store data "on Flock's behalf" where Flock has legal preservation obligations, so Flock "may retrieve the data from Agency upon demand."
- Section 10.2: Flock may assign the entire agreement without SJSO's consent. SJSO cannot assign without Flock's consent. - Non-Agency End Users: the recitals and Section 6.5 wire private cameras (HOAs, schools, businesses, individuals) into SJSO's feed; Non-Agency users and Flock "may, in their sole discretion, leave access open," and the hotlist No-Fee Term survives termination.

5. Purpose limitation (a hook, not just a flaw)

Section 2.4(a) confines use to "gathering evidence that could be used in a lawful criminal investigation... and not for tracking activities that the system is not designed to capture" (the Permitted Purpose). Uses outside a lawful criminal investigation are not just policy problems; they are contract breaches. Pair this with the audit logs when they arrive.

6. Security posture 'n the contract

- No CJIS Security Addendum appears anywhere in the 113 pages. The word CJIS never appears. Either it exists and was not produced (follow up), or it was never executed (a finding).
- No data breach notification clause of any kind.
- Section 7.6 lists “acts of hackers” among force majeure events. Whether the clause only excuses delayed or failed performance caused by hacking, or reaches liability for a breach, depends on the full clause and should be read on the page-numbered scan before it is characterized further.
- Section 8.1: Flock disclaims liability for loss, inaccuracy, or corruption of data, and caps all liability at 12 months of fees.
- Section 7.5: insurance is an unspecified commercial general liability policy “reasonably commensurate” with Flock’s business risk. No stated limits, no cyber liability requirement, no additional insured.
- Section 8.4: indemnity runs one way. SJSO indemnifies Flock, including for “Agency’s sharing of any data in connection with the Flock system” and any claim that use of the services violates law or third-party rights. The agreement places specified indemnity obligations on SJSO.
- Section 2.1: Flock may use third parties to host and deliver the service; third-party warranties are the agency’s sole remedy for third-party failures.

7. Capab'l'ties acknowledged 'n the contract package

- Master agreement recitals: the Flock Services “are capable of capturing audio, image, and recordings data of suspected vehicles.”
- Section 4.1: Agency Data includes geolocation information and “environmental data collected by sensors built into the Units.”
- Company overview pages included in the package describe a platform of LPR, live video, and audio detection collecting “visual, audio, and situational evidence across an entire city.”
- Vehicle Fingerprint search filters listed: make, body type, color, plates (partial, missing, temporary), state recognition, decals, bumper stickers, back racks, top racks.
- Nationwide Network access: the Dec 2024 order form cites 10 billion additional plate reads per month; the 2024 overview cites 1B+ per month.
- External alert databases available on the platform include FL Expired Licenses, FL Expired Tags, FL Sanctioned Drivers, FL Sex Offenders, California SVS, FDLE, Georgia DOR, IL SOS, Illinois LEADS, NCIC, NCMEC, REJIS, CCIC, and FBI. Expired tags and licenses are administrative violations, well beyond the public stolen-and-wanted framing. Whether SJSO enabled these lists is answerable from the hot list configuration and audit logs.
- Unlimited Custom Hot Lists; Vehicle Location Analysis (sequential alerts with direction of travel); an Insights and Audits module listing user and network audits, plate read reports, hot list alert reports, and event logs. The audit capability exists natively, supporting the proposition that responsive audit records should exist; production and redaction burden is a separate question.
- Advanced Search package purchased in the original 2022 order.

8. Perm'ts and the FDOT order

Section 2.7.2 makes SJSO solely responsible for all permits and permitting costs, and provides that where a location requires permits, Flock installs at a “temporary alternate location” pending permitting, relocating later at no cost. Open questions with teeth after the governor’s removal order: which units sit in state rights-of-way, were FDOT permits ever obtained, and are any current units still at “temporary alternate locations” that were never permitted? MASH-tested DOT-crashworthy poles appear on the Dec 2024 order (4) and Dec 2025 order (15), consistent with roadway placements. The FDOT records request is the map.

9. Fleet and timeline reconstruction

- June 1, 2022: master Government Agency Agreement + order for 15 Falcon cameras and Advanced Search, \$43,750 year 1 (\$40,000 recurring), signed by Flock GC Mark Smith; 60-day pilot window
- 2022-2023 (undated in OCR): Falcon Flex x5 plus extended retention x20, \$21,000/yr
- June 6, 2024: additional hardware/software, 2-year agreement, \$22,700
- December 3, 2024: FlockOS Essentials, 16 Falcon + 2 Solar Falcon LR, 24 months, 30-day retention, \$128,700
- March 21, 2025: extended retention for 18 cameras (360 days), \$9,509.22; separate order for 4 additional LPRs
- December 17, 2025: 23 cameras, all with 1-year retention, 60-month term, \$427,050

Fleet reconciliation (resolved by the second production): the October 1, 2023 order form, produced with the policy batch, covers 137 units. With the 18 units of December 2024, four of March 2025, and 23 of December 2025, the documented total is 182, consistent with the roughly 180 SJSO cites publicly. The December 2025 DocuSign envelope references a "FLOCK-updated Law Enforcement Agreement" that was not produced; which terms govern that order remains an open question for the County Attorney.

10. Immediate follow-ups

1. Reply on R042893-082726: request any CJIS Security Addendum, the updated Law Enforcement Agreement referenced in the December 2025 envelope, any order forms not included, and confirmation of the currently configured retention period per camera group.
2. FDOT District 2 request: all permits for SJSO/Flock installations in state rights-of-way, now against the 30-day removal clock.
3. Obtain the "FLOCK-updated Law Enforcement Agreement" referenced in the December 2025 envelope and determine which terms govern that order.
4. When audit logs arrive, cross-reference against Section 2.4(a): any search outside a lawful criminal investigation is a contract breach on top of everything else.
5. Board question: was the Board informed that the December 17, 2025 five-year commitment of \$427,050 carried 365-day retention, given that the last retention figure stated to the public was 30 days?

Tab 5: Policy 41.35, News Release, and Order Form Findings

Why this matters to the Board: The Sheriff's own policy sets one-year retention, authorizes hot lists well beyond stolen and wanted vehicles, permits group credentials, and requires audits and annual evaluations that were requested and not produced. A policy that promises responsible use is not a reason to normalize a system this powerful.

Second Production Batch: Findings Memo

Covers SJSO Policy 41.35 (eff. 5/8/2017, amended 6/7/2024, signed Sheriff Robert A. Hardwick), the SJSO 2026 LPR news release, the Flock Customer Implementation Guide, and a previously unseen order form attached to the policy production. Compiled September 1, 2026. Companion: contract_findings.md.

1. The buried lead: the October 2023 master order (DocuSign envelope 20683CC1)

A full order form not included in the contract production surfaced in this batch:

- Effective date fixed by special terms at 10/01/2023; Initial Term 60 months (runs to Sept 30, 2028), Renewal 24 months
- Flock Safety Falcon: quantity 132. Falcon Flex: 5. Advanced Search: \$5,000
- Extended data retention (Up to 1 Year): quantity 137, at \$300/unit, \$41,100/yr
- Retention Period stated on the form: 365 Days
- \$391,100 per year; Contract Total \$1,955,500 over five years, after \$342,500 in discounts
- Signed by Matthew Cline (as General Counsel) Sept 1, 2023, Shari Shuman (CFO) Sept 15, 2023, Flock GC Mark Smith Sept 7, 2023

This resolves the fleet reconciliation flagged in contract_findings.md section 9: 137 cameras here, plus 18 (Dec 2024), 4 (Mar 2025), and 23 (Dec 2025) equals 182, matching the roughly 180 SJSO cites publicly. It also means extended 1-year retention was purchased for effectively the entire fleet, not a subset. The \$1.955M five-year commitment predates and dwarfs the \$427K December 2025 order.

Special terms in the 2023 order: three termination provisions and an exclusivity clause

1. Non-Appropriation: payment obligations are payable only from appropriated funds; absence of appropriation renders the Agreement "null and void" with no penalty and no removal fees. The Board of County Commissioners appropriates the Sheriff's budget at the category level under s. 30.49, F.S. Whether and how the Board's budget authority can reach this particular expenditure, and thereby trigger this clause, is a question for the County Attorney.
2. Sheriff Term / Binding Upon Future Parties: the Agreement extends the current Sheriff's term; a newly elected Sheriff who does not agree to extend may cancel on 30 days' written notice without penalty.
3. Change in Florida law: if laws prohibit LPR use in Florida at any time, the Agreement "shall immediately be terminated with no penalty." The governor's FDOT memo is not such a law, but spring legislation could be. If the change-in-law provision applies as written, a law prohibiting LPR use would terminate the agreement without penalty.
4. Exclusivity: Customer "agrees to not contract with any other LPR company during the term" should funds become available later. A sole-source lock-out written into a public contract, and confirmation that all ~180 cameras are Flock.

5. Support: hardware/software not restored to fully operational within 10 days of notice puts Flock in breach and renders the Agreement null and void. Another no-cost exit if performance ever slips.

2. Policy 41-35 vs. the public story

Retention: the policy says one year, not 30 days

Section .30: the retention period “for all scanned data” is up to one anniversary year, citing F.S. 316.0778, with the system “set up to purge data automatically at the conclusion of the one (1) year period.” This matches the purchased 365-day retention and is the fleet-wide condition. The public was last told, in February 2023, that data purged in 30 days; the 2026 news release omits the retention period. One-year retention is within the state’s General Records Schedule (GS2), which permits up to three anniversary years; the issue is governance, not compliance.

Authorized hot lists go far beyond “stolen and wanted”

Section .6 authorizes hot lists for vehicles: with outstanding warrants, in missing person cases, AMBER alerts, stolen, believed involved in crime, and also registered to or operated by persons without a valid license or on the revoked/suspended list, with expired registrations, registered to persons subject to restraining orders or any order restricting movements, persons of interest in a specific investigation, and persons on any state or federal homeland security watch list. Section .11 sources include NCIC Supervised Release (federal probationers), Nationwide DV Protection Orders, the Violent Gang and Terrorist Organization File, Sexual Offender, and DHSMV suspended/revoked registrations, plus agency-generated manual lists authorized by the Intelligence Sergeant. The 2026 news release describes the tool as locating wanted and missing individuals, recovering stolen vehicles, and investigating violent crimes. The policy authorizes alerting on expired tags, suspended licenses, un-charged persons of interest, and watch lists. The gap between the public framing and the signed policy is a document-vs-document contradiction, no interpretation required.

The “no PII” claim

Section .27 asserts LPR data “contains no personally identifying information that may be used to connect license plate detection to an individual.” Stated precisely: the base ALPR record does not contain the registered owner’s name, and a 2026 Florida legislative analysis describes obtaining the associated personal information as a separate authorized inquiry into another restricted database. Section .5 of the policy itself acknowledges that a DMV lookup converts a plate to an owner. The statement in §.27 is accurate as to the record and incomplete as to the system: the name is one authorized query away, and the vendor now sells a product (Nova) that performs that enrichment within its own platform.

The “FDLE approved server” claim

Section .26 states the LPR database and software reside “in a Florida Department of Law Enforcement (FDLE) approved server within a secure data center.” The contract places the data on vendor infrastructure hosted by a third-party provider and accessed by the Sheriff’s Office through a web interface, and the production contains no CJIS Security Addendum and no FDLE approval documentation. Either the approval paperwork exists and must be produced, or section .26 is an unsupported assertion in a signed policy.

Group credentials complicate individual attribution

Sections .13 and .15 require individual credentials but allow group credentials “on a case-by-case basis” as authorized by the Intelligence Unit, with an explicit exception to the no-sharing rule for group-credential users. Queries under a group credential cannot be attributed to an individual from the credential alone; whether other session or device metadata permits attribution is not established by the documents produced. Every misuse case in the abuse file was built on per-user logs; a group login is a hole in exactly that fabric. Follow-up: how many group credentials exist, who holds them, and what queries ran under them.

Oversight that must have left a paper trail

Section .16 requires random audits by the LPR Administrator. Section .17 requires an offense, CAD, or case number before any historical search, and says logs are available for auditing with random audits conducted to ensure compliance. Section .18 requires an annual evaluation of the LPR program. The current policy requires an annual evaluation; I requested all such evaluations and audit reports from 2017 forward; none were produced in the completed response to R042893-082726.

Redactions

Two full sections are blacked out (the block following .9 in Training, and a block following .23). Under s. 119.07(1)(e)-(f), the agency must cite the specific statutory exemption for each redaction in writing. Follow up for the exemption citations; if the cited exemption doesn't fit, challenge it.

Points in SJSO's favor, noted for accuracy

The policy prohibits harassment, intimidation, and personal use (.20), lists criminal prosecution among sanctions (.21), requires visual verification plus confirmation before a stop (.23), bars using LPR to record plates not exposed to public view absent a court order (.20), and requires a reason entry before historical searches (.17). The policy contains several express safeguards. The issue is not that the policy is empty. The public description and the policy differ in material respects, the policy's factual claims and the contract differ in material respects, and the requested audit and annual-evaluation records were not produced in the completed records response.

3. News release vs. the record

- "LPRs only capture a vehicle and its license plate and do not capture a driver's identity or continuously track where someone travels." The contracted platform includes License Plate Lookup described as location history, Vehicle Location Analysis showing sequential alerts and direction of travel, Vehicle Fingerprint capture of decals and bumper stickers, and one-year storage of every scan. A year of time-stamped, mapped detections of a plate is a travel record; "not continuously" is doing all the work in that sentence.
- "180 cameras countywide" since 2017: consistent with the 182 units documented across the four orders, all Flock.
- Claimed outcomes since 2017: 600+ stolen vehicles, 300 stolen tags, 164 property items, 247 wanted, 180 missing, 831 charged. Those outcomes establish tactical value. They do not resolve whether this surveillance infrastructure should exist.
- "Strict oversight and auditing procedures" and no identified misuse: see section .16-.18 production demand above. Also note the Mooresville lesson: their first real audit surfaced 10 additional potential misuse cases.

4. Implementation guide notables

- Flock's own guide asks whether cameras will sit in state right of way and whether DOT permits are required, warns that permitting can add 2+ months, and proceeds with partial installation at locations that don't need permits. Combined with the master agreement's temporary-alternate-location provision, the permit question for the ~180 installed units is live and specific. The FDOT records request answers it.
- The base service includes data storage for 30 days; SJSO paid \$41,100/yr to extend the whole fleet to a year. The 30-day default was the vendor's design; one-year retention was the Sheriff's Office's choice, purchased annually since 2023.
- National Lookup is described in SJSO's own onboarding materials as the network of agencies that opted to allow their cameras to be used for searches, confirming the opt-in sharing question is a configuration record SJSO holds.

5. Contractual exit mechanisms

- Termination for convenience (2022 Terms 6.2): \$500 per unit across ~182 units is roughly \$91,000, offset by prorated refunds of prepaid fees.
- Non-appropriation (2023 special terms): absence of appropriated funds renders the agreement null and void, with no penalty and no removal fees. Whether and how the Board's budget authority under s. 30.49 can reach this expenditure is a question for the County Attorney.
- New sheriff option: 30-day notice, no penalty, next takes office January 2029.
- Change-in-law: automatic, no penalty, if the legislature acts in spring. Four exit mechanisms exist in the executed documents. Which of them the Board itself can invoke, and at what cost, is for the County Attorney to determine; "locked in" is not established by the documents.

6. Consolidated follow-up demands

1. All random and specific audit reports (.16-.17) and annual program evaluations (.18), 2017 to present
2. Exemption citations for both policy redactions, per s. 119.07(1)(e)-(f)
3. Documentation of the "FDLE approved server" in .26, any CJIS Security Addendum, and any FDLE audit findings
4. Inventory of group credentials issued under .13/.15 and queries executed under them
5. Current hot list configuration: which .6/.11 categories and which external databases (FL Expired Tags, FL Sanctioned Drivers, DHSMV suspended/revoked, watch lists) are enabled
6. The Board's appropriation record for the \$1,955,500 (2023) and \$427,050 (2025) commitments

Tab 6: Wyden and Krishnamoorthi Letter to the FTC

Why this matters to the Board: A United States senator asked the Federal Trade Commission to investigate this vendor's security. The letter establishes that stolen customer credentials were documented in criminal markets, that the vendor did not require multi-factor authentication until 2026, and that federal agents used a local detective's login undetected. Every safeguard since added is vendor-controlled, which is a reason not to host the system, not a reason to trust the safeguards.

The official PDF from the Senator's website is the exhibit. The transcription below is for reference and reproduces the letter's own punctuation.

Wyden-Krishnamoorthi Letter to the FTC on Flock Safety

Verbatim transcription for reference. Official PDF (use this as the exhibit):

https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_ftc_on_flockpdf.pdf Press release: [wyden.senate.gov](https://www.wyden.senate.gov), "Wyden, Krishnamoorthi Urge FTC to Investigate Surveillance Tech Company on Negligently Handling Americans' Personal Data" (Nov. 3, 2025)

November 3, 2025

The Honorable Andrew N. Ferguson Federal Trade Commission 600 Pennsylvania Avenue, NW Washington, D.C. 20580

Dear Chair Ferguson:

We write to request that the Federal Trade Commission (FTC) investigate Flock Safety ("Flock"), the license plate surveillance camera company, and, where appropriate, hold the company responsible for its negligent cybersecurity practices. Flock's surveillance data can reveal Americans' movements over time, including trips to doctors and therapists, support group meetings for alcohol or drug addiction, as well as places of worship and protests. By not requiring industry-standard multi-factor authentication (MFA) to secure law enforcement accounts, Flock has needlessly exposed Americans' sensitive personal data captured by the company's surveillance cameras to theft by hackers and foreign spies, and unauthorized access through multiple documented instances of unauthorized password sharing.

Flock operates the largest network of surveillance cameras in the United States, reportedly contracting with over 5,000 police departments, 1,000 businesses, and numerous homeowners associations across 49 states. When a vehicle passes by a Flock camera, Flock records plate information, vehicle characteristics, and when and where the vehicle was spotted. Flock's network of surveillance cameras generate and store billions of vehicle scans each month. Flock reportedly enables law enforcement to search through this data not just by plate number, but also by make, model, and even bumper stickers.

In addition to being able to search data generated by cameras their agencies pay for, Flock's law enforcement customers can also search data collected by other Flock customers' cameras. Flock customers can allow access by specific law enforcement agencies and can also enroll into the "National Lookup Tool" which allows their data to be searched by all other enrolled Flock customers. Flock informed Congress this August that approximately 75% of Flock's law enforcement customers have opted into the National Lookup Tool, which is likely due to Flock restricting access to nationwide searches to agencies that have agreed to share their data. But because most law enforcement agency customers have access to this tool, hackers, foreign spies, or anyone else that gains access to a Flock customer account can misuse it to track Americans across the country.

Flock has unnecessarily exposed Americans' sensitive personal data to theft by hackers and foreign spies. While Flock offers support for MFA, a widely recognized cybersecurity best practice, Flock does not require it, which the company confirmed to Congress in October. Moreover, Flock continues to support insecure methods of MFA, such as sending a numeric code to a phone by text message, which is vulnerable to interception and phishing. Flock does not natively support phishing-resistant MFA, which the Cybersecurity and Infrastructure Security Agency calls "the gold standard method of [MFA]." Phishing-resistant MFA is required of federal agencies and mandated by both the Federal Communications Commission and the FTC

Flock's failure to natively support and require phishing-resistant MFA means that if hackers or foreign spies steal, phish, or otherwise learn a law enforcement officer's Flock password, they can gain access to law-enforcement-only areas of Flock's website and search the billions of photos of Americans' license plates collected by taxpayer-funded cameras across the country. This threat is not theoretical. A search by Congressional staff of a public tool operated by the cybersecurity company Hudson Rock documenting accounts compromised by a form of malware known as an "infostealer" reveals that passwords for at least 35 Flock customer accounts have been stolen. Security researcher Benn Jordan also recently provided our offices with a screenshot from a Russian-language cybercrime forum in which Flock accounts appear to be offered for sale.

By not requiring MFA, Flock has also enabled unauthorized access through law enforcement officers sharing their Flock passwords. If Flock required MFA, law enforcement users of Flock would be required to approve each login to their account from a new computer. On August 11, 2025, Unraveled Press revealed that a Drug Enforcement Administration officer used the Flock account of a local police detective in Palos Heights, Illinois, to conduct several searches. Public records obtained by the press revealed that the detective confirmed that it was a common practice for members of a DEA task force that he was part of to use his login credentials to conduct Flock searches. That numerous federal agents were able to access Flock's systems using passwords belonging to other users without being detected or blocked raises serious questions about the effectiveness of Flock's cybersecurity defenses. A July 9, 2025, memo by the Palos Heights Deputy Chief of Police about the incident, which was released to the press, revealed that the department had not enabled the MFA option until after the password sharing was first identified by a reporter at 404 Media.

Flock's failure to require MFA is likely an unfair business practice prohibited by Section 5 of the FTC Act. In at least four cases — against Uber, Chegg, Drizly, and Blackbaud — the FTC held that failure to require MFA is an unfair business practice. Flock's negligent cybersecurity practices may also violate state laws related to data protection, consumer privacy or the use of automatic license plate reader (ALPR) systems; for example, California Civil Code § 1798.90.53 requires entities operating ALPR systems to "maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure."

Flock has received vast sums of taxpayer money to build a national surveillance network. But Flock's cavalier attitude towards cybersecurity needlessly exposes Americans to the threat of hackers and foreign spies tapping this data. Accordingly, we urge the FTC to hold Flock accountable for its negligent cybersecurity practices.

Sincerely,

Ron Wyden United States Senator

Raja Krishnamoorthi Member of Congress

Tab 7: Precedent Map

Why this matters to the Board: The courts have drawn a line between observing a vehicle on a public road and reconstructing a person's movements from a stored database. The Board does not need to decide the constitutional question to act; it needs to know that the question is live, that a federal appeals court struck down a program with 45-day retention, and that the durable federal remedy for bulk collection was to stop warehousing the database.

The controlling progression of four cases

United States v. Knotts, 460 U.S. 276 (1983). A person traveling on public roads has a diminished expectation of privacy in movements from one place to another. This is the foundation on which plate readers are lawful: each individual capture is an observation of a public thing.

United States v. Jones, 565 U.S. 400 (2012). Attaching a GPS tracker to a vehicle and monitoring it for 28 days was a search. Five justices, in concurring opinions, identified the real concern as the aggregation of movement data over time, which reveals more than any single observation.

Carpenter v. United States, 138 S. Ct. 2206 (2018). Obtaining historical cell-site location records is a Fourth Amendment search. Such records provide a “detailed chronicle” of a person’s movements, enable retrospective surveillance that ordinary observation could not, and the fact that a third party collected them does not eliminate the privacy interest.

Chatrue v. United States, 609 U.S. __ (2026), No. 25-112, decided June 29, 2026. By a 6 to 3 judgment, with Justice Kagan writing for five justices and Justice Gorsuch concurring in the judgment, the Court held that police conducted a Fourth Amendment search when they obtained an individual’s Google Location History, because people have a reasonable expectation of privacy in their cell phone location information. The limited two-hour window and the fact that a private technology company held the data did not eliminate that interest. The Court did not hold geofence warrants unconstitutional; it remanded on particularity and probable cause. Florida courts are bound by the decision.

What Chatrue does and does not establish for this packet. It does not decide license plate readers. It does establish, as Supreme Court precedent, that police acquisition of an individual’s stored Google Location History was a Fourth Amendment search, despite the limited time window and third-party storage. The relevant structural analogy is that the location data was collected before law enforcement selected the subject for retrospective analysis, which is the structure this packet describes.

The plate reader case that cuts the other way

Schmidt v. City of Norfolk (E.D. Va.). A Fourth Amendment challenge to Norfolk’s 172-camera Flock network survived a motion to dismiss in February 2025 on Carpenter grounds. In January 2026 the city won summary judgment. The court emphasized that the fixed cameras captured discrete observations rather than continuous tracking, that Virginia law limited retention to 21 days, that outside sharing was restricted, and that statutory guardrails applied. The court acknowledged that increasing the number or capabilities of cameras could change the analysis. The case is on appeal to the Fourth Circuit. Florida is in the Eleventh Circuit and is not bound.

The comparison. Norfolk’s challenged Flock network prevailed at summary judgment with 21-day retention and Virginia statutory guardrails. The Sheriff’s Office retains data for 365 days. Florida has ALPR statutes, but they do not impose the same combination of 21-day retention, use restrictions, outside-sharing restrictions, and audit requirements that the Norfolk court identified in Virginia law, and the Sheriff’s Office has stated in a grant application that the retention’s purpose is pattern-of-life analysis.

The closest analog, and 't struck the program down

Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021) (en banc). Baltimore's aerial surveillance program photographed most of the city for twelve hours a day and retained imagery for 45 days. The court held the program unconstitutional under Carpenter because it enabled retrospective tracking of everyone's movements. A federal appeals court ended a municipal mass-location program with 45-day retention. The Sheriff's Office retains data eight times longer.

The federal precedent for the remedy

The government's bulk telephone metadata program was held unauthorized by statute in **ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015)**, and the government's own Privacy and Civil Liberties Oversight Board reported in January 2014 that it could not identify a single instance in which the program made a concrete difference in a counterterrorism investigation. Congress responded with the **USA FREEDOM Act (2015)**: the government stopped warehousing the database, records stayed with the carriers, and queries ran case by case on specific selectors with court approval. The real-time capability survived. The stored archive did not.

What th's means for the Board

The precedents above establish two things. Useful law-enforcement functions do not require government to maintain the underlying bulk movement archive; that was the federal remedy in 2015. And aggregation and retrospective access materially change the character of otherwise lawful individual observations; that is Jones, Carpenter, Chatrle, and Baltimore. For this packet, the point is not to identify the minimum regulation necessary to preserve the current system. It is that government can preserve legitimate investigative tools without maintaining this particular surveillance infrastructure. The Board should direct counsel to identify the lawful mechanisms available to remove the system from county-supported property and funding without waiting for a court to decide the constitutional question.

Citizen research memorandum. Citations should be verified against primary sources before use in any court filing.

Tab 8: Florida Toll Road Surveillance

Why this matters to the Board: Florida already treats a record of where a vehicle has been as sensitive enough to make it confidential, and SunPass's own terms require legal process for outsiders. Florida regulates ALPR confidentiality, disclosure, and maximum retention, but its current statutes do not impose the same combination of use restrictions, short retention, outside-sharing limits, and audit requirements found in some other states. The toll system also documents how a system's functions expand after deployment, which is one reason this packet recommends removal rather than reliance on future rules.

Flor'da Toll Road Surve'llance: Statutes, Cases, and Investigation F'nd'ngs

Research memo for the St. Johns County BOCC comm'ss'oner packet

Prepared September 2026

I. The statutory protection Flor'da already extends to toll data

Primary statute

Section 338.155(6), Florida Statutes SunPass account information, including transponder data and trip records, is exempt from disclosure under Florida's public records law. That is what the statute itself provides. The subpoena-or-court-order restriction is a separate proposition: it comes from SunPass's official Customer Agreement and FDOT's Turnpike FAQ, and the SunPass User Manual (revised November 2025) states that "information concerning a SunPass account is provided only by subpoena or court order."

This means a Florida citizen's toll-road travel history can be obtained by persons outside FDOT and authorized law enforcement only through legal process. A subpoena or a court order stands between the database and outsiders.

Source: s. 338.155(6), F.S.; sunpass.com Customer Agreement (section 3.1); floridasturnpike.com FAQ; SunPass User Manual v7 (Nov. 2025)

II. What the toll system actually does w'th ALPR data, and why the consent argument breaks down

The USA TODAY Network–Florida investigation (September 2022)

The USA TODAY Network–Florida spent six months reviewing more than 2,000 pages of contracts between FDOT and two vendors, Conduent and Transcore, that operate the state's SunPass toll system across 628 miles of highways, expressways, and turnpikes.

Key findings:

1. **The Law Enforcement Notification System.** Toll-road ALPR cameras and SunPass transponder readers feed a database referred to in FDOT contract documents interchangeably as an "enforcement list," a "black list," and a "Law Enforcement Notification System." Police agencies can request that specific plate numbers or transponder signatures be added. When a flagged vehicle is detected, the system sends authorized users the vehicle's location, a timestamp, and photographs, in real time.

William Rapp, executive vice president of Q-Free America (whose software powers the plate readers at Florida's toll plazas), described the system's purpose: "The main premise here is get the damn thing out to law enforcement urgently."

2. **No legal limit on additions.** Florida has no statute limiting when or why a police agency can add a vehicle to the enforcement list. The reporting identified no statutory warrant requirement, purpose restriction, or sunset provision governing additions to the enforcement list.
3. **Total state secrecy.** FDOT denied every public records request the USA TODAY Network filed for even a redacted copy of the enforcement list. The department cited public records exemptions that a government transparency advocate told the outlet did not apply. FDOT also refused to answer basic questions: how frequently cars were tracked, who had access, and what policies governed use. FDOT ignored requests to mediate the dispute under the state Attorney General's program.
4. **The Central Florida Expressway Authority** operates a parallel tracking system on its roads.

Sources: USA TODAY Network–Florida investigation, "Florida has a secret 'black list' to spy on highway drivers" (Sept. 2022); "Florida's secretive toll surveillance program: Five things to know" (Sept. 2022). Reporting by the USA TODAY Network–Florida; also covered by Jalopnik (Sept. 7, 2022) and Yahoo News.

III. The fa'led leg'slative fix

In 2015, State Sen. Ray Rodrigues (R-Estero) filed a bill that would have required warrants for police to use toll plate reader data, with exceptions for emergencies and toll enforcement, and restricted retention periods. Law enforcement agencies testified against it. It died in committee.

Sen. Rodrigues later said: "The question I never was able to answer in that session was how do you permit the uses for automated license plate readers which everyone agrees are useful, such as toll reading and identifying stolen cars, but prevent plate readers from being abused or utilized to increase surveillance."

This is precisely the question SJSO's grant application answered in the opposite direction: store a year of data to "develop a pattern of life to potentially identify home and work locations."

Source: USA TODAY Network–Florida, quoting Sen. Rodrigues (Sept. 2022)

IV. The case law: toll records 'n Flor'da courts

Florida Department of Transportation v. Tropical Trailer Leasing (Fla. Dist. Ct. App., 2017)

In a civil discovery dispute, FDOT sought to quash a subpoena for Toll-By-Plate records (not SunPass transponder accounts, the amended subpoena had excluded those). FDOT argued s. 316.0777 protected the records; the trial court denied the motion but entered a confidentiality order. The appellate court affirmed, finding the records were subject to civil discovery with appropriate protections.

What this establishes for the packet: - Even FDOT, defending its own system, argued that toll location records are confidential and require legal protection before disclosure. - The court treated toll-derived location data as sensitive enough to warrant judicial management even in civil litigation. - SunPass transponder accounts remained categorically protected throughout, the amended subpoena excluded them precisely because s. 338.155(6) shields them more firmly.

Source: FDOT v. Tropical Trailer Leasing, FindLaw (2017); citation: Fla. Dist. Ct. App. (search "FDOT v Tropical Trailer Leasing 2017 Florida").

V. The core argument for the packet

Florida has already drawn the line in a related context. The Legislature determined that trip data collected for billing purposes, in a disclosed, purpose-limited system, deserves statutory protection requiring court process before disclosure.

The toll system comparison exposes four structural failures in the Flock program:

Factor	SunPass/Toll-By-Plate	SJSO Flock Network
Disclosure	Signed gantries; driver knows when scanned	No notice; cameras unmarked in most locations
Purpose	Primary purpose: toll collection. Additional documented function: law-enforcement notification	“Pattern of life” per SJSO grant application
Access	Outsiders: subpoena or court order required	SJSO has committed in writing to sharing grant-related LPR data with ICE and CBP; broader National Lookup enrollment remains unverified
Consent	Optional; driver can take non-toll roads	No opt-out for a driver passing a camera location
Statutory framework	s. 338.155(6), F.S.: confidential; outsiders need subpoena or court order	ss. 316.0777 and 316.0778 regulate confidentiality, disclosure, and maximum retention, but do not impose the same combination of use restrictions, short retention, outside-sharing limits, and audit requirements found in some other states

The toll comparison also documents capability accretion. A purpose-limited, statutorily protected, opt-in system acquired an additional law-enforcement function once the camera infrastructure existed: FDOT built a real-time law enforcement notification system on top of a billing system, with no statute limiting additions to the list, as documented by the USA TODAY Network in 2022. The lesson for the Board is that once collection infrastructure exists, its functions can expand beyond those contemplated at deployment. That capability accretion is one reason this packet recommends removing the infrastructure rather than relying on future rules to contain it.

The podium version: “Florida treats SunPass account information as confidential, and SunPass says people outside FDOT and authorized law enforcement generally need legal process to obtain it. The Sheriff’s Office retains its LPR records for a year and has committed in writing to sharing the grant-related data with ICE and CBP. The systems have different rules governing access, retention, and use.”

VI. The Carpenter connection

The U.S. Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), rejected the argument that cell phone location data is “voluntarily” surrendered to a carrier because carrying a phone is “indispensable to participation in modern life.” The same aggregation concern is relevant here. Neither Carpenter nor Chatrue decides ALPRs. But both demonstrate that retrospective access to stored location information can implicate

the Fourth Amendment even when the data was generated during ordinary daily activity and held by a private company. Driving is not optional in car-dependent St. Johns County.

VII. 2025 legislative session: a statewide fallback, not the requested local outcome

Florida has no statute equivalent to California Civil Code § 1798.90.53, which requires entities operating ALPR systems to maintain “reasonable security procedures and practices” protecting ALPR data from unauthorized access. Senator Wyden’s November 2025 FTC letter to Chair Ferguson cited this California statute as a model.

If Florida continues to permit ALPR systems, statewide safeguards covering retention, access, and security would reduce risk, and the Legislature already built a model in s. 338.155(6) for toll data. That is a statewide fallback. It is not the requested local outcome, which is removal of the system from county-supported property and funding.

Research memo. Verify statutory citations against current Florida Statutes before any court filing. Primary sources: s. 338.155(6), F.S.; SunPass User Manual v7 (Nov. 2025); FDOT v. Tropical Trailer Leasing (2017); USA TODAY Network–Florida investigation (Sept. 2022).

Tab 9: Documented ALPR Misuse Incidents (Reference)

Why this matters to the Board: Reference material. Misuse of these systems by officers is documented nationally and in Florida, and many cases were first identified by someone outside the agency; in the narrower stalking subset compiled by the Institute for Justice, most surfaced externally. The Sheriff's policy requires the audits that would catch it locally; those audits were requested and not produced.

Documented ALPR / Flock Misuse Incidents

Compiled August 28, 2026; revised September 9, 2026.

Headline finding: The Washington Post, August 19, 2026

At least 69 police officials have been accused, charged with, or convicted of misusing Flock's system or other license plate readers for unauthorized purposes, and in at least 15 of those cases someone outside the department, including victims, activists, and journalists, identified the potential misuse first. Using publicly available data, the Post itself identified three officers whose search histories showed signs of misuse; all three departments said they did not regularly audit use. In Indianapolis, an officer searched vehicles tied to his wife and two acquaintances 3,759 times over ten months, about twelve lookups a day; the department acknowledged it had no regular audit practice and has recommended termination. Flock's CEO has said misuse is inevitable and that abusers are a small fraction of roughly 140,000 active users.

The Institute for Justice snapshot (narrower subset)

The case list below is the Institute for Justice's romantic-stalking list as captured on August 3, 2026: 47 incidents of officers using ALPR systems to track romantic partners, exes, spouses, coworkers, or strangers, 2021 to August 2026, each linked by IJ to original local reporting or public records. Six are in Florida. Perpetrators include two police chiefs, an elected sheriff, lieutenants, detectives, and a district attorney's office investigator. Per IJ, nearly all were charged and lost their jobs, but only a few cases were caught by internal safeguards; most surfaced after victims reported stalking. IJ's broader ALPR abuse database, launched August 12, 2026, exceeds 100 incidents. The Post's 69 is a separate count using its own criteria. Cite each figure with its source and date.

Section 1: Personal stalking and tracking cases (newest first)

August 2026 | Shively, KY | Shively Police Department | Officer Asad Zahir Arrested Aug 25, 2026. Ran 2,048 Flock searches from January into May 2026 tracking two vehicles registered to his child's mother in Kentucky and Indiana, while she held an order of protection against him. 241 searches occurred after the protective order. Charged with official misconduct and unlawful access to a computer. Flagged by Flock's new AI audit tool.

August 2026 | Habersham County, GA | Habersham County Sheriff's Office | Deputy Jonathan Thomas Fired and criminally charged after an internal audit found he used Flock to track a person he was in a relationship with. The office announced new Flock restrictions after his arrest. Second Habersham deputy caught in two months.

August 2026 | Brevard County, FL | Brevard County Sheriff's Office | Deputy Michael Fultz A former Deputy of the Year, resigned after an investigation uncovered misconduct described as egregious, including looking up his ex-girlfriend's plate on Flock.

August 2026 | Bibb County (Macon), GA | Bibb County Sheriff's Office | Deputies Joseph Callaway, Tony Lewis, and Coznavian Stubbs Three deputies charged with stalking and related crimes in a single probe after allegedly using Flock to track people they were in relationships with.

August 2026 | Apache Junction, AZ | Apache Junction Police Department | Officer Joshua McDaniels Resigned at the conclusion of an investigation finding he improperly used Flock to look up his wife's location.

August 2026 | Brentwood, MO | Brentwood Police Department | name not released Outside investigation found sustained policy violations for using Flock to track his ex-wife's location during divorce proceedings. He admitted the tracking to her. St. Louis County Police determined no crime occurred under Missouri law, illustrating a state-law gap.

August 2026 | Mooresville, NC | Mooresville Police Department | Officer Elizabeth Snowman Arrested Aug 5, 2026 after a department Flock audit found she accessed the system 31 times to track her boyfriend's ex-wife, logging most searches as motor vehicle infractions, at least twice while off duty. Charged with computer access crimes. The chief said the audit surfaced 10 more potential misuse cases, 3 of them problematic.

August 2026 | New Bedford, MA | New Bedford Police Department | Officer Emily Pacheco Placed on leave under investigation after her ex-girlfriend obtained an abuse prevention order alleging Pacheco stalked her using Flock cameras.

August 2026 | Jefferson Parish, LA | Jefferson Parish Sheriff's Office | Deputy Nathan Rome Fired after a reporter's inquiry prompted a review that found he searched his ex-fiancee's plate thousands of times over several years.

July 2026 | Habersham County, GA | Habersham County Sheriff's Office | Deputy Christian Brewer Fired and arrested after an internal audit found he used Flock to track a person he was in a relationship with.

July 2026 | Sumter County, FL | Sumter County Sheriff's Office | Detective Brandy Almany Fired and criminally charged for allegedly using Flock and other police databases to track her husband's ex-wife. The sheriff suspended the agency's Flock program after the scandal.

June 2026 | Statesboro, GA | Ogeechee Circuit District Attorney's Office (former Effingham County SO) | Investigator Andrae Wright Arrested by the GBI and charged with stalking and other crimes for alleged misuse of the Flock system.

May 2026 | Pasadena, TX | Pasadena Police Department | Sgt. Michael Palitz Resigned while under investigation for using the department's Flock system to track and stalk a female officer.

April 2026 | Alpharetta, GA | Alpharetta Police Department | Patrolman Dustin Bozzo Internal investigation concluded he used Flock dozens of times to track a former romantic partner employed by the department, plus another officer he mistakenly viewed as a romantic rival. Resigned; referred for criminal investigation.

April 2026 | Gwinnett County, GA | Gwinnett County Police Department | Officer Renee Downer Arrested and relieved of duty for allegedly using law enforcement databases, including an LPR system, to monitor an ex-partner's location.

April 2026 | Conyers, GA | Conyers Police Department Real-Time Crime Center | Supervisor Paige Forte Fired and charged by the GBI after allegedly using Flock to monitor her domestic partner's location. Notable because the abuser was a civilian crime-center supervisor, not a sworn officer.

March 2026 | Mauldin, SC | Mauldin Police Department | Officer Ellie Hammond Fired after using Flock cameras to track a former romantic partner 166 times.

February 2026 | Key West, FL | Monroe County Sheriff's Office | Deputy Lamar Roman Used an ALPR system (Guardian) to track and eventually pull over a woman he met while working security on a TV set. Arrested and charged with accessing a computer or electronic device without authorization. A stranger-targeting case, not an ex.

January 2026 | Reynoldsburg, OH | Reynoldsburg Police Department | Officer Mark Nichols Resigned after an investigation found he searched the plates of a former domestic partner.

December 2025 | Greer, SC | Greer Police Department | Cpl. Kareem Lynch Fired after an internal audit found he used Flock to monitor the whereabouts of a subordinate with whom he had a prior relationship. SLED reviewing.

November 2025 | Bonner Springs, KS | Bonner Springs Police Department | Detective Kyle Rector Allegedly used LPRs to track his estranged wife and two men he suspected were her new partners. Charged with multiple crimes in March 2026.

October 2025 | Menasha, WI | Menasha Police Department | Officer Cristian Morales Placed on leave and charged with misconduct in office after his ex-girlfriend complained he used Flock to track her.

October 2025 | Katy, TX | Katy Police Department | Officer Sergio Rodriguez Fired and indicted on felony stalking and misuse of official information. Tracked his ex-wife via Flock more than 2,000 times over 11 months (Nov 2024 to Apr 2025 per indictments) and also placed a physical tracking device on her vehicle. Pleaded not guilty.

October 2025 | Niceville, FL | Niceville Police Department | Officer Coty Hall Used the department's Flock system to track another officer and that officer's spouse. Caught by internal audit, fired after his October 2025 arrest, later pleaded no contest to several charges.

September 2025 | Kenosha County, WI | Kenosha County Sheriff's Office | Deputy Frank McGrath Resigned with severance after internal investigators found he used Flock to keep tabs on another deputy he was romantically involved with. Charged with two felonies in August 2026.

September 2025 | Prairie Grove / Holiday Hills, IL | Prairie Grove PD (also chief of Holiday Hills PD) | Officer William C. Copp Arrested after prosecutors said he used Flock data hundreds of times to track several former romantic partners and at least one new partner. Fired from Prairie Grove.

July 2025 | Jerome County, ID | Jerome County Sheriff's Office | Sheriff George Oppedyk The elected sheriff searched Flock for his wife's vehicle hundreds of times. Idaho's Attorney General found no crime under state law; Oppedyk retired in April 2026, two years before his term ended.

July 2025 | Winnebago County, IL | Winnebago County Sheriff's Office | Deputy Tyler Bryan Charged with stalking and official misconduct for allegedly monitoring an ex-girlfriend and her new partner. Surfaced when the victims sought an order of protection.

June 2025 | Richmond County (Augusta), GA | Richmond County Sheriff's Office | Deputy Jaquarius Yarbrough Arrested after allegedly running the plate of a woman he was having an affair with 1,639 times over several months.

May 2025 | Greer, SC | Greer Police Department | Officer Sebastian Echeverry Fired for personal use of the Flock system; at least one unauthorized search reportedly targeted his ex-girlfriend.

March 2025 | Milwaukee, WI | Milwaukee Police Department | Officer Josue Ayala Allegedly tracked a woman he was dating and her ex-partner nearly 180 times over two months. Victims discovered it themselves via HaveIBeenFlocked.com. Ayala resigned in 2026 after being charged with misconduct in public office. MPD then revoked Flock access for most officers.

March 2025 | Louisville, KY | Louisville Metro Police Department | Officer Roberto Cedeno Charged with multiple felonies for allegedly using the city's ALPR system to track an ex-partner and her friends hundreds of times over two months.

December 2024 | Matteson, IL | Matteson Police Department | Officer Jaila Cole-Clark Internal documents obtained by stopflock.org showed hundreds of Flock searches for a former domestic partner and that person's new partner. Resigned mid-investigation.

September 2024 | Haines City, FL | Haines City Police Department | Officer Christopher Goodson Placed on leave and arrested after an investigation showed he searched Flock for his estranged wife's car more than 700 times between Sept 1, 2024 and June 30, 2026.

August 2024 | Shelby County, TN | Shelby County Sheriff's Office | Deputy Thadius Gordon Relieved of duty after allegedly using an ALPR database to track his ex-wife's location more than 100 times.

July 2024 | Braselton, GA | Braselton Police Department | Police Chief Michael Steffman The chief himself. Arrested after allegedly using LPRs to stalk and harass multiple people, including a former romantic partner. Resigned shortly before arrest.

June 2024 | Stow, MA | Stow Police Department | Officer Jason Rogers Placed on unpaid leave with a criminal complaint filed after allegedly using Flock and other databases to stalk a former partner who had changed her identity to escape his abuse. She discovered the tracking through HaveIBeenFlocked.

June 2024 | Orange City, FL | Orange City Police Department | Officer Jarmarus Brown Ran his ex-girlfriend's plate at least 69 times, her mother's at least 24 times, and her father's at least 15 times over roughly seven months in 2024. Arrested and charged in 2025.

June 2024 | Riverside County, CA | Riverside County Sheriff's Office | Deputy Alexander Vanny After being arrested for kidnapping his ex-fiancee, was found to have used the department's Flock system to track one of her friends. Convicted on multiple charges at a jury trial in December 2025.

April 2024 | Coffee County, GA | Coffee County Sheriff's Office | Deputy Chris Rozar Fired and charged with multiple offenses for allegedly using Flock to stalk a woman he was romantically interested in.

October 2023 | Sedgwick, KS | Sedgwick Police Department | Police Chief Lee Nygaard Resigned after using Flock to track his ex-girlfriend and her new boyfriend more than 200 times over several months.

June 2023 | Costa Mesa, CA | Costa Mesa Police Department | Officer Robert Josett Used Flock to track his mistress and her other romantic interests, alongside thousands of harassing texts and calls. Pleaded guilty to multiple criminal charges in April 2026.

October 2022 | Kechi, KS | Kechi Police Department | Lt. Victor Heiar Used Flock cameras to track his estranged wife. Pleaded guilty to computer crime and stalking (convicted 2023).

January 2022 | Fort Bend County, TX | Fort Bend County Sheriff's Office | name not released (Lieutenant) Used Flock dozens of times starting Jan 2022 to monitor multiple people, including one in a contentious familial relationship with him. Discipline: a two-day suspension. An example of minimal internal consequences.

September 2021 | Westmoreland County, PA | municipal police | Officer Michael McSherry Pleaded guilty to stalking after using plate readers to track his estranged wife and other family members.

Section 2: Non-romantic documented misuse (systemic)

May 2025 | Johnson County, TX | Johnson County Sheriff's Office A deputy ran a nationwide Flock search across roughly 83,000 cameras for a woman who had self-administered an abortion, with that reason entered

in the search log. Reported by 404 Media; became the flashpoint case for out-of-jurisdiction and purpose-creep searches.

2025 | Denver, CO | Denver Police Department Audit logs obtained through an open records request showed Denver's Flock data was searched more than 1,400 times for ICE and other federal immigration purposes, contrary to city policy. Triggered council backlash.

2025 | Dayton, OH | Dayton Police Department Records showed roughly 7,100 immigration-related searches of the city's Flock data by outside agencies, despite local policy against immigration enforcement use.

January 2026 | Joplin, MO | Joplin Police Department | name not released Officer separated from the department after unspecified policy violations involving Flock cameras. Listed separately by IJ because the target was not confirmed as romantic.

Section 3: Patterns worth c'ting 'n a compla'nt

1. Detection failure. Per IJ's review of all 47 cases, only a few were caught by internal safeguards. Most were exposed by victims filing stalking complaints or checking HaveIBeenFlocked.com themselves. The systems logged the abuse for months or years without anyone noticing.
2. Fake justifications undermine the audit trail. Officers routinely entered false reasons (Mooresville: "motor vehicle infraction"), showing the reason field is self-reported and unverified.
3. Rank is no barrier. Two police chiefs, one elected sheriff, lieutenants, detectives, a DA investigator, and a civilian crime-center supervisor all abused access.
4. Legal gaps. In Missouri and Idaho, prosecutors or the AG concluded no crime occurred, meaning the only protection in some states is agency policy.
5. Consequences arrived only after exposure. Nearly all officers were charged or forced out, but typically after victims had been tracked dozens to thousands of times (166, 700, 1,639, 2,048 searches).
6. Florida is not an outsider to this problem: Orange City, Haines City, Niceville, Key West (Monroe County), Sumter County, and Brevard County. Sumter's sheriff suspended the program entirely after his detective's arrest.

Sources

- Institute for Justice, ALPR abuse database and article by Christopher Ingraham (updated Aug 3, 2026): ij.org/police-have-reportedly-used-license-plate-readers-to-stalk-romantic-interests-at-least-14-times-in-recent-years/ (each incident links to its original local news source or public record)
- 404 Media, "Cops Keep Getting Arrested for Using Flock to Stalk People" (June 2026)
- CNN, Shively KY arrest coverage (Aug 26, 2026)
- ABC News, Mooresville NC arrest coverage (Aug 2026)
- KPRC/Click2Houston, Katy TX indictment coverage (Aug 25, 2026)
- IJ Plate Privacy Project: plateprivacy.com

Tab 10: Flock Contract Cancellations by Agency (Reference)

Why this matters to the Board: Reference material and corroboration only. Removal is being chosen across Florida and the country right now, by counties and cities in the same position as this one. The argument in this packet does not depend on what any other county decided.

Agencies That Canceled, Rejected, Defunded, or Covered Flock / ALPR Programs

Compiled August 28, 2026. Primary source: Institute for Justice ALPR Contract Cancellation Database (launched Aug 26, 2026; 128 local governments as of Aug 27, 182 as of Sept 8). Supplemented by DeFlock, Newsweek, CNN, and local outlets. IJ's database deliberately excludes pauses and vendor switches, so the true number of jurisdictions that have acted against Flock is higher.

Summary

- 182 local governments have canceled or refused to renew ALPR contracts since the start of 2025, per IJ's database page as of September 8, 2026 (128 as of August 27, 2026 when this file was compiled; press reports citing IJ's list on September 12 put the figure at 201; re-verify on September 14), per IJ's database
- DeFlock counts at least 56 cities and towns that deactivated, rejected, or canceled Flock in 2026 alone
- The wave accelerated sharply: roughly 6 cancellations in 2025, then a flood beginning early 2026, with 40+ in August 2026 alone
- Outcome types: early termination, nonrenewal after expiration, defunding, and cancellation before deployment (several jurisdictions killed contracts before a single camera went live)
- Sen. Josh Hawley opened a Senate investigation into Flock, demanding answers from CEO Garrett Langley about the 120,000+ camera network spanning 49 states
- Texas note: on August 27, 2026, Governor Abbott blocked state agencies from spending money on the cameras (Texas Tribune, as reported Sept. 12, 2026).
- Florida note (updated Sept. 9, 2026): Governor DeSantis publicly raised concerns about the expansion of automated plate readers, and on Aug. 31, 2026 the Florida Department of Transportation under his administration issued a memorandum revoking general-use permits for ALPRs in State Highway System rights-of-way, requiring removal within 30 days and ending future permits. Revoking roadway permits is not the same as canceling contracts; the broader decisions that followed were made independently by local sheriffs and commissions.

What triggered the wave (documented Flock conduct and revelations)

1. Federal access denials that proved false. Flock insisted for months it had no federal contracts, then admitted under journalist questioning that it had been running a pilot with Customs and Border Protection, and announced in August 2025 it was ending federal law enforcement partnerships. Cities including Austin, Sedona, and Denver had raised concerns about federal access to their data before that admission.
2. Audits exposing unauthorized searches. Denver logs showed 1,400+ ICE-related searches; Dayton logs showed roughly 7,100 immigration searches by outside agencies; Woodburn OR canceled after an audit revealed ICE access; an Illinois state investigation into data sharing directly triggered the Evanston and Oak Park terminations.
3. Trust language from governments themselves. Cambridge, MA terminated citing a breach of trust by the company. The Bernalillo County, NM sheriff said he fired Flock because he lost trust in it. Sheboygan, WI is terminating over Flock actions it says were inconsistent with its contract. Staunton, VA terminated over a dispute with Flock.

4. Misuse arrests converting directly into cancellations. Stow, MA canceled after its officer's stalking case. Nelson, GA canceled following police misuse reports. St. Charles County, MO dropped Flock after an abnormal pattern of searches surfaced. Chandler and Surprise, AZ ended contracts after audits revealed misuse and policy violations.
5. Capabilities beyond what the public was told. Reporting on the Bellingham, MA nonrenewal noted the police chief's acknowledgment that the system's features go beyond what most people would consider a traditional license plate reader, after the program had been described publicly as plates only.
6. Post-cancellation friction. Multiple jurisdictions physically covered cameras to stop collection while contracts wound down (Sheboygan, Pflugerville, Bolivar, Dickinson County, Springfield OR, Hood County, Dayton). Reporting by The Guardian and Business Insider has documented cities that dropped Flock finding cameras still live or residents still surveilled by neighboring jurisdictions' cameras.

Covered, paused, or termination pending (not counted in IJ's cancellation database)

- **Sheboygan, WI | Aug 25, 2026 | City of Sheboygan / Sheboygan PD.** All 15 Flock cameras physically covered with bags to stop data collection. Police Chief Kurt Zempel and City Administrator Casey Bradley are asking the Common Council on Sept 8 to terminate the contract, after the department learned in July of Flock actions believed inconsistent with the contract's terms that undermined trust. Specifics to be disclosed at the September meeting.
- **Denver, CO | 2025-2026 | Denver City Council.** Council unanimously rejected a two-year extension of the 70-intersection Flock program over privacy and access concerns; a task force was created to decide the program's fate.
- **Dayton, OH | 2026 | Dayton PD.** Bagged its cameras amid the fallout from the immigration-search audit.
- **Milwaukee, WI | 2026 | Milwaukee PD.** Revoked Flock database access for most officers after the Ayala stalking case.
- **Sumter County, FL | July 2026 | Sumter County Sheriff.** Suspended the agency's Flock program after Detective Almany's arrest.

Florida state action (Aug 31, 2026)

- **State of Florida | Aug 31, 2026 | Gov. DeSantis / FDOT.** FDOT Engineering and Operations Memorandum 26-01, revoking general-use permits for automated license plate readers in State Highway System rights-of-way (including interstates such as I-10 and I-75), with 30 days to remove; the state will remove noncompliant units itself, and FDOT will not issue future permits. DeSantis cited growing signs of camera misuse, surveillance concerns, and the potential for misuse by both the private company and law enforcement, referencing a Florida officer who used LPR data to track an ex-girlfriend. Days earlier he called license plate reader use "out of control." The revocation does not reach city or county roads; DeSantis called for a legislative solution in the spring session.
- **Franklin County, FL | Aug 31, 2026 | Franklin County Sheriff's Office.** Announced it is ending its license plate reader program following the governor's order.
- **Liberty County, FL | Aug 31, 2026 | Liberty County Sheriff's Office.** Announced it is ending its license plate reader program following the governor's order.
- **Putnam County, FL | Aug 31, 2026 | Putnam County Sheriff's Office.** Announced it is ending its license plate reader program following the governor's order. Putnam borders St. Johns County.

Full cancellation list by state (IJ database, each entry sourced to local reporting)

Arizona (9)

- Cave Creek | Aug 2026 | early termination | Town canceled after weighing resident concerns, policy limitations, and recent events tied to the Flock system
- Chandler | Aug 2026 | nonrenewal | City discontinued after an audit revealed misuse
- Flagstaff | Dec 2025 | early termination | Council voted unanimously to deactivate all 32 cameras after backlash
- Pinal County | Aug 2026 | nonrenewal | Sheriff canceled citing Fourth Amendment concerns
- Sedona | Sept 2025 | early termination | Council permanently ended the program and banned ALPRs
- Sierra Vista | Apr 2026 | early termination | Council ended contract over privacy concerns
- South Tucson | Feb 2026 | early termination | Council canceled over federal access concerns
- Surprise | Aug 2026 | early termination | City canceled after discovering a potential policy violation and requested removal of all equipment
- Tempe | Aug 2026 | early termination | City shut down its Flock system and said it will not seek another ALPR provider

Arkansas (5)

- Centerton | Aug 2026 | early termination | Council voted to terminate after residents raised privacy concerns
- Farmington | Aug 2026 | nonrenewal | Police recommended cancellation after a false hit and cameras aimed at private property
- Greers Ferry | Aug 2026 | early termination | Town removing cameras after concerns; IJ had earlier demanded the town move a camera pointed at a family's home
- Pea Ridge | Jul 2026 | early termination | Police chief canceled after community pushback
- Searcy | Aug 2026 | early termination | Council voted to end contracts amid privacy concerns

California (5)

- El Cerrito | May 2026 | nonrenewal | Council declined renewal after three years
- Los Altos Hills | Jan 2026 | early termination | Council terminated over privacy concerns
- Mountain View | Feb 2026 | early termination | Council voted unanimously to cancel after backlash; reporting noted allegations of unauthorized use
- Santa Cruz | Jan 2026 | early termination | Council voted 6-1 over privacy and data sharing concerns; first California city to terminate
- Siskiyou County | Jul 2026 | canceled before deployment | Sheriff pulled the plug before implementation over privacy concerns, 13 months after unanimous board approval

Colorado (4)

- Fort Collins | Jun 2026 | early termination | Council canceled one year early and began a surveillance policy review
- Littleton | Aug 2026 | early termination | Town ordered removals starting May, more in August; reporting noted units later found back online
- Moffat County | Aug 2026 | nonrenewal | Sheriff letting contract expire, citing privacy, data sharing, and funding
- Salida | Aug 2026 | early termination | City canceled citing lack of results and community concerns

Connecticut (2)

- Killingworth | Jul 2026 | early termination | Town canceled, arguing the cameras were not worth the cost
- Windsor | Jul 2026 | nonrenewal | Town voted against renewal after an earlier pause

Georgia (1)

- Nelson | Jul 2026 | early termination | City canceled following reports of police misuse of ALPRs

Idaho (2)

- Clearwater County | Jul 2026 | nonrenewal | Sheriff letting contract expire, citing limited utility and funding
- Lincoln County | Aug 2026 | early termination | Sheriff terminated after intense community debate

Illinois (4)

- Evanston | Sept 2025 | early termination | Terminated after the state investigation into data sharing; reporting later noted deactivated units found back online
- Henry County | Aug 2026 | early termination | Ended over community trust concerns
- Oak Park | Aug 2025 | early termination | Terminated after the state investigation into data sharing
- Salem | Apr 2026 | canceled before deployment | Canceled after contract-term changes concerned the mayor

Indiana (2)

- Bloomington | Mar 2026 | nonrenewal | City declined renewal after a months-long evaluation
- Monroe County | Jul 2026 | early termination | Commissioners canceled over data security concerns

Iowa (1)

- Coralville | Feb 2026 | early termination | City canceled following a review by the state attorney general

Kansas (2)

- Gardner | Aug 2026 | early termination | Council voted unanimously over privacy concerns
- Wellsville | Aug 2026 | early termination | Police department canceled so the community would feel heard and respected

Kentucky (5)

- Cynthiaana | Aug 2026 | nonrenewal | Mayor letting contract expire, citing changes in technology, company policies, and enlightening information
- Fort Mitchell | Aug 2026 | early termination | Council canceled over Fourth Amendment concerns
- Hartford | Aug 2026 | canceled before deployment | PD canceled before deployment after residents called it overreach
- Independence | Aug 2026 | early termination | Mayor removed the cameras after resident concerns
- Newport | Jul 2026 | canceled before deployment | City ended its pilot and declined to proceed after public concerns

Maine (2)

- Auburn | May 2026 | defunding | Council removed camera funding from the budget, letting the contract expire
- South Portland | Jun 2025 | early termination | Council voted to permanently end the contract

Massachusetts (13)

- Auburn | Aug 2026 | early termination | PD severed the relationship citing a contractual defect
- Bellingham | Aug 2026 | nonrenewal | PD declined renewal citing transparency and funding concerns; chief acknowledged features beyond a traditional plate reader
- Cambridge | Dec 2025 | early termination | City canceled after a breach of trust by the company
- East Bridgewater | Aug 2026 | canceled before deployment | Chief terminated the program after public outcry

- Framingham | Jun 2026 | nonrenewal | City declined renewal after months of resident opposition
- Grafton | Aug 2026 | early termination | Town canceled one month after implementation, following backlash
- Greenfield | Jan 2026 | early termination | Town ran out of funds for the cameras
- Hopkinton | Aug 2026 | early termination | Town voted to cancel after community pushback
- Littleton | Aug 2026 | early termination | Ended after concerns about unauthorized access
- Natick | Jan 2026 | early termination | Select board quashed the pilot at expiration; chief publicly apologized
- Stow | Aug 2026 | early termination | Chief announced cancellation following officer misuse (the Rogers stalking case)
- Watertown | Jan 2026 | canceled before deployment | City canceled before installation
- Wellesley | Aug 2026 | early termination | Town ended a two-year trial about a year early, citing an overwhelmingly changed landscape

Michigan (8)

- Clawson | May 2026 | early termination | Council canceled over data sharing concerns
- Dickinson County | Aug 2026 | early termination | Local drug enforcement agency ended its contract; sheriff covered all cameras
- Ferndale | Nov 2025 | early termination | City canceled after community pushback
- Menominee | May 2026 | early termination | Council voted unanimously not to proceed
- Oceana County | Aug 2026 | canceled before deployment | Sheriff killed a 90-day trial one week in after significant negative public feedback
- Sumpter County | Aug 2026 | nonrenewal | Sheriff ended a 60-day free trial early after public concerns
- Sumpter Township | Aug 2026 | canceled before deployment | Township canceled before installation after backlash
- Westland | Jul 2026 | early termination | Chief declined renewal after community pushback

Minnesota (4)

- Columbia Heights | Jun 2026 | early termination | Council canceled after resident pushback
- Isanti County | Aug 2026 | nonrenewal | Sheriff canceled citing budget considerations
- Sherburne County | Aug 2026 | early termination | Sheriff canceled before the trial period ended over community concerns
- West St. Paul | Aug 2026 | early termination | City manager canceled the trial after pushback

Missouri (8)

- Bolivar | Aug 2026 | early termination | Council voted unanimously to cancel and ban ALPRs; cameras covered
- Dutchtown | Mar 2026 | early termination | Ended over concerns data was being shared with ICE
- Henry County | Aug 2026 | nonrenewal | Sheriff will not renew at March 2027 expiration after community feedback
- Pulaski County | Aug 2026 | nonrenewal | County canceled Flock and declined an Axon contract
- Seneca | Feb 2026 | early termination | Ended in under 90 days over security concerns
- St. Charles County | Aug 2026 | early termination | Sheriff discontinued use after an abnormal pattern of searches was revealed
- Weston | Apr 2026 | canceled before deployment | Aldermen stopped installation
- Willard | Aug 2026 | nonrenewal | Chief declined renewal following backlash

Nebraska (1)

- Ord | Aug 2026 | early termination | First Nebraska city to remove Flock; unanimous vote after backlash

New Mexico (2)

- Bernalillo County | Aug 2026 | early termination | Sheriff fired Flock after losing trust in the company
- Taos | Jul 2026 | defunding | Council defunded 18 cameras and reallocated the money to other police operations

New York (5)

- Auburn | Aug 2026 | early termination | Unanimous council vote after resident concerns
- Ithaca | Mar 2026 | early termination | Council canceled after months of backlash
- Saranac Lake | Mar 2026 | early termination | Village dropped the plan after public backlash
- Scarsdale | Aug 2025 | early termination | Terminated after a 450-resident petition and loss of funding
- Tompkins County | Apr 2026 | early termination | Legislature voted 12-1 to cancel before auto-renewal

North Carolina (4)

- Asheville | Aug 2026 | early termination | Council voted to cancel; cameras from neighboring jurisdictions remain in city limits
- Davidson County | Aug 2026 | early termination | Commissioners terminated after 14 residents spoke against the cameras at a hearing
- Hillsborough | Oct 2025 | canceled before deployment | Town canceled mid-installation
- Pittsboro | May 2026 | early termination | Board voted 4-1 to terminate and defund

Ohio (3)

- Coshocton County | Aug 2026 | early termination | Sheriff ordered removal after losing community support
- Oxford | Aug 2026 | early termination | Council voted 6-1 over privacy concerns
- Wyandot County | Aug 2026 | early termination | Sheriff removed cameras after community feedback

Oklahoma (1)

- Marietta | Aug 2026 | early termination | Chief canceled after residents raised privacy and data retention concerns

Oregon (9)

- Albany | May 2026 | early termination | Council made an earlier pause permanent
- Bend | Jan 2026 | early termination | Council ended the pilot five months early
- Eugene | Dec 2025 | early termination | City canceled over data security concerns
- Josephine County | Aug 2026 | early termination | Sheriff canceled and deactivated cameras over privacy concerns
- Lane County | Dec 2025 | canceled before deployment | Sheriff canceled before installation
- Lincoln City | Dec 2025 | early termination | PD discontinued use over privacy concerns
- Springfield | Dec 2025 | canceled before deployment | City canceled and covered cameras pending removal after the Eugene revelations
- Winston | Aug 2026 | early termination | Ended amid budget cuts and privacy concerns

- Woodburn | Jun 2026 | early termination | Council permanently ended the contract after an audit revealed ICE access

Rhode Island (3)

- Glocester | Aug 2026 | early termination | Town voted 4-1 after residents packed town hall
- Narragansett | Aug 2026 | early termination | Unanimous council vote over resident concerns
- South Kingstown | Jul 2026 | early termination | Town canceled after residents raised privacy concerns

Tennessee (4)

- Kingston | Aug 2026 | nonrenewal | City ended the contract over financial concerns
- Knox County | Aug 2026 | early termination | Mayor declared the contract invalid; county considering a total ALPR ban
- Sullivan County | Aug 2026 | nonrenewal | Commission voted against renewal
- White County | Jul 2026 | early termination | County rescinded its authorizing resolution after significant public feedback

Texas (12)

- Aransas Pass | Jul 2026 | early termination | Council terminated after community pushback
- Austin | Jun 2025 | nonrenewal | City let the contract expire after backlash during the pilot; an early bellwether
- Bandera | May 2026 | early termination | Council terminated after months of public opposition
- Burnet County | Aug 2026 | early termination | Sheriff removed all cameras following public backlash
- Guadalupe County | Aug 2026 | early termination | Commissioners ended the contract early
- Hays County | Oct 2025 | early termination | Canceled following community pushback
- Hood County | Aug 2026 | early termination | Commissioners shut down and terminated amid privacy concerns; cameras covered
- Ingleside | Aug 2026 | early termination | Unanimous council vote after residents raised privacy concerns
- Kendall County | Aug 2026 | nonrenewal | Commissioners voted unanimously, saying they were not convinced the necessary assurances and protections exist
- Lago Vista | Aug 2026 | early termination | Unanimous council vote after public comment
- Pflugerville | Aug 2026 | early termination | Unanimous council vote to cancel and cover the cameras
- San Marcos | Dec 2025 | nonrenewal | City declined renewal after community pushback

Virginia (4)

- Charlottesville | Dec 2025 | nonrenewal | City declined to continue after a one-year pilot
- Christiansburg | Aug 2026 | early termination | Unanimous council vote to terminate and remove all cameras over data security concerns
- Elkton | Jul 2026 | early termination | Local activists persuaded the town to cancel
- Staunton | Dec 2025 | early termination | City terminated over a dispute with Flock

Washington (4)

- Edmonds | May 2026 | early termination | Council canceled over federal access concerns; third city in its county to do so
- Lynnwood | Feb 2026 | early termination | Unanimous vote after an earlier pause over federal access
- Mountlake Terrace | Dec 2025 | early termination | Unanimous vote over public records concerns
- Skamania County | Nov 2025 | early termination | Sheriff ended the county's contract

Wisconsin (6)

- Appleton | Jul 2026 | early termination | Unanimous council vote over public trust concerns
- Dane County | Apr 2026 | defunding | Board voted 32-1 to strip contract funding
- Kaukauna | Jul 2026 | nonrenewal | City declined renewal over fiscal concerns
- Oshkosh | Apr 2026 | early termination | Council voted unanimously to rescind the contract one day after approving it, after the chief raised trust and access issues
- Stoughton | Jul 2026 | early termination | Unanimous council vote after just three months
- Verona | Nov 2025 | nonrenewal | City voted against renewal over data concerns; later reporting noted the city having to work to get hardware removed

Sources

- Institute for Justice, ALPR Contract Cancellation Database (Dan King, Aug 26, 2026): ij.org/institute-for-justice-unveils-new-database-tracking-cancellations-of-license-plate-reader-contracts/ (every entry links to its original source)
- IJ press release, "As Abuses Mount Nationwide..." (Sept 2025): documents Flock's denial and later admission of the CBP pilot
- DeFlock tally via Newsweek map coverage (Aug 2026)
- CNN, Aug 26, 2026 (Tempe cancellation, IJ abuse count)
- WTMJ / Sheboygan Press / CBS 58 / WHBL, Aug 25-27, 2026 (Sheboygan covering and termination request)
- CBS Colorado (Denver council extension rejection)

Northeast Flor'da snapshot follow'ng the FDOT order (status ver'fied through September 9, 2026; to be re-ver'fied through September 14)

- Florida Department of Transportation | Aug 31, 2026 | state action | Revoked general use permits for LPRs in state rights-of-way; 30 days to comply; FDOT to remove non-compliant units; no future permits. Does not reach county or city roads.
- Duval County (JSO) | Aug 31, 2026 | discontinued countywide | Sheriff T.K. Waters: "it is my responsibility to listen to the concerns of our citizens and act accordingly"; discontinuing is "the appropriate course of action at this time"
- Putnam County | Aug 31, 2026 | ended program | Sheriff DeLoach: technology "advancing faster than the laws and regulations governing its use"
- Franklin County, Liberty County | Aug 31, 2026 | ended programs | Sheriffs ended programs the same day
- Baker County | Aug 31, 2026 | discontinued program | Sheriff Scotty Rhoden: decision made "to maintain public confidence" while calling LPRs a valuable tool
- Bradford County | Aug 31, 2026 | discontinued countywide | Sheriff directed the office to stop using LPR technology anywhere in the county, effective immediately
- Flagler County | Sept 2, 2026 | suspended Flock use, effective immediately | Counterexample on policy: Sheriff Rick Staly complied with FDOT and suspended Flock use, while publicly defending the technology, comparing the backlash to "defund the police," and calling for strong protections and accountability. Illustrates that the regional response includes regulated-use positions as well as discontinuation.
- Brevard County | Sept 2026 | terminated Flock use | Sheriff Wayne Ivey
- Clay County | Sept 2026 | removal | Removing all LPRs from county roadways
- Nassau County | Sept 2026 | stopped use | 34 cameras
- Volusia County | Sept 2026 | shut down countywide | Sheriff Chitwood
- Seminole County | Sept 2026 | suspended |

Tab 11: Requested Outcome, Immediate Steps, and Fallback Conditions

Why this matters to the Board: The requested outcome is removal of the system, as St. Lucie County voted. The immediate steps are a budget reduction tied to the program on the record and a workshop with the Board's authority defined by counsel. The fallback conditions apply only if the Board declines removal, and they are mitigations, not the objective.

The requested outcome is removal of the system. The immediate steps are two: a budget reduction tied to the program on the record at tonight's hearing, and a workshop at which the County Attorney defines the Board's authority. The conditions at the end are fallbacks for the case in which the Board declines removal; they are mitigations for a system this packet argues should not exist, not the objective. Everything below is tied to a potential mechanism within the Board's budget or property authority, subject to confirmation by the County Attorney, and written so that counsel can determine the enforceable vehicle. The Sheriff is an independent constitutional officer, and Florida law protects his independence in purchasing equipment (s. 30.53, F.S.); the Board's authority runs through the county budget (s. 30.49, F.S.), county property and rights-of-way, and the conditions attached to county funds.

The requested outcome: removal of the system

Model language. "The Board finds that the automated license plate recognition system operated through Flock Safety, consisting of cameras on county roads and property, a vendor-hosted archive of vehicle scans retained for months, vendor products that join those scans to other records, and sharing relationships with outside agencies, is not a system the county will host on county-controlled rights-of-way or property or support with county appropriation. The County Administrator shall inventory every automated license plate recognition device on county rights-of-way or county property, including portable and trailer-mounted units, within 60 days; the County Attorney shall identify the lawful mechanisms available to the Board to require removal of such devices from county-controlled property and to withhold county appropriation for the program, including the non-appropriation provision in the executed agreement; and the Board shall act on that report at a workshop within 45 days. Any future use of plate-reading technology in the county shall be brought to the Board as a separate public decision."

Reference. On September 1, 2026, the St. Lucie County Commission voted 3 to 2 to remove automated license plate readers from county-controlled roads, halt new permits, review and revoke existing ones, issue 30-day removal notices, and inventory the devices.

Why removal rather than regulation. A retention period is a setting; this county's changed from 30 days to 365 on an order form. A sharing setting can change without the customer's knowledge; Mountain View shows it. Analytical capability arrives as a product; Nova and OS Investigate show it. The safeguards the vendor announced in August are vendor-controlled and revisable. Each of those facts is a reason a rule written today cannot bind the system tomorrow. Infrastructure that is not there cannot be reconfigured, expanded, breached, or repurposed.

Immediate step one: the budget vote

Available at the September 15, 2026 final budget hearing. Under s. 30.49(4), F.S., the Board may reduce items of expenditure in the Sheriff's proposed budget. The motion available is to reduce the law enforcement transfer by \$481,000, the county-funded cost of the program in FY2026 by the Sheriff's own account, and to state on the record that the reduction corresponds to the license plate reader program and that the Board does not intend county funds to support it. Two limits are stated plainly. The Sheriff may appeal a reduction to the Administration Commission under s. 30.49(5). And because the Board does not appropriate line by line,

a reduced total does not by itself prevent the program from being funded from what remains; whether a reduction tied to the program on the record constitutes an absence of appropriated funds under the agreement's non-appropriation provision is a question for the County Attorney. The reduction places the Board's intent on the record; the workshop determines its effect.

Immediate step two: the workshop

Model language. "The County Attorney is directed to review the executed agreements between the Sheriff's Office and Flock Safety, including all order forms and any updated agreement referenced therein; to determine which terms govern the December 17, 2025 order; to identify the enforceable mechanisms available to the Board, including the non-appropriation provision in the 2023 special terms, the assignment provision in section 10.2, and the termination provisions in section 6; to advise on the boundary between the Board's authority and the Sheriff's under sections 30.49 and 30.53, Florida Statutes; and to report to the Board at a workshop to be scheduled within 45 days. The County Administrator shall, within 60 days, inventory every automated license plate recognition device located on county rights-of-way or county property, including portable and trailer-mounted units, and report the location, owner, and permit or authorization status of each to the Board."

Fallback conditions, only if the Board declines removal

Fallback 1: Disclosure as a condition of county funding. Authority: s. 30.49(3), F.S., permits the Board to require the Sheriff to furnish relevant and pertinent expenditure information; s. 30.49(4) permits the Board to amend, modify, increase, or reduce items of expenditure. Model language: "Beginning with the fiscal year 2028 budget submission, the Sheriff's annual budget submission to the Board shall include supporting documentation identifying each surveillance technology system funded in whole or in part by county appropriation, by vendor and capability, including annual cost, the retention period for data collected, the categories of data collected, the agencies and networks with which data is shared, and the provisions of any vendor agreement governing data ownership, licensing, and assignment. The Board shall review this documentation in an open session prior to adopting the budget. The Sheriff's Office shall, as a condition of county appropriation for surveillance technology, provide to the Board annually the audit reports and program evaluations required by its own written policy, with plate numbers redacted as required by s. 316.0777, F.S., and the Board shall make them available to the public." Definition of surveillance technology: "Any device, software, or system, by whatever name and in whatever form, that collects, retains, correlates, or shares data on the movements, locations, or associations of identifiable persons, including automated license plate recognition systems and any product that joins such data to other records."

Fallback 2: Board approval for placements on county property. Potential authority, subject to counsel: the Board's authority over county property and county rights-of-way. Model language: "No automated license plate recognition device shall be placed or remain on county rights-of-way or county property without approval of the Board in an open meeting, under a mechanism the County Attorney identifies as within the Board's authority."

Fallback 3: Notice, a written record, and a vote before expansion, and a retention ceiling. Potential authority, subject to counsel: conditions attached to county appropriations and to the use of county property. Model language: "No new data type, data source, analytical capability, sensing capability, external sharing arrangement, or extension of the retention period shall be activated on any surveillance technology system funded in whole or in part by county appropriation, or located on county property, unless the Board has first received written notice describing the change, the notice has been entered into the public record, and the Board has voted to approve the change in an open meeting. As a condition of county appropriation, data collected by automated license plate recognition systems shall be retained no longer than a period set by the Board in public session, which shall be a ceiling that requires a Board vote to raise, except for specific records preserved in connection with an identified investigation under a documented case number." The vendor's own recommended default of seven days is cited as evidence that 365 days is not necessary, not as the recommended standard. Data that no longer exists cannot be queried, shared, breached, or repurposed.

The principle

A policy governs the conduct of the people who work under it. It does not govern what the system is permitted to become. Policies and contracts can reduce risk. The only way to eliminate the risks created by this infrastructure is to remove it. Do not build the surveillance architecture first and hope that policy can contain everything it becomes later.

Appendix: Primary Documents

Each item below is bound behind a divider that names the document, the pages included, and where the complete document can be obtained. Pages are clipped to those the packet cites; every quotation in the packet can be checked against them. The Master Claims Register, which traces every statement in this packet to its source, is available to any commissioner or staff member on request.

1. Sheriff's Office application IG039 to the State Board of Immigration Enforcement (FDLE cabinet package, Sept. 30, 2025): award table and application narrative.
2. Executed Government Agency Agreement, Sheriff's Office and Flock Safety (2022): title page and sections 4.1, 4.2, 4.4, 6.2, 6.6, 8.1, and 10.2. Records request R042893-082726.
3. Order forms: October 1, 2023 with special terms (including non-appropriation); first pages of the December 3, 2024, March 21, 2025, and December 17, 2025 orders. Same request.
4. Sheriff's Office Policy 41.35, complete. Same request.
5. Sheriff's Office 2026 news release. Same request.
6. County FY2027 Recommended Budget, Sheriff's Office expenditures page, captured September 15, 2026.
7. Public records request R042893-082726 as filed, and the portal page showing it marked "Completed / Full Release."
8. Florida legislative lobbyist registrations for Flock Safety, 2026 (floridalobbyist.gov).
9. Wyden and Krishnamoorthi letter to FTC Chair Ferguson, November 3, 2025, complete (wyden.senate.gov).
10. Florida Department of Transportation Engineering and Operations Memorandum 26-01, August 31, 2026, complete (fdot.gov).
11. Flock Safety, "Flock Updates Privacy, Accountability, Security, and Transparency Safeguards," August 13, 2026, pages 1 to 3 (flocksafety.com).
12. WIRED, "Flock Has a Powerful New AI Tool for Police. We Got Its Code," August 19, 2026, pages 1 to 4 (wired.com).
13. *Chatrie v. United States*, No. 25-112 (U.S. June 29, 2026), syllabus (supremecourt.gov).
14. *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc), opening pages (ca4.uscourts.gov).
15. Chief Financial Officer press release, October 21, 2025, award list and Sheriff Hardwick's statement (myfloridacfo.com).

Cited but not reproduced: the county FY2026 adopted budget workbook page ("Transfer to Officers, \$103,058,446"), cleargov.com; Sheriff Hardwick's text to commissioners as published by Action News Jax; First Coast News, February 2023; St. Lucie County Commission action of September 1, 2026 (CBS12); Mountain View, California statement, February 2026.

Appendix 1

Sheriff's Office application IG039 to the State Board of Immigration Enforcement

Pages included: award table page and application narrative pages (4)

Full document: FDLE, State Board of Immigration Enforcement, Sept. 30, 2025 cabinet package, fdle.state.fl.us

MEETING OF THE STATE BOARD OF IMMIGRATION ENFORCEMENT
September 30, 2025

ITEM 1 Consideration of Rules

(See Attachment 1)

RECOMMEND APPROVAL

ITEM 2 Consideration of Grant Applications

(See Attachment 2)

RECOMMEND APPROVAL

State Board of Immigration Enforcement Award Reviews

Awards below are awaiting an award decision from the Board.

09/25/2025 11:27 AM

Agency Information			Requested Budget Summary									Executive Director Recommendation	Board Decision		
ID #	Organization	County	IGP-A: Training Programs for 287(g)	IGP-B: Detention Beds for ICE	IGP-C: Transportation	IGP-D: Travel and Lodging for 287(g)	IGP-E: LEO Bonuses	IGP-F: CO Bonuses	IGP-G: Equipment, Hardware, Software	IGP-H: Other Costs	Total Funding Request		Circle One		
IG021	Sarasota County Sheriff's Office	Sarasota	\$0.00	\$62,400.00	\$10,324.18	\$0.00	\$44,136.50	\$92,579.00	\$0.00	\$0.00	\$209,439.68	Approved 09/11/25	Approve	Change	Deny
IG022	Polk County Sheriff's Office	Polk	\$0.00	\$508,000.00	\$42,742.00	\$0.00	\$301,420.00	\$89,349.50	\$0.00	\$0.00	\$941,511.50	Approved 09/11/25	Approve	Change	Deny
IG023	Marianna Police Department	Jackson	\$0.00	\$0.00	\$0.00	\$0.00	\$4,306.00	\$0.00	\$18,520.00	\$7,535.50	\$30,361.50	Approved 09/11/25	Approve	Change	Deny
IG024	County of Santa Rosa Sheriff's Office	Santa Rosa	\$0.00	\$50,000.00	\$106,254.46	\$0.00	\$0.00	\$32,295.00	\$2,400.00	\$0.00	\$190,949.46	Approved 09/11/25	Approve	Change	Deny
IG025	City of St. Augustine Police Department	St. Johns	\$0.00	\$0.00	\$0.00	\$0.00	\$12,918.00	\$0.00	\$0.00	\$24,393.00	\$37,311.00	Approved 09/11/25	Approve	Change	Deny
IG029	City of Largo Police Department	Pinellas	\$45,385.24	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$45,385.24	Approved 09/25/25	Approve	Change	Deny
IG030	Franklin County Sheriff's Office	Franklin	\$0.00	\$0.00	\$37,695.48	\$0.00	\$8,612.00	\$2,153.00	\$0.00	\$0.00	\$48,460.48	Approved 09/18/25	Approve	Change	Deny
IG031	Charlotte County Sheriff's Office	Charlotte	\$0.00	\$68,000.00	\$27,425.50	\$0.00	\$43,060.00	\$26,912.50	\$0.00	\$0.00	\$165,398.00	Approved 09/11/25	Approve	Change	Deny
IG034	Lake County Sheriff's Office	Lake	\$0.00	\$44,800.00	\$0.00	\$0.00	\$0.00	\$32,295.00	\$0.00	\$0.00	\$77,095.00	Approved 09/11/25	Approve	Change	Deny
IG035	Alachua County Sheriff's Office	Alachua	\$0.00	\$315,000.00	\$96,176.00	\$0.00	\$0.00	\$16,147.50	\$27,674.00	\$0.00	\$454,997.50	Approved 09/18/25	Approve	Change	Deny
IG036	Madison County Sheriff's Office	Madison	\$0.00	\$0.00	\$178,810.20	\$0.00	\$13,994.50	\$12,918.00	\$40,849.24	\$0.00	\$246,571.94	Approved 09/18/25	Approve	Change	Deny
IG037	Holly Hill Police Department	Volusia	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$4,306.00	\$12,900.00	\$15,262.83	\$32,468.83	Approved 09/25/25	Approve	Change	Deny
IG038	City of Miami Springs Police Department	Miami-Dade	\$0.00	\$0.00	\$0.00	\$6,798.00	\$2,153.00	\$0.00	\$17,960.00	\$40,575.24	\$67,486.24	Approved 09/25/25	Approve	Change	Deny
IG039	St. Johns County Sheriff's Office	St. Johns	\$0.00	\$48,000.00	\$5,210.00	\$0.00	\$68,896.00	\$37,677.50	\$840,216.50	\$0.00	\$1,000,000.00	Approved 09/11/25	Approve	Change	Deny
IG040	Marion County Sheriff's Office	Marion	\$0.00	\$0.00	\$69,117.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$69,117.00	Approved 09/11/25	Approve	Change	Deny
IG041	Hernando County Sheriff's Office	Hernando	\$0.00	\$31,500.00	\$163,638.30	\$0.00	\$0.00	\$40,907.00	\$0.00	\$0.00	\$236,045.30	Approved 09/11/25	Approve	Change	Deny
IG042	Clay County Sheriff's Office	Clay	\$75,738.31	\$15,000.00	\$364,442.32	\$0.00	\$61,360.50	\$21,530.00	\$68,080.00	\$0.00	\$606,151.13	Approved 09/11/25	Approve	Change	Deny

**State Board of Immigration Enforcement
Application Budget Details**

ID #: IG039

Participating Agency: St. Johns County Sheriff's Office

Budget Request Summary

Budget Category	Amount Allocated
IGP-A: Training Programs for 287(g)	\$0.00
IGP-B: Detention Beds for ICE	\$48,000.00
IGP-C: Transportation	\$5,210.00
IGP-D: Travel and Lodging for 287(g)	\$0.00
IGP-E: Law Enforcement Bonuses	\$68,896.00
IGP-F: Corrections Bonuses	\$37,677.50
IGP-G: Equipment, Hardware, Software	\$840,216.50
IGP-H: Other Costs	\$0.00
Total Requested Amount	\$1,000,000.00

Proposed Budget Details by Category

IGP-B: Subletting Detention Beds

Item Name	Description	Amount
SJSO- Detention Beds	\$100 per day x approx. 480 bed days= \$48,000	\$48,000.00

IGP-C: Transportation on Behalf of ICE

Item Name	Description	Amount
SJSO - Transportation - OT	Overtime: 35 hours x \$64.00= \$2,240.00	\$2,240.00
SJSO- Transportation - Travel	Meals: \$36 per day x 10 days x 2 people: \$720.00 Lodging: \$225.00 per night x 10 nights= \$2,250.00	\$2,970.00

IGP-E: LEO Bonus Payments

Item Name	Description	Amount
SJSO- DIO Bonus	\$1,000 bonus x approx. 64 officers= \$64,000 FICA: 7.65% x \$64,000= \$4,896.00	\$68,896.00

IGP-F: CO Bonus Payments

Item Name	Description	Amount
SHSO- WSO Bonus	\$1,000 bonus x 35 officers = \$35,000 FICA: \$35,000x 7.65% = \$3,677.50	\$37,677.50

IGP-G: Equipment, Hardware, Software for 287(g)

Item Name	Description	Amount
SJSO- Rapid ID scanners	(75) Rapid ID devices at \$3,265.25 = \$244,894.00	\$244,894.00
SJSO- LPR's and LPR Trailers	(23)-Flock LPR's at approx. \$18,567.39 = \$427,050.00 (6) LPR mobile trailers at approx. \$16,595.83 = \$99,575.00 (3) Wanco small speed trailer with LPR at approx. \$22,899.16= \$68,697.50	\$595,322.50

Additional Justification:

State Board of Immigration Enforcement Application Budget Details

St. Johns County Sheriff's Office would like to purchase 75 Rapid ID fingerprint scanners for our DIO's to use. The Rapid ID fingerprint scanners will identify suspected unauthorized aliens with warrants that have no identification to identify them or id they present a false identification. Rapid ID fingerprint scanners will give our law enforcement deputies the ID of the unauthorized alien within seconds. If there is an active deportation warrant, this device will alert the officer so they can take the next steps on detaining the unauthorized person and notifying ICE. Our agency would also like to purchase mobile surveillance platforms with license plate readers (LPR's) and license plate readers camera's-both fixed and mobile. This would be a purchase of 23 LPR's and 9 trailers- 6 small speed trailers with flex LPR cameras attached and 3 compact speed trailers with LPR's. The LPR scan captures the date, time and location of passing vehicles and the data is stored for up to one year. We will share this data with federal agencies including ICE and CBP. If ICE or CBP is searching for a specific person (for example, someone with an outstanding deportation order), LPR data can be used to track where their vehicle has been spotted. This allows law enforcement to develop a pattern of life to potentially identify home and work locations and plan enforcement actions. If a vehicle is associated to a known subject with an immigration warrant listed in NCIC, then the LPR will scan the license plate and alert our agency of the hit to take immediate enforcement action. The mobile surveillance/LPR platforms (trailers) can be deployed to various check points or areas with the county as intelligence dictates. These mobile surveillance platforms can be overt in nature as needed. The fixed LPR cameras would be placed in high traffic areas such as interstate 95 (I-95). It is well established these thoroughfares are known for human smuggling of illegal immigrants to avoid detection.

Appendix 2

Executed Government Agency Agreement, Sheriff's Office and Flock Safety (2022)

Pages included: title page and the pages carrying sections 4.1, 4.2, 4.4, 6.2, 6.6, 8.1, 10.2
(production pages 80, 87 to 92)

Full document: public records request R042893-082726 (113 pages), St. Johns County Sheriff's Office

flock safety

GOVERNMENT AGENCY AGREEMENT

This Government Agency Agreement (this “**Agreement**”) is entered into by and between Flock Group, Inc. with a place of business at 1170 Howell Mill Rd NW Suite 210, Atlanta, GA 30318 (“**Flock**”) and the police department or government agency identified in the signature block of the order form (“**Agency**”) (each a “**Party**,” and together, the “**Parties**”).

RECITALS

WHEREAS, Flock offers a software and hardware solution for automatic license plate detection through Flock’s technology platform (the “**Flock Service**”), and upon detection, the Flock Services are capable of capturing audio, image, and recordings data of suspected vehicles (“**Footage**”) and can provide notifications to Agency upon the instructions of Non-Agency End User (“**Notifications**”);

WHEREAS, Agency desires access to the Flock Service on existing cameras, provided by Agency, or Flock provided Hardware (as defined below) in order to create, view, search and archive Footage and receive Notifications, including those from non-Agency users of the Flock Service (where there is an investigative or bona fide lawful purpose) such as schools, neighborhood homeowners associations, businesses, and individual users;

WHEREAS, Flock deletes all Footage on a rolling thirty (30) day basis, Agency is responsible for extracting, downloading and archiving Footage from the Flock System on its own storage devices for auditing for prosecutorial/administrative purposes; and

WHEREAS, Flock desires to provide Agency the Flock Service and any access thereto, subject to the terms and conditions of this Agreement, solely for the awareness, prevention, and prosecution of crime, bona fide investigations by police departments, and archiving for evidence gathering (“**Purpose**”).

AGREEMENT

NOW, THEREFORE, Flock and Agency agree as follows and further agree to incorporate the Recitals into this Agreement.

1. DEFINITIONS

Certain capitalized terms, not otherwise defined herein, have the meanings set forth or cross-referenced in this Section 1.

Information may include processing the Proprietary Information to send Agency alerts, such as when a car exits Agency 's neighborhood, or to analyze the data collected to identify motion or other events. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (a) is or becomes generally available to the public, or (b) was in its possession or known by it prior to receipt from the Disclosing Party, or (c) was rightfully disclosed to it without restriction by a third party, or (d) was independently developed without use of any Proprietary Information of the Disclosing Party. Nothing in this Agreement will prevent the Receiving Party from disclosing the Proprietary Information pursuant to any judicial or governmental order, provided that the Receiving Party gives the Disclosing Party reasonable prior notice of such disclosure to contest such order. For clarity, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to: (a) comply with a legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Flock, its users, a third party, or the public as required or permitted by law, including respond to an emergency situation. Agency hereby expressly grants Flock a non-exclusive, worldwide, perpetual, royalty-free right and license (during and after the term hereof) to disclose the Agency Data (inclusive of any Footage) to enable law enforcement monitoring against law enforcement hotlists as well as provide Footage search access to law enforcement for investigative purposes only. Flock may store deleted Footage in order to comply with certain legal obligations but such retained Footage will not be retrievable without a valid court order.

4.2 Agency Data.. As between Flock and Agency, all right, title and interest in the Agency Data, belong to and are retained solely by Agency. Agency hereby grants to Flock a limited, non-exclusive, royalty-free, worldwide license to use the Agency Data and perform all acts with respect to the Agency Data as may be necessary for Flock to provide the Flock Services to Agency, including without limitation the Support Services set forth in Section 2.9 above, and a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify and distribute the Agency Data as a part of the Aggregated Data (as defined in Section 4.4 below). As between Agency and Non-Agency End Users that have prescribed access of Footage to Agency, each of Agency and Non-Agency End Users will share all right, title and interest in the Non-Agency End User Data. This Agreement does not by itself make any Non-Agency End User Data the sole property or the Proprietary Information of Agency. Flock will automatically delete Footage older than thirty (30) days. Agency has a thirty (30) day window to view, save and/or transmit Footage to the relevant government agency prior to its deletion.

4.3 Feedback. If Agency provides any suggestions, ideas, enhancement requests, feedback, recommendations or other information relating to the subject matter hereunder, Agency hereby assigns (and will cause its agents and representatives to assign) to Flock all right, title and interest (including intellectual property rights) with respect to or resulting from any of the foregoing.

4.4 Aggregated Data. Notwithstanding anything in this Agreement to the contrary, Flock shall have the right to collect and analyze data that does not refer to or identify Agency or any individuals or de-identifies such data and other information relating to the provision, use and performance of various aspects of the Services and related

systems and technologies (including, without limitation, information concerning Agency Data and data derived therefrom). For the sake of clarity, Aggregated Data is compiled anonymous data which has been stripped of any personal identifying information. Agency acknowledges that Flock will be compiling anonymized and/or aggregated data based on Agency Data input into the Services (the "*Aggregated Data*"). Agency hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right and license (during and after the Service Term hereof) to (i) use and distribute such Aggregated Data to improve and enhance the Services and for other development, diagnostic and corrective purposes, other Flock offerings, and crime prevention efforts, and (ii) disclose the Agency Data (both inclusive of any Footage) to enable law enforcement monitoring against law enforcement hotlists as well as provide Footage search access to law enforcement for investigative purposes only. No rights or licenses are granted except as expressly set forth herein. Flock shall not sell Agency Data or Aggregated Data.

5. PAYMENT OF FEES

5.1a Wing Fees. For Wing products, the Agency will pay Flock the first Usage Fee and the Implementation Fee (as described on the Order Form attached hereto, together the "*Initial Fees*") as set forth on the Order Form on or before the 30th day following the Effective Date of this Agreement. Flock shall have no liability resulting from any delay by the Agency in installing the Embedded Software on the Agency Hardware. If applicable, Agency shall pay the ongoing Usage Fees set forth on the Order Form with such Usage Fees due and payable thirty (30) days in advance of each payment period. All payments will be made by either ACH, check, or credit card.

5.1b Falcon Fees. For Falcon products during the Initial Term, Agency will pay Flock fifty percent (50%) of the first Usage Fee, the Implementation Fee and any fee for Hardware (as described on the Order Form attached hereto, together the "*Initial Fees*") as set forth on the Order Form on or before the 30th day following receipt of initial invoice after Effective Date. Upon commencement of installation, Flock will issue an invoice for twenty-five percent (25%) of the Initial Fees, and Agency shall pay on or before 30th day following receipt of invoice. Upon completion of installation, Flock will issue an invoice for the remaining balance and Agency shall pay on or before 30th day following receipt of final invoice. Flock is not obligated to commence the Installation Services unless and until the first payment has been made and shall have no liability resulting from any delay related thereto. For a Renewal Term, as defined below, Agency shall pay the entire invoice on or before the 30th day following receipt of invoice.

5.2 Changes to Fees. Flock reserves the right to change the fees or applicable charges and to institute new charges and fees at the end of the Initial Term or any Renewal Term, upon sixty (60) days' notice prior to the end of such Initial Term or Renewal Term (as applicable) to Agency (which may be sent by email). If Agency believes that Flock has billed Agency incorrectly, Agency must contact Flock no later than sixty (60) days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Flock's Agency support department. Agency acknowledges and agrees that a failure to contact Flock within this sixty (60) day period will serve as a waiver of any claim Agency may have had as a result of such billing error.

5.3 Invoicing, Late Fees; Taxes. Flock may choose to bill through an invoice, in which case, full payment for invoices issued in any given month must be received by Flock thirty (30) days after the mailing date of the invoice.

If Agency is a non-tax exempt entity, Agency shall be responsible for all taxes associated with Services other than U.S. taxes based on Flock's net income.

6. TERM AND TERMINATION

6.1a Wing Term. Subject to earlier termination as provided below, the initial term of this Agreement shall be for the period of time set forth on the Order Form (the "**Initial Term**"). The Term shall commence upon execution of this Agreement. *Following the Initial Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form* (each, a "**Renewal Term**", and together with the Initial Term, the "**Service Term**") *unless either party gives the other party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.*

6.1b Falcon Term. Subject to earlier termination as provided below, the initial term of this Agreement shall be for the period of time set forth on the Order Form (the "**Initial Term**"). The Term shall commence upon first installation and validation of a Unit. *Following the Initial Term, unless otherwise indicated on the Order Form, this Agreement will automatically renew for successive renewal terms for the length set forth on the Order Form* (each, a "**Renewal Term**", and together with the Initial Term, the "**Service Term**") *unless either party gives the other party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.*

6.2 Termination for Convenience. At any time during the agreed upon Term, an Agency not fully satisfied with the service may self-elect to terminate this Agreement for convenience. Termination for convenience will result in a one-time fee of \$500 per Flock Hardware. Upon termination for convenience, a refund will be provided for Falcon Cameras, prorated for any fees for the remaining Term length set forth previously. Agency will remain liable to pay the full outstanding fees for any Wing product on the effective date of termination of that Order Form. Flock will invoice, and Agency will pay, any unbilled fees and any unpaid fees covering the remainder of the term of that Order Form had it not been terminated. Termination for convenience of the Agreement by the Agency will be effective immediately. Flock will provide advanced written notice and remove all Flock Hardware at Flock's own convenience, within a commercially reasonable period of time upon termination.

6.3 Termination. Notwithstanding the termination provisions in Section 2.4(b), in the event of any material breach of this Agreement, the non-breaching party may terminate this Agreement prior to the end of the Service Term by giving thirty (30) days prior written notice to the breaching party; provided, however, that this Agreement will not terminate if the breaching party has cured the breach prior to the expiration of such thirty (30) day period. Either party may terminate this Agreement, without notice, (i) upon the institution by or against the other party of insolvency, receivership or bankruptcy proceedings, (ii) upon the other party's making an assignment for the benefit of creditors, or (iii) upon the other party's dissolution or ceasing to do business. Upon termination for Flock's material breach, Flock will refund to Agency a pro-rata portion of the pre-paid fees for Services not received due to such termination.

6.5 No-Fee Term. For the Term of this Agreement, Flock will provide Agency with complimentary access to 'hot-list' alerts, which may include 'hot tags', stolen vehicles, Amber Alerts, etc. ("**No-Fee Term**"). In the event a Non-Agency End User grants Agency access to Footage and/or Notifications from a Non-Agency End User Unit, Agency will have access to Non-Agency End User Footage and/or Notifications until deletion, subject to the thirty (30) day

retention policy. Non-Agency End Users and Flock may, in their sole discretion, leave access open. The No-Fee Term will survive the Term of this Agreement. Flock, in its sole discretion, can determine not to provide additional No-Fee Terms or can impose a price per No-Fee Term upon thirty (30) days' notice. Agency may terminate any No-Fee Term or access to future No-Fee Terms upon thirty (30) days' notice.

6.6 Survival. The following Sections will survive termination: 2.4, 2.5, 3, 4, 5 (with respect to any accrued rights to payment), 5.4, 6.5, 7.4, 8.1, 8.2, 8.3, 8.4, 9.1 and 10.5.

7. REMEDY; WARRANTY AND DISCLAIMER

7.1 Remedy. Upon a malfunction or failure of Flock Hardware or Embedded Software (a "*Defect*"), Agency must notify Flock's technical support as described in Section 2.9 above. If Flock is unable to correct the Defect, Flock shall, or shall instruct one of its contractors to repair or replace the Flock Hardware or Embedded Software suffering from the Defect. Flock reserves the right in their sole discretion to refuse or delay replacement or its choice of remedy for a Defect until after it has inspected and tested the affected Unit provided that such inspection and test shall occur within seventy-two (72) hours after Agency notifies the Flock of a known Defect. In the event of a Defect, Flock will repair or replace the defective Unit at no additional cost. In the event that a Unit is lost, stolen, or damaged, Agency may request that Flock replace the Unit at a fee according to the then-current Reinstall Policy (<https://www.flocksafety.com/reinstall-fee-schedule>). Agency shall not be required to replace subsequently lost, damaged or stolen Units, however, Agency understands and agrees that functionality, including Footage, will be materially affected due to such subsequently lost, damaged or stolen Units and that Flock will have no liability to Agency regarding such affected functionality nor shall the Usage Fee or Implementation Fees owed be impacted. Flock is under no obligation to replace or repair Hardware.

7.2 Exclusions. Flock will not provide the remedy described in Section 7.1 if Agency is found to have misused the Flock Hardware, Agency Hardware or Embedded Software in any manner.

7.3 Warranty. Flock shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Installation Services in a professional and workmanlike manner. Upon completion of any installation or repair, Flock shall clean and leave the area in good condition. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Flock or by third-party providers, or because of other causes beyond Flock's reasonable control, but Flock shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

7.4 Disclaimer. THE REMEDY DESCRIBED IN SECTION 7.1 ABOVE IS AGENCY'S SOLE REMEDY, AND FLOCK'S SOLE LIABILITY, WITH RESPECT TO DEFECTIVE EMBEDDED SOFTWARE. THE FLOCK DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED OR ERROR FREE; NOR DOES IT MAKE ANY WARRANTY AS TO THE RESULTS THAT MAY BE OBTAINED FROM USE OF THE SERVICES. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED "AS IS" AND FLOCK DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE AND NON-INFRINGEMENT. THIS DISCLAIMER OF SECTION 7.4 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 10.6, OR IF NO STATE IS MENTIONED IN SECTION 10.6, BY THE LAW OF THE STATE OF GEORGIA.

7.5 Insurance. Flock will maintain commercial general liability policies with policy limits reasonably commensurate with the magnitude of Flock's business risk. Certificates of Insurance can be provided upon request.

7.6 Force Majeure. Flock is not responsible nor liable for any delays or failures in performance from any cause beyond its control, including, but not limited to acts of God, changes to law or regulations, embargoes, war, terrorist acts, acts or omissions of third-party technology providers, riots, fires, earthquakes, floods, power blackouts, strikes, weather conditions or acts of hackers, internet service providers or any other third party or acts or omissions of Agency or any Authorized End User.

8. LIMITATION OF LIABILITY; NO FEE TERM; INDEMNITY

8.1 Limitation of Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY, FLOCK AND ITS SUPPLIERS (INCLUDING BUT NOT LIMITED TO ALL HARDWARE AND TECHNOLOGY SUPPLIERS), OFFICERS, AFFILIATES, REPRESENTATIVES, CONTRACTORS AND EMPLOYEES SHALL NOT BE RESPONSIBLE OR LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT OR TERMS AND CONDITIONS RELATED THERETO UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY, OR OTHER THEORY: (A) FOR ERROR OR INTERRUPTION OF USE OR FOR LOSS OR INACCURACY, INCOMPLETENESS OR CORRUPTION OF DATA OR FOOTAGE OR COST OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES OR TECHNOLOGY OR LOSS OF BUSINESS; (B) FOR ANY INDIRECT, EXEMPLARY, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES; (C) FOR ANY MATTER BEYOND FLOCK'S ACTUAL KNOWLEDGE OR REASONABLE CONTROL INCLUDING REPEAT CRIMINAL ACTIVITY OR INABILITY TO CAPTURE FOOTAGE OR IDENTIFY AND/OR CORRELATE A LICENSE PLATE WITH THE FBI DATABASE; (D) FOR ANY PUBLIC DISCLOSURE OF PROPRIETARY INFORMATION MADE IN GOOD FAITH; (E) FOR CRIME PREVENTION; OR (F) FOR ANY AMOUNTS THAT, TOGETHER WITH AMOUNTS ASSOCIATED WITH ALL OTHER CLAIMS, EXCEED THE FEES PAID AND/OR PAYABLE BY AGENCY TO FLOCK FOR THE SERVICES UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS PRIOR TO THE ACT OR OMISSION THAT GAVE RISE TO THE LIABILITY, IN EACH CASE, WHETHER OR NOT FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN THE EVENT OF AN EMERGENCY, AGENCY SHOULD CONTACT 911 AND SHOULD NOT RELY ON THE SERVICES. THIS LIMITATION OF LIABILITY OF SECTION 8 ONLY APPLIES TO THE EXTENT ALLOWED BY THE GOVERNING LAW OF THE STATE MENTIONED IN SECTION 10.6, OR IF NO STATE IS MENTIONED IN SECTION 10.6, BY THE LAW OF THE STATE OF GEORGIA.

8.2 Additional No-Fee Term Requirements. IN NO EVENT SHALL FLOCK'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THE COMPLIMENTARY NO-FEE TERM AS DESCRIBED IN SECTION 6.5 EXCEED \$100, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE. Parties

acknowledge and agree that the essential purpose of this Section 8.2 is to allocate the risks under the No-Fee Term described in Section 6.5 and limit potential liability given the aforementioned complimentary service, which would have been substantially higher if Flock were to assume any further liability other than as set forth herein. Flock has relied on these limitations in determining whether to provide the complimentary No-Fee Term. The limitations set forth in this Section 8.2 shall not apply to claims or damages resulting from Flock's other obligations under this Agreement.

8.3 Responsibility. Each Party to this Agreement shall assume the responsibility and liability for the acts and omissions of its own employees, deputies, officers, or agents, in connection with the performance of their official duties under this Agreement. Each Party to this Agreement shall be liable (if at all) only for the torts of its own officers, agents, or employees that occur within the scope of their official duties. Agency will not pursue any claims or actions against Flock's suppliers.

8.4 Indemnity. Agency hereby agrees to indemnify and hold harmless Flock against any damages, losses, liabilities, settlements and expenses in connection with any claim or action that arises from an alleged violation of Section 3.2, a breach of this Agreement, Agency's Installation Obligations, Agency's sharing of any data in connection with the Flock system, Flock employees or agent or Non-Agency End Users, or otherwise from Agency's use of the Services, Flock Hardware, Agency Hardware and any Embedded Software, including any claim that such actions violate any applicable law or third party right. Although Flock has no obligation to monitor Agency's use of the Services, Flock may do so and may prohibit any use of the Services it believes may be (or alleged to be) in violation of Section 3.2 or this Agreement.

9. RECORD RETENTION

9.1 Data Preservation. The Agency agrees to store Agency Data in compliance with all applicable local, state and federal laws, regulations, policies and ordinances and their associated record retention schedules. As part of Agency's consideration for paid access and no-fee access to the Flock System, to the extent that Flock is required by local, state or federal law to preserve the Agency Data, Flock will notify Agency of the requirement and applicable retention period, and Agency agrees to preserve and securely store this data on Flock's behalf so that should Flock be legally compelled by judicial or government order, Flock may retrieve the data from Agency upon demand.

10. MISCELLANEOUS

10.1 Severability. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

10.2 Assignment. This Agreement is not assignable, transferable or sublicensable by Agency except with Flock's prior written consent. Flock may transfer and assign any of its rights and obligations, in whole or in part, under this Agreement without consent.

- Pasco County | Sept 2026 | partial removal | About 60 removed from public roads; roughly 110 private cameras remain
- Hernando County | Sept 2026 | removal from county rights-of-way |
- Neptune Beach, Atlantic Beach | Sept 2026 | shut down / suspended | Per local reporting; Jacksonville Beach retained its municipal network
- St. Lucie County | Sept 1, 2026 | county commission vote, 3 to 2 | Remove ALPRs from county-controlled rights-of-way; halt new permits; review and revoke existing; 30-day removal notices; inventory. Added to the agenda the same day by Commissioner Clasby; dissenters cited inadequate notice.
- St. Johns County (SJSO) | Sept 2, 2026 | complying on state roads only | Fate of roughly 180 county-road cameras not stated; SJSO statement supports “the development of legislation which addresses concerns around LPR technology and establishes clear standards for its use”

Sources: FDOT memo (COO Will Watts, Aug 31, 2026); News4Jax, Action News Jax, Jacksonville Today, First Coast News, SJ Citizen, CBS12, Sept 1 to 3, 2026.

Appendix 3

Order forms

Pages included: Oct. 1, 2023 order with special terms (4 pages); Dec. 3, 2024, Mar. 21, 2025, and Dec. 17, 2025 orders, first page of each showing retention period and term

Full document: public records request R042893-082726

**Flock Safety + FL - St. Johns County
SO**

Flock Group Inc.
1170 Howell Mill Rd, Suite 210
Atlanta, GA 30318

MAIN CONTACT:
Stephen Johnston
stephen.johnston@flocksafety.com
(470) 627-5704

flock safety



EXHIBIT A ORDER FORM

Customer: FL - St. Johns County SO
 Legal Entity Name: FL - St. Johns County SO
 Accounts Payable Email: soaccountspayable@sjso.org
 Address: 4015 Lewis Speedway Saint Augustine, Florida 32084

Initial Term: 60 Months
 Renewal Term: 24 Months
 Payment Terms: Net 30
 Billing Frequency: Annual Plan - First Year Invoiced at Signing.
 Retention Period: 365 Days

Hardware and Software Products

Annual recurring amounts over subscription term

Item	Cost	Quantity	Total
Flock Safety Platform			\$391,100.00
Flock Safety Flock OS			
FlockOS™	Included	1	Included
Flock Safety LPR Products			
Flock Safety Falcon ®	Included	132	Included
Flock Safety Falcon ® Flex	Included	5	Included
Flock Safety FlockOS Add Ons			
Flock Safety Advanced Search	\$5,000.00	1	\$5,000.00
Flock Safety Platform Add Ons			
Extended data retention (Up to 1 Year)	\$300.00	137	\$41,100.00

Professional Services and One Time Purchases

Item	Cost	Quantity	Total
One Time Fees			

Subtotal Year 1:	\$391,100.00
Annual Recurring Subtotal:	\$391,100.00
Discounts:	\$342,500.00
Estimated Tax:	\$0.00
Contract Total:	\$1,955,500.00

Taxes shown above are provided as an estimate. Actual taxes are the responsibility of the Customer. This Agreement will automatically renew for successive renewal terms of the greater of one year or the length set forth on the Order Form (each, a "Renewal Term") unless either Party gives the other Party notice of non-renewal at least thirty (30) days prior to the end of the then-current term.

Special Terms

Effective Date of the Contract. The first day of the Term of this Agreement, which shall be 10/01/2023.

Non-Appropriation. Subject to Section 6.4 of the executed Agreement, the awarding or continuation of this Agreement is dependent upon the availability of funding. CUSTOMER'S payment obligations are payable only and solely from funds Appropriated and available for this Agreement. The absence of Appropriated or other lawfully available funds shall render the Agreement null and void to the extent funds are not Appropriated or available and any deliverables delivered but unpaid shall be returned to FLOCK. The CUSTOMER shall provide FLOCK written notice of the failure to make an adequate Appropriation for any fiscal year to pay the amounts due under the Agreement, or the reduction of any Appropriation to an amount insufficient to permit the CUSTOMER to pay its obligations under the Agreement. In the event of non or inadequate appropriation of funds, there will be no penalty nor removal fees.

charged to the CUSTOMER. CUSTOMER agrees to not contract with any other LPR company during the term of this Agreement should funds become available at a later date.

Binding Upon Future Parties. Subject to Section 6.2 of the executed Agreement, in the event a new Sheriff is elected and does not want to maintain services, the agency may terminate this Agreement upon thirty (30) day written notice without penalty

Support Services. If any hardware and/or software is not repaired to fully operational within ten (10) days of notification from CUSTOMER to FLOCK, FLOCK shall be deemed in breach of this Agreement and the Agreement shall be rendered null and void.

Sheriff Term. The Term of the Agreement extends the current Sheriff's term. If a newly elected Sheriff does not agree to extend this Agreement, said CUSTOMER will provide FLOCK a thirty (30) day written notice of cancellation

Change in Florida law. If at any time during this Agreement, the laws prohibit the use of LPR technology in Florida, this Agreement shall immediately be terminated with no penalty to CUSTOMER.

Billing Schedule

Billing Schedule	Amount (USD)
Year 1	
At Contract Signing	\$391,100.00
Annual Recurring after Year 1	\$391,100.00
Contract Total	\$1,955,500.00

*Tax not included

Discounts

Discounts Applied	Amount (USD)
Flock Safety Platform	\$342,500.00
Flock Safety Add-ons	\$0.00
Flock Safety Professional Services	\$0.00

Product and Services Description

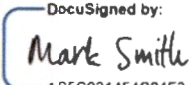
Flock Safety Platform Items	Product Description	Terms
Flock Safety Falcon ®	An infrastructure-free license plate reader camera that utilizes Vehicle Fingerprint® technology to capture vehicular attributes.	The Term shall commence upon first installation and validation of Flock Hardware.
Flock Safety Falcon® Flex	An infrastructure-free, location-flexible license plate reader camera that enables the Customer to self-install.	The Term shall commence upon execution of this Statement of Work.

One-Time Fees	Service Description
Installation on existing infrastructure	One-time Professional Services engagement. Includes site & safety assessment, camera setup & testing, and shipping & handling in accordance with the Flock Safety Advanced Implementation Service Brief.
Professional Services - Standard Implementation Fee	One-time Professional Services engagement. Includes site and safety assessment, camera setup and testing, and shipping and handling in accordance with the Flock Safety Standard Implementation Service Brief.
Professional Services - Advanced Implementation Fee	One-time Professional Services engagement. Includes site & safety assessment, camera setup & testing, and shipping & handling in accordance with the Flock Safety Advanced Implementation Service Brief.

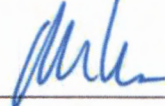
By executing this Order Form, Customer represents and warrants that it has read and agrees all of the terms and conditions contained in the Terms of Service located at <https://www.flocksafety.com/terms-and-conditions>

The Parties have executed this Agreement as of the dates set forth below.

FLOCK GROUP, INC.

By: 
Name: Mark Smith
Title: General Counsel
Date: 9/7/2023

Customer: FL - St. Johns County SO

By: 
Name: Matthew Cline
Title: General Counsel
Date: 09-01-2023
PO Number: _____


Shari Shuman (Sep 15, 2023 08:54 EDT)

Shari Shuman

CFO

Sep 15, 2023

**Flock Safety + FL - St. Johns County
SO**

Flock Group Inc.
1170 Howell Mill Rd, Suite 210
Atlanta, GA 30318

MAIN CONTACT:
Jason Boutselis
jason.boutselis@flocksafety.com
+18139046145

flock safety

**Flock Safety + FL - St. Johns County
SO**

Flock Group Inc.
1170 Howell Mill Rd. Suite 210
Atlanta, GA 30318

MAIN CONTACT:
Jason Boutselis
jason.boutselis@flocksafety.com
+18139046145

flock safety

**Flock Safety + FL - St. Johns County
SO**

Flock Group Inc.
1170 Howell Mill Rd, Suite 210
Atlanta, GA 30318

MAIN CONTACT:
Jake Downs
jake.downs@flocksafety.com
5854146554

Quote Number: Q-158192
Expiration Date: 12/31/2025

flock safety

flock safety

ORDER FORM

This order form ("Order Form") hereby incorporates and includes the terms of the previously executed agreement (the "Terms") which describe and set forth the general legal terms governing the relationship (collectively, the "Agreement"). The Terms contain, among other things, warranty disclaimers, liability limitations and use limitations.

This additional services Agreement will be effective when this Order Form is executed by both Parties (the "Effective Date")

Customer: FL - St. Johns County SO
 Legal Entity Name: FL - St. Johns County SO
 Accounts Payable Email: soaccountspayable@sjso.org
 Address: 4015 Lewis Speedway Saint Augustine,
 Florida 32084

Initial Term: 60 Months
 Renewal Term: 24 Months
 Payment Terms: Net 30
 Billing Frequency: Annual Plan - Invoiced at First Camera Validation.
 Retention Period: 365 Days

Hardware and Software Products

Annual recurring amounts over subscription term

Item	Cost	Quantity	Total
Flock Safety Platform			\$427,050.00
Flock Safety LPR Products			
Flock Safety LPR, fka Falcon	Included	5	Included
Flock Safety LPR, fka Falcon	Included	13	Included
Solar Long-Range LPR, fka Solar Falcon LR	Included	2	Included
Flock Safety LPR Flex, fka Falcon Flex	Included	3	Included
Flock Safety Platform Add Ons			
Extended data retention (Up to 1 Year)	Included	5	Included
Extended data retention (Up to 1 Year)	Included	15	Included
Extended data retention (Up to 1 Year)	Included	3	Included

Professional Services and One Time Purchases

Item	Cost	Quantity	Total
One Time Fees			
Flock Safety Professional Services			
Professional Services - Standard Implementation Fee	\$650.00	5	\$3,250.00
Professional Services - MASH Tested Pole Implementation Fee - Non-Coastal Region	\$1,250.00	13	\$16,250.00
Professional Services - MASH Tested Pole Implementation Fee - Non-Coastal Region	\$275.00	2	\$550.00
		Discounts:	\$1,950.00
		Estimated Tax:	\$0.00
		Total Contract Due At First Camera Validation:	\$427,050.00

Appendix 4

Sheriff's Office Policy 41.35, Automated License Plate Readers

Pages included: complete (7 pages); effective May 8, 2017, amended June 7, 2024

Full document: public records request R042893-082726



ST. JOHNS COUNTY SHERIFF'S OFFICE

ROBERT A. HARDWICK, SHERIFF

License Plate Reader

Policy 41.35

Effective Date: 05/08/2017

Amended Date: 06/07/2024

ACCREDITATION STANDARDS

CALEA: 41.3.9

CFA:

FCAC:

FLA-TAC:

FMJS:

Discussion: The use of License Plate Reader (LPR) systems is consistent with law enforcement's fundamental goal of safeguarding lives and property. The Sheriff has authorized personnel of the St. Johns County Sheriff's Office to utilize LPR systems as designated by this policy. [41.3.9]

DEFINITIONS

Agency – Refers to St. Johns County Sheriff's Office

Alert - An audible and / or visual signal activated upon the read of a license plate by the LPR system that has not been visually verified by the deputy against the photo in the LPR system.

Confirmation (Confirmed Hit) - A hit by the LPR system that has been confirmed as valid and active by the original entering agency through secondary checks.

Hotlist - Data files extracted from the law enforcement databases including FCIC and agency databases, which contain a listing of stolen license plates, stolen vehicles, wanted persons, and other vehicles / persons actively being sought by a law enforcement agency. These data extracts are generally facilitated numerous times per day in an effort to provide current data.

Live Query Transaction - A hit by the LPR system that has been validated as active, but has not been confirmed as valid, by the entering agency.

LPR - License Plate Recognition System or License Plate Reader – is a system of one (1) or more mobile or fixed high-speed cameras combined with computer algorithms to convert images of license plates into computer-readable data.

Tentative Hit - An alert by the LPR system that has been visually verified by the deputy against the LPR hotlist and photo but has not been validated by the deputy or the Communications Center as a live query transaction or confirmed as valid with the original entering agency.



GENERAL

- .1 The availability and use of LPR systems provides opportunities for the enhancement of law enforcement productivity, effectiveness and safety and is consistent with law enforcement's fundamental goals of safeguarding lives and property.
- .2 LPR systems and information gathered will only be utilized for official law enforcement purposes. [41.3.9, c]
- .3 LPRs are computer-based systems which assist the agency in detection, identification, and recovery of stolen vehicles, wanted persons, missing and / or endangered children / adults, and serious and / or violent offenders. LPR data can help law enforcement 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.
- .4 A LPR scans, captures, and compares license plate information to wanted vehicles, vehicles associated with wanted people, crimes, and missing and / or endangered persons. A match to a license plate results in an alert. LPRs can store the digital image of the license plate, the time, date, location of the image capture, and the capturing camera information.
- .5 The agency may, as a separate step and for legitimate law enforcement purposes per the Federal Driver's Privacy Protection Act (DPPA), undertake to identify the owner of a vehicle in the event the LPR system generates an alert, such as running the license plate number through the State's Department of Motor Vehicle (DMV) database.
- .6 The agency shall utilize LPR system hot lists where there is a legitimate and specific law enforcement reason for identifying a vehicle: [41.3.9, a]
 - Associated with an outstanding arrest warrant.
 - Related to missing person investigations
 - Associated with AMBER Alerts
 - Stolen vehicles
 - Reasonably believed to be involved in the commission of a crime
 - 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
 - With expired registrations
 - Registered to persons who are subject to a restraining order / injunction issued by a court or who are subject to any other duly issued order restricting their movements
 - Registered to persons who are of interest in a specific investigation
 - Registered to persons who are on any watch list issued by a State or Federal agency responsible for homeland security when information has been received concerning a specific individual
- .7 The Criminal Investigations Division Director shall assign an LPR Administrator to manage the LPR system. [41.3.9, a, c]
- .8 In case of any technical issues, the Intelligence Unit will serve as the liaison between LPR users and the service provider.



Appendix 5

Sheriff's Office 2026 news release on license plate reader technology

Pages included: complete (1 page)

Full document: public records request R042893-082726; sjso.org



ST. JOHNS COUNTY **SHERIFF'S OFFICE**

ROBERT A. HARDWICK, SHERIFF

4015 LEWIS SPEEDWAY, ST. AUGUSTINE, FL 32084 | 904.824.8304 | www.SJSO.org

License plate reader technology in St. Johns County

The St. Johns County Sheriff's Office is aware of the conversations about License Plate Reader [LPR] technology. We hear the concerns from the community and would like to clarify how the technology is utilized in St. Johns County.

SJSO introduced license plate reader technology in 2017 and currently operates 180 cameras countywide.

SJSO utilizes LPRs as an investigative tool to assist with locating wanted and missing individuals, recover stolen vehicles, and investigate violent crimes. When a vehicle of interest is identified, the license plate number is flagged in the database, and law enforcement is immediately notified if the vehicle is located. LPRs only capture a vehicle and its license plate and do not capture a driver's identity or continuously track where someone travels.

License plate readers are a valuable tool for public safety efforts in St. Johns County, and since 2017, have assisted with:

- Locating 600+ stolen vehicles & 300 stolen tags
- Recovering 164 items of stolen property
- Locating 247 wanted individuals
- Locating 180 missing individuals
- Charging 831 individuals responsible for crimes

"License plate reader technology is an essential tool helping to keep St. Johns County safe. As sheriff, I took an oath to defend the U.S. Constitution and protect our community. We uphold both by using proven technology lawfully and holding our personnel accountable for proper use. Technology-based policing has been proven to save lives and solve crimes efficiently. The technology is too valuable to lose; it's here to stay, Sheriff Robert A. Hardwick said.

SJSO has strict oversight and auditing procedures to prevent the misuse of license plate reader technology. To date, SJSO has not identified any instances of intentional misuse of the system by our personnel.



Appendix 6

County FY2027 Recommended Budget, Sheriff's Office expenditures

Pages included: 1 page, captured Sept. 15, 2026

Full document: [county-st---johns-fl-budget-book.cleargov.com](https://county-st-johns-fl-budget-book.cleargov.com)



St. Johns

Fiscal Year 2027 Recommended Budget

FY2024

FY2025

FY2026

FY2027

- Sheriff: Bailiff
- Sheriff: Corrections
- Sheriff: Law Enforcement

Expenditures by Department ^

Category	FY 2027 Requested	FY 2027 Recommended
Sheriff: Law Enforcement		
Transfer To Officers	-	\$109,234,299
Total Sheriff: Law Enforcement	-	\$109,234,299
Sheriff: Bailiff		
Transfer To Officers	-	\$3,104,169
Total Sheriff: Bailiff	-	\$3,104,169
Sheriff: Corrections		
Contractual Services	\$1,650,000	\$1,650,000
Insurance	\$92,621	\$92,621
Transfer To Officers	-	\$34,936,442
Total Sheriff: Corrections	\$1,742,621	\$36,679,063
Total Expenditures	\$1,742,621	\$149,017,531

Appendix 7

Public records request R042893-082726

Pages included: the request as filed Aug. 27, 2026, and the portal page showing it marked Completed / Full Release with the files provided, captured Sept. 9, 2026

Full document: St. Johns County Sheriff's Office records portal



Public Records Request :: R042893-082726

St. Johns County Sheriff Records Department <sjsr@govqa.us>
To: sterling@patriotcapitalllc.com <sterling@patriotcapitalllc.com>

Thu, Aug 27 at 1:05 PM

Dear Sterling Seizert:

Thank you for contacting the Records Unit of the St. Johns County Sheriff's Office.

We are in receipt of your records request.

Your request, received on August 27, 2026, was given the reference number R042893-082726 for tracking purposes.

Records Requested: I'd like to request the following:

- All current agreements, contracts, statements of work, and renewal documents between SJSO and Flock Safety, including data ownership and data use terms
- The written ALPR use policy adopted pursuant to s. 316.0779, F.S.
- ALPR system audit logs from installation date per work orders to present showing search date, user agency, stated reason, and case number field, in native electronic format (CSV export).
- Records sufficient to show all agencies with access to SJSO ALPR data, and current National Lookup and federal sharing settings
- Records of any subscription to or use of Flock Nova or similar data-integration products
- Pursuant to s. 316.0777(4)(b), F.S., I request all ALPR images, detections, and data relating to license plates XF5GB, 39KWC, and 10EYFL. My name is Sterling Seizert. I am the registered owner of all of these vehicles and the owner of the owner of the 39KWC registered to Pineland Capital LLC. This is verifiable through your records.

Please provide records electronically in native format, and provide a written cost estimate before incurring any fees exceeding \$25. I've provided a photo of my driver's license for proof of identity.

You can expect an email response from our unit representative, as email is our primary means of contact. Response times may vary for requests submitted outside of regular business hours, on weekends, or holidays.

Please review the attached fee schedule.

Background Checks \$10
Crash Reports \$10 & \$2 processing fee
Records Requests Flat fee of \$50 hourly
Digital Forensics Flat fee of \$50 hourly
Body Worn Camera Videos Flat fee of \$50 hourly
Complex Requests 2 hours of work \$125
3 hours of work \$200
4 hours of work \$275

If any of the above factors change your request, you can reply to this email with the modifications you would like to make.

***Individuals requesting body worn camera footage may choose to obtain only the footage involving the responding or arresting deputy if applicable.**

This option reduces the review and redaction time, lowering the overall cost. Anyone submitting a public records request may select this streamlined option if it meets their needs.

Please note that this option may not be applicable in all situations. Video footage availability is subject to internal review and standard statutory regulations.

[Submit a Records Request](#)

[Search by Reference Number](#)

[My Request Center](#)

[Trending Topics](#)

Records Unit

(904) 810-6610

Custodian of Records

Supervisor Bonnie Jimmerson
(904) 209-2214
bjimmerson@sjso.org

FAQs

[See All FAQs](#)

How do I obtain a copy of a traffic crash report?

How can I request a Public Record?

Request Type: Public Records Request

Primary Requester E-Mail / Username: sterling@patriotcapitalllc.com

Reference No: R042893-082726

Status: Full Release

UPLOAD DATE		
Files:	09/09/2026	attachment
	09/09/2026	attachment
	09/09/2026	attachment
	09/09/2026	attachment
	09/09/2026	attachment
	09/03/2026	LPR_Contract.pdf
	09/03/2026	LPR_Implementation_Guide.pdf
	09/03/2026	LPR_SJSO_Policy_41.35.pdf
	09/03/2026	SJSO_LPR_Technology_News_Release_2026.pdf
	08/27/2026	IMG_7076.jpeg

Additional Information

Requester Type:
Law Enforcement



Appendix 8

Florida legislative lobbyist registrations for Flock Safety, 2026

Pages included: principal list page and the registration pages for Korb, Simmons, Burleson, and Coppola (5), captured Sept. 9, 2026

Full document: floridalobbyist.gov

- [Candice D. Ericks](#)

FLIX NORTH AMERICA INC.

- [Shawn Foster](#)
- [Andrew S. Kalel](#)
- [Wallace Gene McGee Jr.](#)

Flock Group Inc. d/b/a Flock Safety

- [Andrea Korb](#)
- [Kameron Simmons](#)

Flock Safety

- [Bradley S. Burleson](#)
- [Courtney F. Coppola](#)

Florida Crystals Corporation

- [Davis Bean](#)
- [Anita Berry](#)
- [Melissa Braude](#)
- [Michael G. Cantens](#)
- [William Travis Cummings](#)
- [David R. Custin](#)
- [Sydney Fowler](#)
- [Jeffrey M. Johnston](#)
- [Earl Jones Jr.](#) (Canceled: 06/17/26)
- [Lee M. Killinger](#)
- [Cody McCloud](#) (Canceled: 07/27/26)
- [Amanda Stewart](#)

Florida Fish & Wildlife Conservation Commission

- [Jessica Crawford](#)



FloridaLobbyist

Registration and Compensation



2026 Legislative Lobbyist Detail

[Back to Search](#)

Andrea Korb

Mailing Address:

c/o 28 Liberty Ship Way
Suite 2815
Sausalito, CA 94965

Phone Number:

[\(415\) 903-2800](tel:(415)903-2800)

Principals:

- Lobbyists registered to lobby the House and Senate will not display any chamber reference.
- Lobbyists registered to lobby one chamber and/or the PSCNC (Public Service Commission Nominating Council) will display the names of the entity(ies) next to their names (e.g., (Senate, PSCNC)) within the principal's information.
- Lobbyists registered to lobby all three legislative entities will display all entity names (e.g., (House, Senate, PSCNC)).

Flock Group Inc. d/b/a Flock Safety

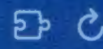
28 Liberty Ship Way
Ste 2815

Sausalito, CA 94965-3321

Industry Code: 561621 Security alarm systems sales combined with installation, repair, or monitoring services

Effective Date: 3/18/2026

[Back to Search](#)



FloridaLobbyist

Registration and Compensation



2026 Legislative Lobbyist Detail

[Back to Search](#)

Kameron Simmons

Mailing Address:

28 Liberty Ship Way Ste 2815
Sausalito, CA 94965-3321

Phone Number:

[\(415\) 903-2800](tel:(415)903-2800)

Principals:

- Lobbyists registered to lobby the House and Senate will not display any chamber reference.
- Lobbyists registered to lobby one chamber and/or the PSCNC (Public Service Commission Nominating Council) will display the names of the entity(ies) next to their names (e.g., (Senate, PSCNC)) within the principal's information.
- Lobbyists registered to lobby all three legislative entities will display all entity names (e.g., (House, Senate, PSCNC)).

Flock Group Inc. d/b/a Flock Safety

28 Liberty Ship Way Ste 2815
Sausalito, CA 94965-3321

Industry Code: 561621 Security alarm systems sales combined with installation, repair, or monitoring services

Effective Date: 1/28/2026

[Back to Search](#)



FloridaLobbyist

Registration and Compensation

2026 Legislative Lobbyist Detail

[Back to Search](#)

Bradley S. Burleson

Mailing Address:

201 East Park Avenue
5th Floor
Tallahassee, FL 32301

Phone Number:

[\(850\) 577-0444](tel:(850)577-0444)

Principals:

- Lobbyists registered to lobby the House and Senate will not display any chamber reference.
- Lobbyists registered to lobby one chamber and/or the PSCNC (Public Service Commission Nominating Council) will display the names of the entity(ies) next to their names (e.g., (Senate, PSCNC)) within the principal's information.
- Lobbyists registered to lobby all three legislative entities will display all entity names (e.g., (House, Senate, PSCNC)).

[Ajax Paving Industries of FL, LLC](#)

One Ajax Drive North
Venice, FL 34275
Industry Code: 237310 Asphalt paving (i.e., highway, road, street, public sidewalk)
Effective Date: 1/6/2026

[American Veterinary Medical Association](#)

1931 North Meacham Road
Suite 100
Schaumburg, IL 60173-4360
Industry Code: 541940 Veterinary services
Effective Date: 1/6/2026



2026 Legislative Lobbyist Detail

[Back to Search](#)

Courtney F Coppola

Mailing Address:

201 East Park Avenue
5th Floor
Tallahassee, Florida 32301

Phone Number:

[850-577-0444](tel:850-577-0444)

Principals:

- Lobbyists registered to lobby the House and Senate will not display any chamber reference.
- Lobbyists registered to lobby one chamber and/or the PSCNC (Public Service Commission Nominating Council) will display the names of the entity(ies) next to their names (e.g., (Senate, PSCNC)) within the principal's information.
- Lobbyists registered to lobby all three legislative entities will display all entity names (e.g., (House, Senate, PSCNC)).

[Access Restoration Services US, Inc.](#)

27657 Commerce Oaks Drive
Conroe, TX 77385
Industry Code: 624230 Disaster relief services
Effective Date: 1/8/2026

[Amazon.com, Inc.](#)

601 New Jersey Avenue
Suite 900
Washington, DC 20001
Industry Code: 454110 Business to Consumer retail sales Internet sites
Effective Date: 1/8/2026

[American Coastal Insurance Company](#)

Appendix 9

Letter of Senator Ron Wyden and Rep. Raja Krishnamoorthi to FTC Chair Ferguson, November 3, 2025

Pages included: complete (2 pages)

Full document: [wyden.senate.gov/imo/media/doc/wyden_letter_to_ftc_on_flockpdf.pdf](https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_ftc_on_flockpdf.pdf)

Congress of the United States

Washington, DC 20515

November 3, 2025

The Honorable Andrew N. Ferguson
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Chair Ferguson:

We write to request that the Federal Trade Commission (FTC) investigate Flock Safety (“Flock”), the license plate surveillance camera company, and, where appropriate, hold the company responsible for its negligent cybersecurity practices. Flock’s surveillance data can reveal Americans’ movements over time, including trips to doctors and therapists, support group meetings for alcohol or drug addiction, as well as places of worship and protests. By not requiring industry-standard multi-factor authentication (MFA) to secure law enforcement accounts, Flock has needlessly exposed Americans’ sensitive personal data captured by the company’s surveillance cameras to theft by hackers and foreign spies, and unauthorized access through multiple documented instances of unauthorized password sharing.

Flock operates the largest network of surveillance cameras in the United States, reportedly contracting with over 5,000 police departments, 1,000 businesses, and numerous homeowners associations across 49 states. When a vehicle passes by a Flock camera, Flock records plate information, vehicle characteristics, and when and where the vehicle was spotted. Flock’s network of surveillance cameras generate and store billions of vehicle scans each month. Flock reportedly enables law enforcement to search through this data not just by plate number, but also by make, model, and even bumper stickers.

In addition to being able to search data generated by cameras their agencies pay for, Flock’s law enforcement customers can also search data collected by other Flock customers’ cameras. Flock customers can allow access by specific law enforcement agencies and can also enroll into the “National Lookup Tool” which allows their data to be searched by all other enrolled Flock customers. Flock informed Congress this August that approximately 75% of Flock’s law enforcement customers have opted into the National Lookup Tool, which is likely due to Flock restricting access to nationwide searches to agencies that have agreed to share their data. But because most law enforcement agency customers have access to this tool, hackers, foreign spies, or anyone else that gains access to a Flock customer account can misuse it to track Americans across the country.

Flock has unnecessarily exposed Americans’ sensitive personal data to theft by hackers and foreign spies. While Flock offers support for MFA, a widely recognized cybersecurity best practice, Flock does not require it, which the company confirmed to Congress in October. Moreover, Flock continues to support insecure methods of MFA, such as sending a numeric code to a phone by text message, which is vulnerable to interception and phishing. Flock does not natively support phishing-resistant MFA, which the Cybersecurity and Infrastructure Security Agency calls “the gold standard method of [MFA].” Phishing-resistant MFA is required of federal agencies and mandated by both the Federal Communications Commission and the FTC

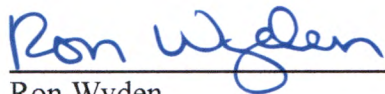
Flock's failure to natively support and require phishing-resistant MFA means that if hackers or foreign spies steal, phish, or otherwise learn a law enforcement officer's Flock password, they can gain access to law-enforcement-only areas of Flock's website and search the billions of photos of Americans' license plates collected by taxpayer-funded cameras across the country. This threat is not theoretical. A search by Congressional staff of a public tool operated by the cybersecurity company Hudson Rock documenting accounts compromised by a form of malware known as an "infostealer" reveals that passwords for at least 35 Flock customer accounts have been stolen. Security researcher Benn Jordan also recently provided our offices with a screenshot from a Russian-language cybercrime forum in which Flock accounts appear to be offered for sale.

By not requiring MFA, Flock has also enabled unauthorized access through law enforcement officers sharing their Flock passwords. If Flock required MFA, law enforcement users of Flock would be required to approve each login to their account from a new computer. On August 11, 2025, Unraveled Press revealed that a Drug Enforcement Administration officer used the Flock account of a local police detective in Palos Heights, Illinois, to conduct several searches. Public records obtained by the press revealed that the detective confirmed that it was a common practice for members of a DEA task force that he was part of to use his login credentials to conduct Flock searches. That numerous federal agents were able to access Flock's systems using passwords belonging to other users without being detected or blocked raises serious questions about the effectiveness of Flock's cybersecurity defenses. A July 9, 2025, memo by the Palos Heights Deputy Chief of Police about the incident, which was released to the press, revealed that the department had not enabled the MFA option until after the password sharing was first identified by a reporter at 404 Media.

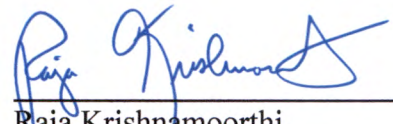
Flock's failure to require MFA is likely an unfair business practice prohibited by Section 5 of the FTC Act. In at least four cases — against Uber, Chegg, Drizly, and Blackbaud — the FTC held that failure to require MFA is an unfair business practice. Flock's negligent cybersecurity practices may also violate state laws related to data protection, consumer privacy or the use of automatic license plate reader (ALPR) systems; for example, California Civil Code § 1798.90.53 requires entities operating ALPR systems to "maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure."

Flock has received vast sums of taxpayer money to build a national surveillance network. But Flock's cavalier attitude towards cybersecurity needlessly exposes Americans to the threat of hackers and foreign spies tapping this data. Accordingly, we urge the FTC to hold Flock accountable for its negligent cybersecurity practices.

Sincerely,



Ron Wyden
United States Senator



Raja Krishnamoorthi
Member of Congress

Appendix 10

Florida Department of Transportation, Engineering and Operations Memorandum 26-01, August 31, 2026

Pages included: complete (1 page)

Full document: [fdot.gov, Engineering and Operations Memorandum index](https://fdot.gov/Engineering-and-Operations/Memorandum-index) (ecom26-01.pdf)



Florida Department of Transportation

RON DESANTIS
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

JARED W. PERDUE, P.E.
SECRETARY

ENGINEERING AND OPERATIONS MEMORANDUM NO. 26-01

DATE: August 31, 2026
TO: Local Agency Permitholders
FROM: Will Watts, P.E., Chief Operating Officer, Assistant Secretary
COPIES: State Agency Officials
Rudy Powell, P.E., Chief Engineer of Operations

SUBJECT: Revocation of General Use Permits for Automated License Plate Readers

The purpose of this memorandum is to notify local law enforcement agencies of updates related to the Florida Department of Transportation's (Department) authority regarding the placement or use of automated license plate recognition systems (LPR) within the right of way of a road on the State Highway System by local agencies.

Automated License Plate Recognition Systems (LPR)

Pursuant to s. 316.0777, Florida Statutes, FDOT is provided with broad authority to approve or deny a local law enforcement agency's request to place a LPR within the right-of-way of a road on the State Highway System—and the authority to remove such at the Department's discretion.

While Florida law limits the issuance of permits for LPR systems to law enforcement agencies, the recent exponential increase in deployments along our roadways, coupled with concerning reports of misuse, data privacy concerns, and surveillance schemes merit immediate action to preserve Floridians' sovereignty and quality of life.

Active Permits

Approvals for the placement of assets in state rights-of-way by the Department are considered temporary in nature. As such, all LPR-related LPR related approvals issued by the Department to a local law enforcement agency are hereby revoked and must be removed by the permittee within 30 days of the date of this memorandum. If such removal has not occurred within the 30-day period, the Department will remove any remaining devices subject to this memorandum.

To that end, nothing in this memorandum prevents or restricts the Department from immediately removing any individual LPR device that is an immediate safety concern or that is causing an unsafe condition.

Discontinuance of All Future LPR Placement Requests

Further, as of the date of this memorandum, the Department will use its discretionary authority to cease the issuance of all future requests for LPR systems within its jurisdictional authority.

Appendix 11

Flock Safety, "Flock Updates Privacy, Accountability, Security, and Transparency Safeguards," Garrett Langley, August 13, 2026

Pages included: pages 1 to 3 of 7 (retention, Evidence Mode, audit, case codes, MFA)

Full document: flocksafety.com/blog/flock-guardrails-address-lpr-privacy-concerns-and-police-transparency



BLOG > LATEST NEWS

Flock Updates Privacy, Accountability, Security, and Transparency Safeguards

Garrett Langley

Flock is cutting default data retention to seven days, making misuse detection mandatory for every customer, and inviting the rest of the industry to meet the same standard.

ELECTED OFFICIALS

LAW ENFORCEMENT

SECURITY UPDATES

TECHNOLOGY

Published: August 13, 2026



Key Points



- Flock is recommending a 7-day ALPR data retention period and introducing Evidence Mode to preserve specific data for active investigations when needed.
- New offense filtering, required Audit Assistance, proactive lockouts, and required case codes will give agencies more control while strengthening oversight of system use.
- Flock is strengthening data security through mandatory multi-factor authentication, an independent security review by Bishop Fox, and a new Coordinated Vulnerability Disclosure program.
- Customers retain ownership and control of their data, while Flock is expanding transparency and reinforcing safeguards around ALPR accuracy, access, sharing, and review.



I want to share several updates on how Flock is further addressing three areas that are critical to the company: strengthening privacy, accountability, and security.

Privacy

When we started Flock 9 years ago, we set the default ALPR retention period to 30 days, unless state or local policy decided on a shorter or longer period. We believed this struck a careful balance between safety and privacy.

Today, we are updating our recommendation and default to a **7-day retention**, and introducing “**Evidence Mode**.” Our analysis shows that over 90% of searches without a full plate are done within a week. Evidence Mode, which will roll out in the coming weeks, addresses the exceptional cases that take longer: detectives can preserve specific ALPR data as evidence for an active investigation in cold storage, consistent with existing laws and policies.

Existing customers will keep their current, democratically approved retention periods. Customers who adopt the 7-day recommendation will receive Evidence Mode at no cost. Every community will continue to choose the retention period that fits its public safety strategy.

We are also introducing **Offense filtering for sharing**. Now, cities can choose which type of offenses are permissible for other agencies to access their cameras. For example, City A could allow City B to search its cameras only for a stolen vehicle, missing person, or violent crime while blocking searches related to immigration enforcement. This gives communities more control over data sharing while preserving collaboration where policies align.



Accountability

Abuse of Flock technology, at any level, is unacceptable. We have strengthened safeguards over the past nine years, from basic audit logs to proactive monitoring. 16 weeks ago, we introduced **Audit Assistance**, which detects abnormal activity and flags it for Administrator review. In recent weeks, those reviews have been associated with arrests of several law enforcement officers who allegedly abused the system. More than one-third of our customers have voluntarily adopted Audit Assistance.

We will now require all law enforcement customers to adopt this feature by the end of this year. In addition, we will institute **proactive lockdown**. When a user's activity meets defined criteria for abnormal behavior, Flock will automatically suspend access pending administrator review. The goal is to intervene before misuse becomes recurring or widespread.

In July 2025, we introduced an optional case code requirement for searches. Results from participating agencies have been promising, so we will now **require case codes** for all law enforcement searches by the end of the year. Agencies may bypass the requirement in emergencies, but every exigent search will be flagged for administrator review.

TRAINING

[41.3.9, c]

- .9 Training on the LPR system will be contracted with the service provider and / or coordinated through the Intelligence Unit.
- Access to the LPR system will only be granted to LPR trained agency personnel.

HOT LISTS

- .11 Designation of hot lists to be utilized by the LPR system shall be made by the Intelligence Unit Sergeant or designee. Hot lists shall be obtained or compiled from sources consistent with the purposes of the LPR system. These sources may include, as available:
- NCIC Stolen Vehicle files
 - NCIC Stolen license plates and Stolen Canadian license plates
 - NCIC Wanted persons
 - NCIC Missing or Endangered person files
 - NCIC Supervised Release (Federal Probationers)
 - NCIC Nationwide Domestic Violence Protection Orders
 - NCIC Violent Gang and Terrorist Organization File
 - NCIC Sexual Offender
 - DHSMV Records of Suspended / Revoked Registrations
 - Agency-generated hot list(s) or manual entries of license plate numbers to existing hot list(s) as may be authorized by the Intelligence Sergeant or designee
- .12 The agency shall regularly monitor agency hot lists utilized by the LPR system to ensure hot lists remain reasonably current.



LOGIN PROCEDURE

- .13 All users will be required to have individual credentials for access and use of the systems and / or data to ensure proper operation and facilitate oversight of the LPR system. Group credentials may be issued to certain groups / individuals on a case-by-case basis.
- .14 The LPR administrator will provide user level access based on the role of the person accessing the system (i.e., criminal investigation or criminal intelligence) to ensure the integrity of the systems and confidentiality of the data. The LPR system shall be sufficiently designed to minimize the compromise, unauthorized access or use, destruction, modification, or inappropriate disclosure of data.
- .15 Each user will be given a unique username and password which shall not be shared with any other person. In addition, no authorized user will allow another person to access the LPR system using the authorized username and password. Exception: users using group credentials as authorized by the Intelligence Unit. [41.3.9, b]

AUDITING AND OVERSIGHT

- .16 All activities (license plate detections, queries, reports, etc.) are automatically recorded by the system for auditing purposes to ensure proper oversight and accountability into the use of the system. Random auditing of the LPR system will be conducted by the LPR Administrator to include all access to data captured, stored, generated or otherwise produced by the LPR to ensure only authorized users are accessing LPR data. In addition, the LPR Administrator or their designee may conduct specific audits of LPR use by any user.
- .17 All investigative queries into collected LPR data are logged by the LPR system according to the user conducting the query. In addition, prior to conducting any search of historical LPR data, users are required to enter an offense, CAD, or case number provided by an outside agency. These logs are available for auditing and review and random audits will be conducted by the LPR Administrator to ensure compliance with this policy. The LPR Administrator may conduct audits or inspections of any feature of the LPR system in order to ensure functionality of the LPR system.
- .18 Annually, the LPR administrator will conduct an evaluation of the LPR program to include measuring LPR program effectiveness, data quality issues and ensure proper planning of future LPR use and deployments.



PROPER AND IMPROPER USE

- .19 The LPR system and all data collected is the property of the agency. Personnel may access and use the LPR system only for official and legitimate law enforcement purposes.
- .20 The following uses of the LPR system are specifically prohibited:
- Invasion of Privacy - Except when done pursuant to a court order - utilizing the LPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).
 - Harassment or Intimidation
 - Personal Use
- .21 Anyone who engages in an improper use of the LPR system or associated scan files or hot lists may be subject to:
- Revocation of access to the LPR system
 - Criminal prosecution
 - Civil liability
 - Administrative sanctions, up to and including suspension or termination

REQUIRED STEPS PRELIMINARY TO LAW ENFORCEMENT ACTION

- .22 The LPR system does not have access to real time data, therefore, an alert alone shall not be a basis for law enforcement action (other than following the vehicle of interest) due to possible errors in the LPR's read of a license plate or hot lists updated data not uploaded in to the agency's system.
- .23 Prior to initiating a stop of a vehicle or other intervention based on an alert, the deputy shall undertake the following:
- Visual verification of license plate number - Deputies shall visually verify that the license plate on the vehicle of interest matches identically with the image of the license plate number captured (read) by the LPR, including both the alphanumeric characters of the license plate and the state of issue, before proceeding with a traffic stop.
 - Confirmation (Confirmed hit) - The deputy must receive confirmation by running the visually verified license plate through the MDC terminal or verifying through teletype the plate is still associated with the alert (i.e. stolen vehicle, amber alert, etc.) Once the license plate number and wanted status is confirmed, a traffic stop of the wanted vehicle can be initiated.
 - Nothing in this policy prevents a deputy from taking law enforcement action on a vehicle if probable cause exists independent of the LPR alert.



RECORDKEEPING

- .25 The Intelligence Unit will support efforts to properly manage LPR system implementation, ensure compliance, enable transparency of operations, enable appropriate auditing review, and help document program benefits realization.

SECURITY / STORAGE AND PRIVACY

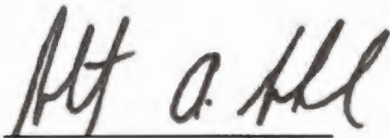
[41.3.9, b]

- .26 The LPR system database and software resides in a Florida Department of Law Enforcement (FDLE) approved server within a secure data center featuring full redundancy and access controls. The data remains property of the agency. [41.3.9, b]
- .27 The LPR data contains no personally identifying information that may be used to connect license plate detection to an individual. It is only with permissible purpose that an investigator may make this connection (verifying with other systems), and this access is already governed by the Federal Driver's Privacy Protection Act (DPPA).
- .28 Public record requests for LPR data shall be considered in accordance with F.S. 316.0777.
- .29 LPR data may be disclosed by or to a criminal justice agency in the performance of the criminal justice agency's official duties.

DATA RETENTION

[41.3.9, d]

- .30 The retention period for all scanned data will be no longer than one (1) anniversary year (pursuant to F.S. 316.0778) unless the data is evidence in a criminal investigation. In this case, the data must be saved to other media and should be submitted as evidence. Unless LPR data has been saved as evidence, all data will be purged, destroyed, or deleted in accordance with F.S. 316.0778. The LPR system will be set up to purge data automatically at the conclusion of the one (1) year period.



Robert A. Hardwick
Sheriff



FLOCK GROUP INC.
ADDITIONAL SERVICES AGREEMENT

This Agreement combined with the existing agreement referenced in Exhibit A describe the relationship between Flock Group Inc. ("Flock") and the customer identified below ("Customer") (each of Flock and Customer, a "Party"). This order form ("Order Form") hereby incorporates and includes the terms of the previously executed agreement (the "Terms") which describe and set forth the general legal terms governing the relationship (collectively, the "Agreement"). The Terms contain, among other things, warranty disclaimers, liability limitations and use limitations.

This additional services Agreement will be effective when this Order Form is executed by both Parties (the "Effective Date").

Agency: FL - St. Johns County SO Legal Entity Name:	Contact Name:
Address: 4015 Lewis Speedway Saint Augustine, Florida 32084	Phone: E-Mail:
Expected Payment Method:	Billing Contact: (if different than above)

Initial Term: 12 months Renewal Term: 12 months	Billing Term: Annual payment due Net 30 per terms and conditions
--	---

Sales tax will be added to all fees as applicable. If your organization is tax exempt, please check this box:
and email your Sales Tax Exemption Certificate to billing@flocksafety.com.

Appendix 12

**WIRED, "Flock Has a Powerful New AI Tool for Police. We Got Its Code,"
Mehrotra and Cameron, August 19, 2026**

Pages included: pages 1 to 4 of 21

Full document: [wired.com/story/flock-safety-os-investigate/](https://www.wired.com/story/flock-safety-os-investigate/)



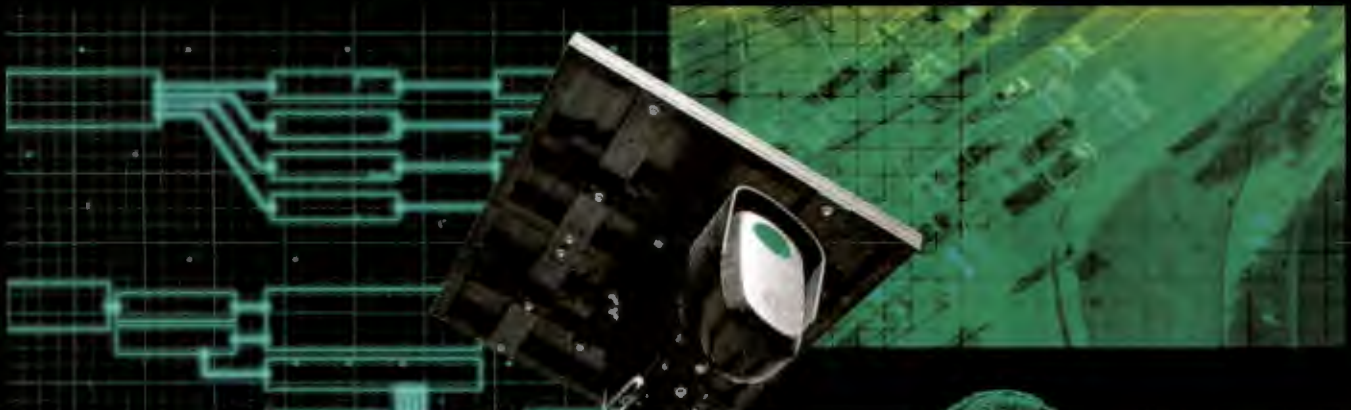
DHUV MEHROTRA

DELL CAMERON

SECURITY AUG 19, 2026 5:00 AM

Flock Has a Powerful New AI Tool for Police. We Got Its Code

Flock's surveillance cameras have already sparked outrage. WIRED reconstructed its next-generation AI system, already in use by some police, to confirm it goes much further than tracking license plates.



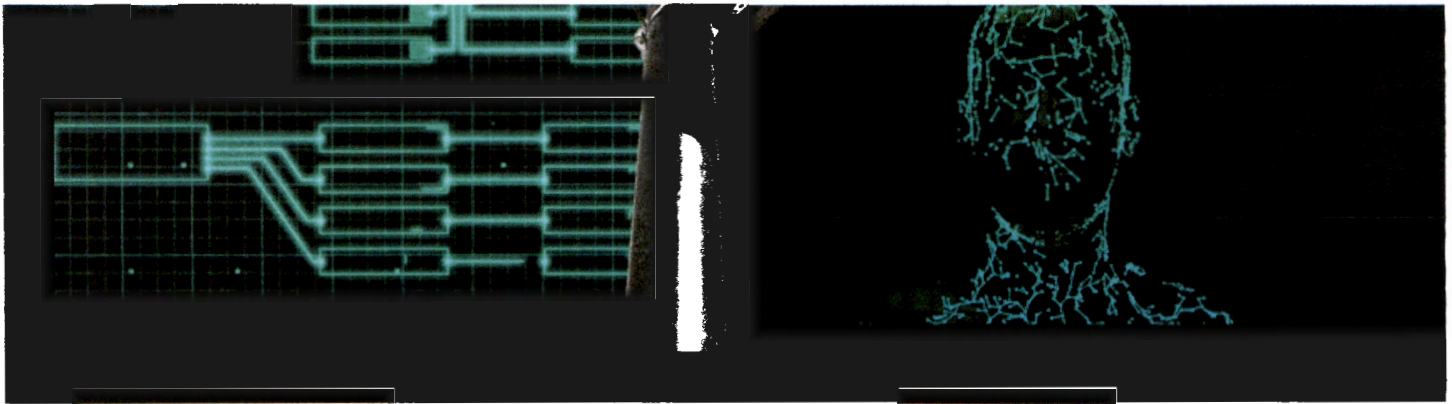


PHOTO-ILLUSTRATION: JOBANNY CABRERA; GETTY IMAGES



SAVE THIS STORY



Listen • 19 minutes

VEHICLE SURVEILLANCE GIANT Flock Safety has told the public for years that its technology “cannot recognize, identify, or track individuals.” It has now built a system that does both, an artificial intelligence tool for police that can identify drivers and track vehicles by their patterns of movement alone, WIRED has learned.

Drawing on a network of cameras that logs the movements of drivers in more than 6,000 communities, the tool can pick out potential witnesses by how often their cars pass through a neighborhood, or surface a driver’s “associates” from the cameras they pass together. Because the system also reaches police case files, 911 dispatch logs, and commercial identity records, those plates can be turned into names, home addresses, and relatives. It can search for people in an area drawn on a map based on nothing more than a physical description.

The software, originally called Nightshift and more recently renamed OS

Investigate, ships with 69 prewritten prompts that officers can select, review, or edit, and then submit to the AI. Officers can also input prompts of their own.

The suggested prompts sit in a cache of more than 450 files that WIRED found on Flock's own website, served by its login pages to anyone who loaded them. The code describes 45 tools at the AI's disposal, giving it access to plate scans and camera metadata, arrest records, case files, dispatch logs, ballistics results, and commercial databases that contain Social Security numbers, dates of birth, phone numbers, email addresses, relatives and associates.

Flock says it is testing the product with a small group of law enforcement partners and describes it as still in development, with capabilities that may not reflect what it eventually sells. It arrives as the company faces bipartisan political pressure, a growing record of officers caught misusing its platform, and a wave of vandalism that has left cameras sawed off and lenses painted over in cities across the country.

Privacy and legal experts say Flock's tools already raise serious constitutional concerns by giving police broad, often warrantless access to a vast record of people's movement. But the prompts WIRED examined go further, turning a tool for finding a known vehicle into one that casts suspicion on drivers based on where and how often they drive, regardless of whether they are wanted for a crime.

Flock built its business on a simple transaction: A camera photographs a passing car, converts the plate to text, and checks it against a list of vehicles

Appendix 13

Chatrie v. United States, No. 25-112 (U.S. June 29, 2026)

Pages included: syllabus, pages 1 to 2 of the slip opinion (72 pages)

Full document: supremecourt.gov/opinions/25pdf/25-112_0am4.pdf

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

CHATRIE *v.* UNITED STATESCERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR
THE FOURTH CIRCUIT

No. 25–112. Argued April 27, 2026—Decided June 29, 2026

On May 20, 2019, a man robbed a credit union in Midlothian, Virginia. Local police officers learned from witness interviews and surveillance footage that the robber had approached the credit union from a corner of an adjacent church while appearing to talk on a cell phone, but they could not find out anything more, and the robber remained at large. On June 14, the police officers applied to a Virginia magistrate for a geofence warrant directed to Google, which would require Google to hand over data about the cell phones located within a 150-meter radius of the credit union—the so-called “geofence”—near the time of the crime. The application described the cell-phone location data Google collects through a service called Location History, which records the location of a user’s cell phone every two minutes or so. The application also explained how that cell-phone location data could help identify the robber, possible accomplices, or additional witnesses. The warrant described a three-step process that the police would follow: at step one, Google would produce anonymized location data for all cell phones within the geofence 30 minutes before to 30 minutes after the robbery; at step two, officers would attempt to narrow the list, and Google would provide additional anonymized data for that narrowed list, consisting of cell-phone locations both inside and outside the geofence during a two-hour period surrounding the robbery; and at step three, officers would further narrow the list, and Google would turn over identifying information, including names and phone numbers, for users on the final list. The magistrate issued the warrant, and through this process, Google ultimately produced three cell-phone users’ identifying information, including petitioner Okello Chatrie, whose location data showed that he entered the geofence about ten minutes before the robbery and headed toward a residential area immediately after leaving

Syllabus

the bank.

Following further police work, a federal grand jury charged Chatrie with robbery and related firearms offenses, and he moved to suppress the information the police obtained from Google. According to Chatrie, the officers had acquired that data through a Fourth Amendment search, and the warrant ostensibly authorizing that search was invalid. The District Court found that the geofence warrant “plainly violates the rights enshrined in [the Fourth] Amendment” but denied the motion based on the good-faith exception to the exclusionary rule. 590 F. Supp. 3d 901, 905, 937–938. A divided panel of the Fourth Circuit affirmed on different reasoning, holding that no search occurred because Chatrie “did not have a reasonable expectation of privacy in two hours’ worth of Location History data voluntarily exposed to Google.” 107 F. 4th 319, 325. The Fourth Circuit granted rehearing en banc and affirmed in a one-sentence *per curiam*, with the court dividing evenly on whether a Fourth Amendment search had occurred. This Court granted certiorari solely on the question whether the police violated the Fourth Amendment in obtaining Chatrie’s location data.

Held: Police officers conducted a Fourth Amendment search when they acquired Chatrie’s location data from Google because an individual has a reasonable expectation of privacy in his cell-phone location information. Pp. 10–33.

(a) The Fourth Amendment protects individuals’ reasonable expectations of privacy, and governmental “intrusion into that private sphere generally qualifies as a search.” *Carpenter v. United States*, 585 U. S. 296, 304. The Amendment’s “basic purpose” is “to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials,” *id.*, at 303, and it was designed “to place obstacles in the way of a too permeating police surveillance,” *United States v. Di Re*, 332 U. S. 581, 595. Pp. 10–29.

(1) In *Carpenter*, this Court held that accessing cell-site location information (CSLI) constitutes a Fourth Amendment search because “individuals have a reasonable expectation of privacy in the whole of their physical movements,” 585 U. S., at 310. The Court reasoned that CSLI provides a “detailed” and “encyclopedic” portrait of a person’s whereabouts, *id.*, at 309, and, with that, “an intimate window into a person’s life,” *id.*, at 311. Because people “compulsively carry” their cell phones “all the time,” the Court explained, a cell phone “tracks nearly exactly the movements of its owner,” and thus “faithfully follows” him not only through “public thoroughfares [but] into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Ibid.* The Court further observed that the “newfound tracking capacity” that CSLI gives the police “runs against everyone”—not just those “under investigation”—and “travel[s] back

Appendix 14

**Leaders of a Beautiful Struggle v. Baltimore Police Department,
2 F.4th 330 (4th Cir. 2021) (en banc)**

Pages included: caption and opening pages 1 to 3 of 76

Full document: ca4.uscourts.gov/opinions/201495A.P.pdf

ON REHEARING EN BANC

PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 20-1495

LEADERS OF A BEAUTIFUL STRUGGLE; ERRICKA BRIDGEFORD; KEVIN JAMES,

Plaintiffs – Appellants,

v.

BALTIMORE POLICE DEPARTMENT; MICHAEL S. HARRISON, in his official capacity
as Baltimore Police Commissioner,

Defendants – Appellees.

NAACP LEGAL DEFENSE & EDUCATION FUND, INC.; CASA DE MARYLAND, INC.;
RABBI DANIEL COTZIN BURG; CITIZENS POLICING PROJECT; EQUITY MATTERS;
REVEREND GREY MAGGIANO; ELECTRONIC FRONTIER FOUNDATION;
BRENNAN CENTER FOR JUSTICE; ELECTRONIC PRIVACY INFORMATION
CENTER; FREEDOMWORKS FOUNDATION; NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS; RUTHERFORD INSTITUTE; POLICING PROJECT;
CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW,

Amici Supporting Rehearing Petition.

Appeal from the United States District Court for the District of Maryland, at Baltimore.
Richard D. Bennett, District Judge. (1:20-cv-00929-RDB)

Argued: March 8, 2021

Decided: June 24, 2021

Before GREGORY, Chief Judge, WILKINSON, NIEMEYER, MOTZ, KING, AGEE,
KEENAN, WYNN, DIAZ, FLOYD, THACKER, HARRIS, RICHARDSON,
QUATTLEBAUM, and RUSHING, Circuit Judges.

Reversed and remanded by published opinion. Chief Judge Gregory wrote the opinion, in which Judge Motz, Judge King, Judge Keenan, Judge Wynn, Judge Floyd, Judge Thacker, and Judge Harris joined. Chief Judge Gregory wrote a concurring opinion, in which Judge Wynn, Judge Thacker, and Judge Harris joined. Judge Wynn wrote a concurring opinion, in which Judge Motz, Judge Thacker and Judge Harris joined. Judge Wilkinson wrote a dissenting opinion, in which Judge Niemeyer, Judge Agee, and Judge Quattlebaum joined, in which Judge Diaz joined Part I, Judge Richardson joined Parts I, II, and III, and Judge Rushing joined Parts I and II. Judge Niemeyer wrote a dissenting opinion. Judge Diaz wrote a dissenting opinion.

ARGUED: Brett Max Kaufman, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, for Appellants. Andre M. Davis, Baltimore, Maryland, for Appellees. **ON BRIEF:** David R. Rocah, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND, Baltimore, Maryland; Ashley Gorski, Alexia Ramirez, Nathan Freed Wessler, Ben Wizner, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, for Appellants. Dana M. Moore, Acting City Solicitor, Elisabeth S. Walden, Chief Legal Counsel, Kara K. Lynch, Chief Solicitor, Police Legal Affairs Practice Group, Rachel Simmons, Co-Director, Michael Redmond, Co-Director, Appellant Practice Group, BALTIMORE CITY DEPARTMENT OF LAW, Baltimore, Maryland, for Appellees. Sherrilyn A. Ifill, President and Director-Counsel, Samuel Spital, Kevin E. Jason, New York, New York, Christopher Kemmitt, Mahogane Reed, NAACP LEGAL DEFENSE & EDUCATIONAL FUND, INC., Washington, D.C., for Amicus NAACP Legal Defense & Educational Fund, Inc. Rachel Levinson-Waldman, Laura Hecht-Felella, BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW, Washington, D.C.; Elizabeth Franklin-Best, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, ELIZABETH FRANKLIN-BEST, P.C., Columbia, South Carolina; John W. Whitehead, Douglas R. McKusick, RUTHERFORD INSTITUTE, Charlottesville, Virginia; Sophia Cope, Mark Rumold, Adam Schwartz, Saira Hussain, Hannah Zhao, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amici Electronic Frontier Foundation, Brennan Center for Justice, Electronic Privacy Information Center, Freedomworks Foundation, National Association of Criminal Defense Lawyers, and Rutherford Institute. Laura Moy, Michael Rosenbloom, Communications & Technology Law Clinic, GEORGETOWN LAW, Washington, D.C., for Amicus Center on Privacy & Technology at Georgetown Law. Barry Friedman, Farhang Heydari, Max Isaacs, POLICING PROJECT AT NEW YORK UNIVERSITY SCHOOL OF LAW, New York, New York, for Amicus The Policing Project.

GREGORY, Chief Judge:

The Plaintiffs—a group of grassroots community advocates in Baltimore—moved to enjoin implementation of the Aerial Investigation Research (“AIR”) program, a first-of-its-kind aerial surveillance program operated by the Defendants—the Baltimore Police Department (“BPD”) and Commissioner Michael Harrison.

While appeal was pending, the program completed its pilot run and Baltimore City leadership decided not to renew its operation. Defendants deleted the bulk of the AIR data, only retaining materials that relate to specific investigations. Defendants then moved to dismiss this appeal as moot. Because Plaintiffs also sought to enjoin Defendants’ access to any data collected by the AIR program, and Defendants retain the data that proved fruitful, we hold that the appeal is not moot.

On the merits, because the AIR program enables police to deduce from the whole of individuals’ movements, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment. Therefore, we reverse and remand.

I.

“Any Fourth Amendment analysis . . . must be grounded on an accurate understanding of the facts.” *United States v. Curry*, 965 F.3d 313, 316 (4th Cir. 2020). In this case, reaching such an understanding has been controversial. We present the facts in detail, given their high degree of relevance. *See generally Leaders of a Beautiful Struggle v. Balt. Police Dep’t*, 456 F. Supp. 3d 699, 703–06 (D. Md. 2020).

Appendix 15

Chief Financial Officer press release, October 21, 2025, listing the \$1,000,000 award to the Sheriff's Office

Pages included: pages 1 to 2 of 4 (award list and Sheriff Hardwick's statement)

Full document: myfloridacfo.com

News



FLORIDA DEPARTMENT OF FINANCIAL SERVICES **CHIEF FINANCIAL OFFICER RUNDOWN**

[Home](#) | [Past Issues](#) | [Current Issue](#) | [Subscribe](#)

Chief Financial Officer Blaise Ingoglia Awards Over \$1.8 Million to Local Law Enforcement Agencies to Combat Illegal Immigration

10/21/2025

ST. AUGUSTINE, Fla.- Today, Chief Financial Officer (CFO) Blaise Ingoglia awarded over \$1.8 million through the State Board of Immigration Enforcement to local law enforcement agencies to support their efforts in combating illegal immigration. These agencies include the Bradford County Sheriff's Office, Jacksonville Sheriff's Office, St. Johns County Sheriff's Office, Clay County Sheriff's Office, and Putnam County Sheriff's Office.

Chief Financial Officer Blaise Ingoglia said, "Under the failed Biden administration, the detrimental impacts of illegal immigration plagued the nation, but President Trump has made it his mission to rectify these wrongs. By supporting our law enforcement and ensuring they have the resources they need to assist in immigration enforcement efforts, we are further securing our state from criminal illegal aliens. I am thankful for the

efforts of President Donald Trump and Governor Ron DeSantis in securing our border and protecting the citizens of our great state.”

St. Johns County Sheriff Robert Hardwick said, “The money awarded to us by the State Board of Immigration is an investment in the safety and protection of our community. I am grateful for CFO Ingoglia’s support, and his dedication to making sure our law enforcement officers have the resources they need to make St. Johns County and the State of Florida the best place in the nation to live, work, play, raise a family and retire.”

Jacksonville Sheriff T.K. Waters said, “Criminal illegal aliens have no business in our great state of Florida. The Jacksonville Sheriff’s Office is thankful for the CFO’s ongoing commitment to illegal immigration enforcement and keeping Florida safe.”

Clay County Sheriff Michelle Cook said, “Because of CFO Ingoglia’s hard work, we have received the necessary funding for our agency to protect the residents of Clay County. Illegal immigration is a pressing issue in our state and country, this money will be used to strengthen our law enforcement so they can respond quickly and effectively.”

Bradford County Sheriff Gordon Smith said, “In Bradford County, public safety is our top priority and this funding for immigration enforcement ensures that our officers have the capability to assist immigration officials as effectively as possible. I want to thank CFO Ingoglia for prioritizing the needs of law enforcement agencies so we can do our jobs safely and successfully.”

Putnam County Sheriff H.D. “Gator” Deloach said, “With the support of CFO Ingoglia and the State Board of Immigration Enforcement, our officers are better equipped to protect our state from the detrimental impacts of illegal immigration. Through the money awarded today we are keeping Florida safe and secure.”

Funding is made available through the State Board of Immigration Enforcement for local law enforcement agencies that have applied for reimbursement of immigration enforcement. Bonuses awarded to law enforcement are provided through the 287 (g) agreement of the Immigration and Nationality Act. This agreement allows for state and local