OTTAWA COUNTY SHERIFF'S OFFICE

Flock Automated License Plate Reader (ALPR) Program

A Report to the Ottawa County Board of Commissioners

Prepared for the Board of Commissioners Work Session

Submitted by Sheriff Eric J. DeBoer

September 18, 2026

Table of Contents

Table of Contents 2
I. Executive Summary 4
II. Program History and Governance 4
III. Program Overview 5
IV. What the System Captures and What It Does Not 5
V. Data Retention and Storage 6
VI. Access, Search Standards, and Oversight 6
Who can search, and under what standard 6
Warrant requirement 7
What a search actually shows 7
OS Investigate / FreeForm AI search 7
Audits and findings 7
Personal misuse: the national pattern and OCSO's safeguards 7
VII. Alerts, Hotlists, and False Positives 8
VIII. Constitutional Analysis: The Fourth Amendment and ALPR Technology 9
The foundational framework 9
Cases directly addressing ALPR 9
Chatrie v. United States: an important, but distinguishable, decision 9
Other legal considerations 10
IX. Data Sharing: Current Practice, National Context, and the Case for Continued Sharing 10
Current practice 10
The national context 10
OCSO's own posture 11
The case for continued, and eventually expanded, sharing 11
X. Steps Taken to Strengthen Data Protection 12
XI. On Cost-Benefit and Civil-Liberties Analysis 12
XII. Program Outcomes 13
XIII. Case Studies 13
Simon Andrew VanDyke 13
Lance Allen Holland and Ceandra Jackson 14
Andrew Louis Harper 14
Missing/Endangered Juveniles, May 2025 14
XIV. Conclusion and Recommendations 14
Appendix A: OCSO ALPR Policy 15
424.1 Purpose and Scope 15

424.2 Policy 15
424.3 Administration 15
424.4 Operations 15
424.5 Data Collection and Retention 16
424.6 Accountability 16
424.7 Releasing ALPR Data 17
424.8 ALPR Network Data Sharing 17
Appendix B: Case Law Quick Reference 17
Appendix C: ALPR Fourth Amendment Case Compendium 18

I. Executive Summary

The Ottawa County Sheriff's Office (OCSO) operates a network of Automated License Plate Reader (ALPR) cameras under a Master Service Agreement with Flock Safety, Inc., approved by the Ottawa County Board of Commissioners on April 8, 2024 (Contract #2242). This report is prepared to inform the Board's work session on the program, covering its history, current operation, data protections, constitutional footing, and the case for continued interagency data sharing.

In brief: OCSO's ALPR program is a limited, fixed-point camera system that photographs the rear of passing vehicles on public roadways, records a plate number and a small set of vehicle characteristics, and retains that data for 30 days before automatic deletion. It does not capture faces, audio, or continuous video, and it cannot track a vehicle's movement in real time or predict where a vehicle will go next. Access is restricted to trained, credentialed personnel, every search requires a documented case-related reason, and all access is logged and periodically audited. Since program inception, OCSO's audits have identified no violations involving data misuse.

The report also addresses the program's constitutional footing, the national controversy surrounding license-plate-reader data sharing with federal agencies, the steps OCSO has taken, including in direct response to that national conversation, to tighten control over its data, and the case for continuing to share appropriately controlled data with other lawful agencies. Section XII presents the program's full outcomes log, verified against the department's case-tracking data, and Appendix A includes OCSO's formal ALPR policy in full.

II. Program History and Governance

Ottawa County's ALPR program began under then-Sheriff Steve Kempker, who signed the Master Service Agreement with Flock Safety on March 26, 2024. The Board of Commissioners ratified that agreement on April 8, 2024, under Contract #2242. The contract's term began at Board approval; its initial two-year term has since passed and renewed automatically, consistent with the agreement's standard renewal provisions.

The program was not grant-funded. From the outset it has been paid for by the County, with additional cameras added through pass-through arrangements in which participating townships reimburse the County for their share of the cost under the County's existing Flock contract.

Data sharing with other agencies, discussed in detail in Section IX, was part of the program's design from its inception in April 2024. Sheriff DeBoer was not part of OCSO's executive team at that time; based on his understanding, sharing was described as a feature of the system when it was adopted. OCSO has not located Board meeting minutes from that period that would confirm exactly what was presented to or discussed by the Board. What can be said with confidence from OCSO's own records is that the scope of sharing has not changed through any OCSO policy decision since ratification: its growth since then reflects the ordinary addition of new participating agencies and individual sharing requests, not a change in program design.

This work session was prompted by public comment at the Board's August 25, 2026 meeting, after which Commissioner Moss proposed a dedicated session on the program. The Sheriff's Office welcomes this discussion: this process has already produced a more deliberate operation and several concrete changes, discussed throughout this report.

III. Program Overview

OCSO currently operates 31 fixed and mobile ALPR cameras countywide: 15 cameras funded directly by the County, 2 mobile units, and 14 cameras added under pass-through arrangements with individual municipalities, which reimburse the County for their share of the cost.

A note on the camera-count discrepancy: commissioners' questions referenced figures of 29 and 36 cameras. Both stem from the same source of confusion. Newer Flock camera installations include two physical devices at each location: the camera itself, and a separate mechanism that reduces battery/solar draw. An earlier device count included both components as if each were a separate camera, producing an inflated figure. The correct, current count of operational ALPR cameras is 31.

Cost: the County's direct annual cost for its 15 county-funded cameras is $45,000 ($3,000 per camera per year). The 14 cameras added for participating municipalities are billed to and reimbursed by the contracting township under the same pass-through arrangement, rather than funded separately by the County. No additional Flock cameras are budgeted for FY2027.

A related disclosure, offered proactively: OCSO has no plans to add additional Flock cameras. However, OCSO is separately evaluating a records management system (RMS) replacement, and the most cost-effective vendor bundle under consideration includes a number of fixed license-plate-reader cameras from that RMS vendor, a different company than Flock. No decision on that RMS project has been made, and adopting it would not expand the Flock program described in this report; it would introduce a separate camera system from a separate vendor, which would need to be evaluated on its own terms, including its own data, retention, and sharing practices, rather than assumed to carry the same protections described here. The Sheriff is flagging this now, before it is finalized, rather than have the Board or the public learn of it later and reasonably ask why it wasn't mentioned.

All ALPR camera data, including data from the 14 cameras added for participating municipalities, is owned by Ottawa County. The municipal cameras are added through pass-through contracts administered under the County's own Flock agreement, with the participating municipality reimbursing the County for its share of the cost, rather than through a separate contract or separate data ownership. Data is stored by Flock separately from other agencies' data and shared only with agencies OCSO selects.

A note on scope: OCSO patrol vehicles are separately equipped with their own in-car camera license plate reading software. That system is distinct from Flock, runs on different software, and is not addressed in detail in this report because it is not part of the Flock program the Board is being briefed on. The two systems are not integrated in both directions: plate reads captured by the in-car system are uploaded to Flock but captured separately in the system. The reads made by in-car cameras are not available to be shared with or searched by outside agencies. They are only searchable by our agency.

IV. What the System Captures and What It Does Not

Each camera "read" records: the plate number, the plate's state of registration, date and time, GPS location of the camera, and a set of vehicle characteristics (make, model, color, and distinguishing features such as bumper stickers or roof racks). Every passing vehicle generates a read, regardless of whether it triggers an alert.

- No facial recognition capability exists on OCSO's devices.
- No audio recording capability exists.

- No live video feed. The system captures still images at the moment of passage, not continuous video.
- No speed enforcement function.
- Cameras are rear-facing. Michigan does not require a front license plate, and OCSO's cameras are not positioned to photograph drivers or occupants.

V. Data Retention and Storage

Flock retains OCSO ALPR data on a 30-day rolling basis, with automatic deletion after 30 days. Data connected to an active investigation is transferred into the department's digital evidence system (Evidence.com) and retained under standard evidence-retention procedures from that point forward, not the 30-day ALPR window.

Thirty days was chosen deliberately, to balance investigative utility against data minimization. Many investigative leads develop more than a week after an incident, particularly in multi-jurisdictional cases; a shorter window measured in days would foreclose those leads before they are discovered. Flock has recently changed the retention period it sets as a default for new customers to a shorter window; that change affects Flock's default setting, not its underlying recommendation, and OCSO's 30-day policy has not changed.

Data storage is hosted on Flock's Amazon Web Services GovCloud environment, a distributed, redundant cloud infrastructure built to federal government security requirements. Regardless of the underlying infrastructure, the data itself remains OCSO's property and is deleted from Flock's system on the 30-day cycle described above.

OCSO's Master Services Agreement with Flock confirms this ownership directly: it states that all right, title, and interest in Customer Data, defined to include the Footage captured by the cameras, belongs to and is retained solely by OCSO, and that Flock does not own and may not sell that data. Flock is granted only a limited license to use the data to provide the service.

On contract termination: the contract does not include a separate data-purge clause specific to camera footage, because it does not need one. The same rolling 30-day automatic deletion described above runs continuously regardless of the contract's status, so any data older than 30 days is already gone by the time a termination could take effect. For anything captured in the final 30 days before termination, the contract's confidentiality provision independently requires that all of OCSO's proprietary information, defined in the agreement to include the geolocation data collected through the cameras, be returned, destroyed, or erased upon termination, along with any copies. In practice, that means OCSO does not need to rely on Flock's discretion to get its data back or deleted: the ownership and confidentiality terms in the contract already require it.

Data that OCSO lawfully shares with another agency becomes part of that agency's own records at that point, and is thereafter governed by that agency's own retention policy, not OCSO's.

VI. Access, Search Standards, and Oversight

Who can search, and under what standard

Access is limited to trained personnel who hold LEIN (Law Enforcement Information Network) certification and who search under their own individual, audited credentials; there are no shared or generic logins. Every search requires a documented, legitimate law enforcement purpose, and the

platform requires a case number, CAD number, or offense type as a mandatory field before a search can be run.

Warrant requirement

No warrant is required to access OCSO's ALPR data under current department practice. As discussed in Section VIII, OCSO's position is that its camera data is a lawfully captured record of what occurred in public view, not the kind of comprehensive third-party digital record that triggered the warrant requirements in Carpenter or Chatrie. Practically, this is also enforced by the retention design itself: data purges automatically as the 30-day window expires, and there is no mechanism to hold data past that window in anticipation of a future warrant except through the standard evidence-transfer process described in Section V, which applies once a case is already under active investigation.

What a search actually shows

Investigators can search by plate number, camera location, date range, or vehicle description alone. Each read is an independent, fixed-point capture of a vehicle passing a specific camera at a specific moment. It is not continuous tracking. The system can show where and when a vehicle was seen at OCSO's camera locations; it cannot show what happened between those points, and there is no live or predictive tracking capability. This is a meaningful practical limitation: even a vehicle observed at multiple camera locations over the course of a day yields a series of discrete data points, not a continuous account of the vehicle's movement, and substantial gaps remain wherever a vehicle travels outside camera coverage.

OS Investigate / FreeForm AI search

OCSO does not use, and its current contract with Flock does not include, the OS Investigate or FreeForm natural-language search capability. Search remains limited to the structured fields described above (plate number, camera location, date range, and vehicle description) rather than an open-ended AI query across the full dataset. This is not a dormant feature waiting to be switched on: activating it would require negotiating a change to OCSO's existing contract, not an administrative decision within the current agreement.

Audits and findings

Approximately 20 audits have been conducted since the program's inception. No violations involving data misuse have been identified in any of those audits. The audits did identify instances of incomplete search-form documentation: officers running searches without fully completing the optional narrative fields. This was a training issue, not a misuse issue: the underlying case or offense-type field, which is mandatory, was always present. It has since been resolved through additional training and a platform update that made the relevant fields mandatory rather than optional.

No enforcement action is ever taken on the basis of a Flock alert alone. Before any stop, deputies are required to independently verify the LEIN/NCIC record, visually confirm the plate and vehicle, and establish independent legal justification for the stop. This layered-verification requirement is discussed further in Section VII, in the context of a national conversation about false-positive stops.

Personal misuse: the national pattern and OCSO's safeguards

A separate national concern, distinct from the federal-access issue discussed in Section IX, is individual officers misusing ALPR systems for personal rather than investigative purposes, most commonly to track a current or former romantic partner. This has become one of the most serious documented problems with license-plate-reader systems nationally. A Washington Post investigation, reviewing

police and court records, identified at least 50 law enforcement officers nationwide accused, charged, or convicted of misusing license-plate-reader systems for unauthorized personal purposes; Flock's system was involved in 46 of those cases, and in 26 of them the target was a wife, girlfriend, ex-partner, an ex-partner's new partner, or a woman the officer wanted to meet. The Institute for Justice, which maintains a public database of ALPR misuse, has documented more than 100 incidents nationally, including cases of officers running the same plate dozens or hundreds of times over several months. On August 25, 2026, a nationwide class-action lawsuit, Schulte v. Flock Group Inc., was filed in Georgia alleging that Flock knew its system carried a recurring risk of this kind of abuse and failed to build in adequate safeguards against it.

Reporting on these cases has identified a common pattern worth naming directly: officers entering a false or generic reason to get past a mandatory-justification field, then running the same plate repeatedly, often while off duty. That pattern is a real limitation on any system, including OCSO's, that relies on a self-reported reason at the point of search. A mandatory field raises the bar over having no barrier at all, but it does not by itself stop someone determined to enter false information; the real defense against that pattern is what happens after the search, not the field itself.

OCSO's safeguards here are the same access and audit controls described earlier in this section, applied to this specific risk: every search is tied to an individual, non-shared, audited credential rather than a generic login, so every search is attributable to a specific deputy by name; the recent platform updates includes a built-in analytics and audit tool that gives administrators visibility into user-level and network-level search history, plate-read reports, and event logs, the same kind of tool that, in other jurisdictions, surfaced misuse once someone finally looked; and OCSO has conducted approximately 20 audits since the program's inception, none of which has identified a violation involving data misuse.

In direct response to this national pattern, OCSO has activated Flock's newer audit assistance capability, which automatically flags certain search activity, such as unusual search volume or patterns concentrated on a small number of plates, for closer review by administration, rather than relying solely on a manual, after-the-fact audit to catch it. This moves part of the safeguard from periodic review to ongoing, automated screening, a meaningfully different posture than most of the departments in the national reporting had in place when their misuse cases came to light.

The Sheriff has also stated two positions the Board should be aware of. First, he supports state legislation that would classify ALPR data as CJIS-protected information, the same category of legal protection that already governs other criminal justice information systems, which would attach specific legal penalties to misuse rather than leaving discipline solely to individual department policy. Second, independent of whether such legislation is ever adopted, the Sheriff has stated his willingness to discipline any OCSO employee found to have misused the system under current policy, now, without waiting for a new law to require it.

VII. Alerts, Hotlists, and False Positives

Every plate read is checked automatically against the National Crime Information Center (NCIC) database and against Flock "hotlists," lists of specific plates flagged by individual police agencies, typically in connection with a specific investigation. A hit is broadcast to system users within a selected proximity of the camera that generated it. Plates are not run against the Michigan Secretary of State database as part of this process, and the registered owner of a vehicle is not identified within the Flock system itself.

On the national reports of officers stopping the wrong vehicle based on a Flock hit: this is a real phenomenon, but it is not a defect specific to Flock or to ALPR technology. Ottawa County's own patrol deputies already receive comparable alerts every day from LEIN/NCIC when running a plate manually

on their mobile computers, including occasional hits generated by a mistyped plate or a plate matching a wanted vehicle registered in a different state. NCIC is built to tolerate that kind of data-entry error deliberately, so that an officer is not penalized or placed at a disadvantage for running a plate that turns out to have been mis-keyed elsewhere in the system. What NCIC and Flock alerts have in common is that a hit is a lead, not a conclusion: it is the receiving officer's responsibility, in every case, to confirm all available information before taking any enforcement action. The national incidents that have drawn attention typically involve a breakdown in that verification step, poor police work, rather than a flaw in the underlying alert technology. OCSO's own layered-verification requirement, described in Section VI, exists precisely to prevent that breakdown.

VIII. Constitutional Analysis: The Fourth Amendment and ALPR Technology

This is an actively developing area of constitutional law. There is not yet a single controlling U.S. Supreme Court decision specific to fixed ALPR cameras, but the weight of authority to date, at both the federal and state level, supports OCSO's practice. This section summarizes that authority; Appendix B lists foundational case citations, and Appendix C is an extensive national compendium of ALPR-specific decisions.

The foundational framework

Courts analyzing ALPR technology generally start from Katz v. United States (1967) and United States v. Knotts (1983), which hold that a person has no reasonable expectation of privacy in what is knowingly exposed to public view, including the fact of one's movements on public roads. United States v. Jones (2012) and Carpenter v. United States (2018) mark the outer edge of that doctrine — Jones addressed physical GPS attachment, and Carpenter addressed a warrant requirement for seven or more days of comprehensive third-party cell-site location data — but neither squarely governs a stationary camera photographing a vehicle's exterior in public view. Kyllo v. United States (2001), addressing sense-enhancing technology aimed at a private home, has informed OCSO's own internal line: the Sheriff's Office has avoided technology, such as passive RFID scanning, that would let it see information not visible to the naked eye. Full citations appear in Appendix B.

Cases directly addressing ALPR

Courts that have addressed ALPR technology directly, including Commonwealth v. McCarthy (Mass. 2020), State v. Simonson (Wash. Ct. App. 2026), and the currently pending Schmidt v. City of Norfolk (E.D. Va. 2026, on appeal to the Fourth Circuit), have consistently held that limited, fixed-point ALPR use of the kind OCSO operates does not constitute a Fourth Amendment search. Appendix C compiles an extensive national survey of these and dozens of additional federal and state decisions reaching the same conclusion.

Chatrie v. United States: an important, but distinguishable, decision

On June 29, 2026, the U.S. Supreme Court held in Chatrie v. United States, 609 U.S. ___ (2026), that a cell-phone geofence warrant compelling Google to disclose comprehensive Location History data was a Fourth Amendment search. Chatrie is a cell-phone geofence case, not an ALPR case: it addresses continuous, automatically transmitted digital location data, a fundamentally different and more comprehensive record than a momentary photograph of a vehicle's exterior on a public road. Stationary ALPR cameras trace their legal lineage to Knotts rather than to the third-party-doctrine cases Chatrie extends, and OCSO's program — 31 cameras, a 30-day retention window, and no live or

predictive tracking — sits well within the range of programs courts have upheld to date. This remains genuinely developing law, and OCSO will continue to monitor it.

Other legal considerations

First Amendment: OCSO's mandatory, case-linked search-authorization requirement is the primary safeguard against using the program to target protected First Amendment activity, such as attendance at a protest or house of worship. There is no way to search the system for who was present at a location without a documented, case-linked purpose.

Public records (FOIA): OCSO currently denies FOIA requests for ALPR read data, search records, and audit logs, on the position that this data, while owned by the County, is not in the County's physical possession because it resides on Flock's platform. That position is not legally settled: a pending Michigan lawsuit, Tewolde v. Genesee County (filed August 2026), challenges the same reasoning at another Michigan agency, and its outcome could affect OCSO's practice.

Emergency powers: neither OCSO's contract nor its internal policy expands ALPR search authority during a declared emergency or curfew; the same documented, case-linked purpose requirement always applies.

Pending Michigan legislation: House Bills 5492 and 5493 would create a new statutory framework for ALPR use, and several of their prospective requirements already reflect OCSO's practice. As written, the Sheriff and the Michigan Sheriffs' Association do not support the bills, though the Sheriff supports separate legislation that would classify ALPR data as CJIS-protected, as discussed in Section VI.

IX. Data Sharing: Current Practice, National Context, and the Case for Continued Sharing

Current practice

As of September 11, 2026, Flock delivered a platform update giving OCSO the ability to control, case type by case type, which categories of case an external agency may search when accessing OCSO's shared data, rather than only an all-or-nothing sharing toggle. The Sheriff's Office has configured those permissions, and is renewing nationwide and out-of-state sharing consistent with the framework already authorized in OCSO's formal ALPR policy (Appendix A). We had previously suspended out of state sharing when we realized that we could not control which crime types could be entered as justification for a search from external agencies. What this update delivered is the ability to control every case type, which is what let OCSO move from an all-or-nothing external sharing decision to a case-type-by-case-type one, addressing the vague or overly broad search-reason concern previously held by the OCSO.

OCSO's ALPR data currently is shared with approximately 175 agencies within Michigan, and nationwide and out-of-state sharing is being renewed under the newly configured case-type controls. Michigan agencies continue to receive automated acceptance of sharing requests under the department's policy; federal agencies remain excluded from that automated acceptance, consistent with Appendix A.

The national context

The Board should be aware that ALPR data sharing, and Flock's national sharing network specifically, has become a significant national controversy over the past year. Public-records requests in multiple states, most notably a Freedom of Information Act disclosure from Danville, Illinois, documented more

than 4,000 searches of shared ALPR networks nationwide, run by local and state police, for stated reasons including immigration enforcement, despite state laws in some jurisdictions (including Illinois) that prohibit exactly that use. Audits by other cities identified similar problems, including agencies that had gained access to shared networks without the host agency's knowledge, and at least one documented case in which a federal analyst improperly accessed a local Flock system. These findings led dozens of cities and counties nationally to cancel their Flock contracts over the course of 2025 and 2026, and led Illinois to remove 47 agencies from its shared network entirely.

Flock's own response to this controversy directly affects what protections are now available to OCSO's data even though OCSO was not implicated in any of the reported misuse: federal agencies were removed from Flock's national search network in August 2025; a mandatory, standardized offense-type field was added to every search platform-wide in December 2025, improving audit precision; sensitive fields in network audit exports were masked to protect officer safety and active investigations; and in January 2026, Flock introduced a single administrative "Federal Sharing" toggle that lets any agency immediately cut off all federal access to its data. ICE has no direct contract with Flock and no direct access to Flock's systems; any documented instances of ICE benefiting from Flock searches nationally have involved local agencies running searches on ICE's behalf, not federal access to the platform itself. OCSO's data has not been implicated in any of the publicly reported misuse.

OCSO's own posture

Section X details the specific, proactive steps OCSO has taken. In short: OCSO restricted its own personnel's search categories, and kept nationwide and out-of-state sharing turned off until it had the specific case-type controls described above, rather than waiting for a problem to surface in an audit, as happened elsewhere. That the Flock platform delivered the missing control on September 11, 2026 and OCSO configured and acted on it the same day, is itself an example of the posture this report describes throughout: watching for the specific gaps, and adjusting as soon as the tool to close it becomes available, rather than treating the program's current configuration as fixed.

The case for continued, and eventually expanded, sharing

The Sheriff wants to address why data sharing matters, as it is not only a risk to be managed. The 9/11 Commission's central and most widely cited finding was that the September 11 attacks were not primarily an intelligence-collection failure. The relevant pieces of information existed within the government. **It was an information-sharing failure.** Legal and institutional barriers between agencies, and a culture that defaulted to withholding rather than sharing, meant that no single agency or analyst was ever in a position to "connect the dots." The Commission's recommendations, and the reforms that followed, shifted the legal default from a presumption against sharing to a presumption in favor of it, the creation of regional fusion centers, and the Information Sharing Environment mandated by Congress, were built directly on that finding.

The same basic dynamic exists, at a much smaller and more mundane scale, in ordinary multi-jurisdictional crime. A single county's investigators cannot see patterns that only become visible across county or state lines: a vehicle involved in a string of thefts with a common method of operation in three counties will look, from any one county's vantage point, like a single unconnected incident. When an outside agency investigating that pattern searches a shared ALPR network and finds that the suspect vehicle also passed through Ottawa County, that agency can reach out to OCSO, ask whether similar incidents have occurred locally, and hand OCSO a lead into a case OCSO did not know it had, the same "connect the dots" mechanism the 9/11 Commission's reforms were built to enable, applied to auto theft, burglary rings, or missing-persons cases rather than terrorism. Ottawa County has long benefited from this sharing posture in the relationships it has with partner agencies at the personnel level. Flock and its sharing is one small example of how OCSO is looking to take this posture at the system level.

A concrete Ottawa County example of this mechanism is that in October 2024, the Kent County Sheriff's Office arrested a suspect connected to a string of trailer and equipment thefts. When Kent County investigators ran the suspect's plate through the shared Flock network, it returned multiple hits in the Holland area of Ottawa County. Kent County shared that information with local law enforcement agencies, including OCSO. That notification gave OCSO a lead it had no independent way to generate, connecting the suspect to an open Ottawa County breaking-and-entering complaint in which a local resident had tools stolen from an Allendale address. OCSO investigators then obtained a search warrant for the suspect's historical GPS data, which further tied him to that theft and to related thefts in both counties. The recovered property was returned to the victim, and the case was forwarded to the prosecutor's office on larceny charges. None of this would have started without Kent County's outside search surfacing an Ottawa County connection neither agency knew existed on its own.

This is the same reasoning behind OCSO's decision to renew out-of-state sharing now that the platform-level case-type controls described above are in place: the value of the network scales with its reach, and the risk being managed is not sharing itself but sharing without adequate control over what is shared and for what purpose. That is the distinction the steps in Section X are specifically designed to preserve.

X. Steps Taken to Strengthen Data Protection

OCSO has taken the following concrete steps to tighten control over its ALPR data:

- Filtered and disabled immigration-enforcement and reproductive-health-related search categories at the platform level for OCSO personnel, because several states condition access to their own shared data on that restriction and because neither purpose is part of OCSO's mission.
- Identified, through OCSO's own internal review, that restricting a category of search for OCSO's own personnel did not automatically restrict that same category for other agencies searching OCSO's shared data, a platform limitation Flock remedied on September 11.
- Suspended nationwide and out-of-state sharing of OCSO's data until case-type-level control over outside-agency searches was available, then renewed sharing the same day that control was delivered and configured (September 11, 2026).
- Adopted Flock's platform-wide requirement (effective December 2025) that every search include a standardized, NIBRS-based offense-type field, improving the precision and auditability of every search of OCSO's data.
- Made previously optional search-justification fields mandatory following an internal audit finding of incomplete (not improper) documentation.
- Combined OCSO's ALPR use policy with related department policy into a single, consolidated document as part of the department's ongoing accreditation process (see Appendix A).

XI. On Cost-Benefit and Civil-Liberties Analysis

Commissioners have asked whether an independent cost-benefit analysis or civil-liberties assessment of the program has been conducted. No formal, third-party cost-benefit study exists, and the Sheriff does not believe one would be methodologically sound: there is no reliable way to assign a dollar value to a solved crime, a prevented crime, or a missing child located, and any attempt to calculate a return on investment in terms of investigative hours saved would have to account for leads that would never have existed at all without the program, a number that is, by definition, unknowable.

On civil liberties specifically, the Sheriff's approach has not been to commission an outside study but to ground the program's design directly in constitutional case law and to apply the reasoning of closely analogous precedent to OCSO's own technology choices, with the Kyllo analysis described in Section VIII as the clearest example. That same reasoning is why OCSO has declined to consider technology, such as passive RFID scanning, that would let the department see more than what is already visible to the public eye from a public vantage point, even where such technology might have investigative value.

XII. Program Outcomes

The figures below are drawn from OCSO's ALPR case-outcomes log, which tracks individual case entries where a Flock search or alert played a role, from the program's earliest logged entry in February 2024 through September 8, 2026. The log contains 241 distinct logged cases in that period.

Metric	Total (Feb. 2024 – Sept. 8, 2026)
Arrests	131
Cash/property value recovered	$917,250
Stolen vehicles recovered	72
Firearms recovered	11
Missing, lost, or runaway persons located	15

Beyond these headline totals, the underlying log is worth presenting honestly in full, because it also shows the program's limits alongside its successes. Of the 241 logged cases:

Disposition	Count
Cleared by arrest	86
Cleared by other means (recovery, citation, referral, etc. without a new arrest)	80
Lead generated (investigative lead; no further disposition logged)	64
Still in progress	24
Warrant issued	2
Suspect unable to locate	1

In other words, roughly a third of logged cases (the "lead generated" and "in progress" categories) had not reached a final disposition as of this report, and in one case a suspect identified through the system still could not be located. The Board should read the arrest and recovery totals above as outcomes tied to real, individually logged cases, not an estimate, while understanding that a meaningful share of the system's use produces an investigative lead rather than an immediate arrest or recovery, which is consistent with how the tool is described throughout this report: it generates leads for investigators to develop, not conclusions on its own.

XIII. Case Studies

Simon Andrew VanDyke

VanDyke was connected to numerous cases across Ottawa County occurring concurrently in 2025, including child sexual abuse material (CSAM), assault, computer crimes, and burglary. Flock data was used to identify the multiple vehicles VanDyke used during these offenses, providing supporting evidence that contributed to multiple convictions.

Lance Allen Holland and Ceandra Jackson

Holland and Jackson worked together to steal numerous high-value boats from dealerships, valued at over $400,000, in Indiana and Kentucky, and sold them online. Both had extensive criminal histories in Indiana, including weapons offenses, assault, theft, and vehicle theft. Flock data was instrumental in locating the suspects' vehicle across multiple state lines, leading to their arrest and conviction.

Andrew Louis Harper

Harper was identified as the primary suspect in a shooting at a Holland-area club in which two people were shot; he had an extensive criminal history including a prior attempted-murder charge. Flock data placed Harper's vehicle entering and exiting the area of the shooting both before and after it occurred, establishing additional probable cause that led to his arrest and conviction for attempted murder.

Missing/Endangered Juveniles, May 2025

OCSO investigated a missing/endangered-children complaint involving three juveniles, aged 8, 10, and 14, and a mother who was having a mental health emergency. Flock data was used to locate the mother's vehicle in Indiana, where evidence indicated the children were being moved from a motel; further evidence indicated the family had continued on to St. Louis, Missouri, where the mother and children were subsequently located.

XIV. Conclusion and Recommendations

Ottawa County's ALPR program, as currently configured, is a limited, well-documented, and closely audited investigative tool operating well within the range of programs that courts have upheld against Fourth Amendment challenge. The outer boundaries of that legal question, particularly around data aggregation and interagency sharing, continue to develop nationally, and remain genuinely open questions this report has tried to present honestly rather than resolve. OCSO has not waited for those questions to be settled elsewhere before tightening its own controls, and intends to keep doing so as the platform and the surrounding law continue to evolve.

The Sheriff's Office recommends that the Board treat this report, together with the department's ALPR policy (Appendix A), as the operative record of the program's current state, and welcomes continued Board input, including requesting periodic reporting on program metrics going forward.

Appendix A: OCSO ALPR Policy

The following is Policy 424 of the Ottawa County Sheriff's Office Policy Manual, governing Automated License Plate Readers. As explained in Section IX, OCSO's current sharing numbers will likely increase as we transition from the restricted sharing posture taken before the latest Flock platform update on September 11 back to the sharing expressly allowed in the following policy.

424.1 Purpose and Scope

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

424.2 Policy

The policy of the Ottawa County Sheriff's Office is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by the ALPR are for the official use of this office. Because such data may contain confidential information, it is not open to public review.

424.3 Administration

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

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, is managed by the Investigative Services Captain, who assigns members to administer the day-to-day operation of the ALPR equipment and data.

424.4 Operations

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

- An ALPR shall only be used for official law enforcement business.
- An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.
- While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped vehicles to canvass areas around homicides, shootings, and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.
- No member of this office shall operate ALPR equipment or access ALPR data without first completing office-approved training.
- No ALPR operator may access confidential office, state, or federal data unless authorized to do so.
- If practicable, the deputy shall verify an ALPR response through the appropriate official law enforcement database (LEIN, NCIC, SOS) before taking enforcement action that is based solely on an ALPR alert.

- All searches of an ALPR system shall include a reason for the search and the case/CAD number.
- Searches related to broadcasts by dispatch that do not have a case/CAD number, such as suspected drivers or vehicles wanted by other jurisdictions, will include "Broadcast" and the reason (for example, "Broadcast, GRPD Shooting Suspect Vehicle").

When notified of an NCIC hit from an ALPR system, officers shall verify the response through LEIN before taking enforcement action; action shall not be based solely on an ALPR alert. Occasionally there may be errors in an ALPR system's reading of a license plate, so an alert alone is never a basis for police action.

Prior to initiating a stop or other intervention based on an alert, officers shall:

- Verify the status on the hot list. An officer must confirm the vehicle is still stolen, wanted, or otherwise of interest before proceeding, absent exigent circumstances. Without confirmation, deputies cannot stop a vehicle solely on an ALPR alert, and must have independent legal justification for the stop, such as a traffic violation, reasonable suspicion, or probable cause.
- Visually verify the license plate number. Officers shall visually confirm that the plate of interest matches the ALPR-captured image, including the alphanumeric characters, state of issue, and vehicle descriptors, before proceeding.
- Recognize that an alert relates to a vehicle plate, not necessarily the person operating it. Officers need independent reasonable suspicion or probable cause to make an enforcement stop; where a vehicle is entered into the system because of its association with a wanted individual, officers shall attempt to visually match the occupant to that individual's description, or have another legal basis for the stop.

424.5 Data Collection and Retention

The Investigative Services Captain is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data is transferred from vehicles to designated storage in accordance with office procedures. All stored ALPR data is retained in accordance with the established records retention schedule; thereafter, ALPR data is purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action, or is subject to a discovery request or other lawful action to produce records. In those circumstances, the applicable data is downloaded onto Evidence.com and stored digitally.

424.6 Accountability

All data is closely safeguarded and protected by both procedural and technological means. OCSO observes the following safeguards:

- All ALPR data downloaded to the mobile workstation and in storage is accessible only through a login/password-protected system capable of documenting all access to information by name, date, and time.
- Members approved to access ALPR data are permitted to do so for legitimate law enforcement purposes only, such as a specific criminal investigation or office-related civil or administrative action.
- ALPR system audits are conducted regularly by the Professional Standards Captain or other assigned system administrator.

424.7 Releasing ALPR Data

ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes, or as otherwise permitted by law, using the following procedures:

- ALPR data may be shared with the Prosecutor's Office in accordance with other digital evidence sharing procedures.
- The requesting agency makes a written request that includes the name of the agency, the name of the requesting person, and the intended purpose of obtaining the information.
- The request is reviewed by the Investigative Services Captain or an authorized designee and approved before it is fulfilled.
- The approved request is retained on file.

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

424.8 ALPR Network Data Sharing

A. Network Discoverability and Access Preferences. To facilitate multi-jurisdictional cooperation while maintaining data security, the ALPR network presence is configured as follows: the OCSO ALPR network is categorized as a "discoverable network" nationwide, allowing other law enforcement agencies to identify the network and formally request data access; approved external agencies are granted both historical search capabilities and real-time alert functions within the system.

B. Geographic Sharing Parameters. Sharing is controlled by geographic boundaries and agency-type designation. State of Michigan agencies (local, county, and state law enforcement) receive automated acceptance of incoming sharing requests; federal agencies are explicitly excluded from this automated acceptance. Camera data is also actively shared with approved law enforcement agencies within a 500-mile radius of Ottawa County under the same regional sharing tier; federal organizations are explicitly excluded from this tier as well.

C. Data Governance and Restrictions. All shared ALPR data is designated "For Official Use Only" and must be used for legitimate law enforcement and public safety purposes. Data may only be shared with official law enforcement or prosecutorial agencies. The Investigative Services Captain, or a designated system administrator, retains authority to manage, audit, and revoke network sharing access to ensure ongoing policy compliance. Urgent or ad hoc requests from agencies outside the automated sharing parameters must be reviewed and approved by the Investigative Services Captain or an authorized designee before fulfillment.

D. Data Sharing Preferences. The Sheriff's Office reserves the right to determine what offense-type data will be shared with other law enforcement agencies. Shared data is limited to major crimes and public safety-related matters only; examples of data not shared include traffic analysis and civil traffic offenses.

Appendix B: Case Law Quick Reference

The cases below are the foundational Fourth Amendment framework cited in Section VIII. For an extensive national compendium of decisions addressing ALPR technology specifically, see Appendix C.

Katz v. United States, 389 U.S. 347 (1967): Reasonable-expectation-of-privacy framework.

United States v. Knotts, 460 U.S. 276 (1983): No expectation of privacy in movements on public roads.

Kyllo v. United States, 533 U.S. 27 (2001): Sense-enhancing tech revealing non-public information = search.

United States v. Jones, 565 U.S. 400 (2012): Physical GPS attachment = search (trespass theory).

Carpenter v. United States, 585 U.S. 296 (2018): 7+ days of historical CSLI from a third party = search.

Chatrie v. United States, 609 U.S. ___ (2026): Geofence warrant for cell location data = search; remanded on warrant validity. Distinguishable from fixed ALPR.

Appendix C: ALPR Fourth Amendment Case Compendium

The attached document, "Automated License Plate Recognition (ALPR) Technology: Judicial Rejection of Fourth Amendment Challenges" (Major County Sheriffs of America), compiles federal and state court decisions from across the country rejecting Fourth Amendment challenges to ALPR technology, or holding that there is no reasonable expectation of privacy in a license plate displayed in public. It is provided as a separate attachment to this report and is referenced throughout Section VIII.

Automated License Plate Recognition (ALPR) Technology
Judicial Rejection of Fourth Amendment Challenges

The use of Automated License Plate Reader (ALPR) technology by law enforcement **does not constitute a Fourth Amendment search or violate the Fourth Amendment**. Courts across the country have repeatedly rejected Fourth Amendment challenges to law enforcement's use of ALPR.

Some advocates wrongly equate law enforcement's use of ALPR data with access to cell site location information, which the Supreme Court addressed in *Carpenter v. United States*, 585 U.S. 296 (2018). In *Carpenter*, the Court held that the government's warrantless acquisition of an extensive history of cell site location information generated by a person's cell phone constituted a Fourth Amendment search. ALPR data is fundamentally different: it consists of discrete observations of publicly displayed license plates captured in plain view at particular times and locations. Courts at all levels around the country have made a clear distinction between those public observations and the comprehensive non-public location history at issue in *Carpenter*.

The following courts have rejected Fourth Amendment challenges to law enforcement's use of ALPR technology or have held that there is no reasonable expectation of privacy in license plates displayed in public.

FEDERAL CASES

UNITED STATES COURTS OF APPEALS

FIFTH CIRCUIT

United States v. Porter, 170 F.4th 381, 386 (5th Cir. 2026), *petition for cert. filed*, No. 26-5121, (U.S. July 20, 2026) (holding that use of an LPR, a system that provides only periodic observations of a vehicle on public streets and highways and not comprehensive tracking of an individual's movements, "did not constitute a search, so no warrant was required").

NINTH CIRCUIT

United States v. Yang, 958 F.3d 851, 862 (9th Cir. 2020) (Bey, J., concurring) (concluding that the ALPR query was not a search because it did not reveal the whole of the defendant's movements).

ELEVENTH CIRCUIT

United States v. Wilcox, 415 F. App'x 990, 992 (11th Cir. 2011) (per curiam) (holding that motorists have no reasonable expectation of privacy in license plates exposed to public view).

SIXTH CIRCUIT

United States v. Ellison, 462 F.3d 557, 561 (6th Cir. 2006) ("[A] motorist has no reasonable expectation of privacy in the information contained on his license plate under the Fourth Amendment.").

TENTH CIRCUIT

United States v. Matthews, 615 F.2d 1279, 1285 (10th Cir. 1980) (holding that motorists have no reasonable expectation of privacy in license plates exposed to public view).

UNITED STATES DISTRICT COURTS

KANSAS

United States v. Oakes, No. 25-cr-40006, 2026 WL 1020818, at *8 (D. Kan. Apr. 15, 2026) (denying motion to suppress finding "no privacy interest in a license plate number and that license plate readers are outside *Carpenter*'s reach").

NORTH DAKOTA

United States v. Lawrence, No. 3:22-CR-69, 2026 WL 765307, at *1-2 (D.N.D. Mar. 18, 2026) (denying motion to suppress and finding that use of ALPR data does not constitute a search under the Fourth Amendment).

VIRGINIA

Schmidt v. City of Norfolk, 819 F. Supp. 3d 492, 504-17 (E.D. Va.), *appeal filed*, No. 26-1227 (4th Cir. Feb. 26, 2026) (granting summary judgment, finding operation of 176 ALPR cameras located in seventy-five clusters does not constitute a search and distinguishing the "quality of the data collected here and that collected in *Carpenter* and *Beautiful Struggle*").

PENNSYLVANIA

Heller v. Brookhaven Borough, No. Civ. A. No. 25-5550, 2026 WL 381175, at *7-8 (E.D. Pa. Feb. 11, 2026) (dismissing § 1983 claim finding that "installation and general operation" of ALPR system does not constitute a Fourth Amendment search but finding that allegation that querying the system with no articulable law enforcement basis for doing so stated a viable claim for relief that survives a motion to dismiss).

OLKAHOMA

United States v. Schoggins, No. CR-25-189, 2026 WL 713083, at *4 (E.D. Okla. Jan. 28, 2026), *report and recommendation adopted*, No. 25-CR-189, 2026 WL 371256 (E.D. Okla. Feb. 10, 2026) (recommending denial of motion to suppress four months of ALPR data and finding that "[t]his Court does not perceive that the same expectation is afforded the reader information which provides historical location data on a public highway" as is afforded cell phone data).

FLORIDA

United States v. Floyd, 811 F. Supp. 3d 1345, 1348-50 (M.D. Fla. 2025) (denying motion to suppress and finding defendant "lacks a reasonable expectation of privacy in his license plate and in the information stored in the license plate reader systems").

ILLINOIS

Scholl v. Illinois State Police, 776 F. Supp. 3d 701, 714-21 (N.D. Ill. 2025) (granting motion to dismiss, finding that ALPR scanning of license plates did not constitute a Fourth Amendment search, and upholding constitutionality of Illinois's statewide ALPR program).

OHIO

United States v. Sturdivant, 786 F. Supp. 3d 1098, 1108-14 (N.D. Ohio 2025), *appeal docketed*, No. 26-3426 (6th Cir. May 12, 2026) (finding no reasonable expectation of privacy in the appearance of a vehicle or its license plate and distinguishing ALPR data, involving twenty-six images over six weeks, from the comprehensive tracking in *Carpenter*).

ARIZONA

Sidor v. Thornell, No. CV-25-08141, 2025 WL 3282976, at *8-11 (D. Ariz. Oct. 24, 2025), *report and recommendation adopted*, No. CV-25-08141, 2025 WL 3281746 (D. Ariz. Nov. 25, 2025) (denying habeas

petition finding no reasonable expectation of privacy in cross-country trip that generated one ALPR image in 24 hours but noting that "the mere use of ALPRs is not yet a search in American law—though in a more developed record, or a future more rife with cameras, it might well be a search").

FLORIDA

Schemel v. City of Marco Island Fla., No. 2:22-cv-79, 2025 WL 2958798, at *2-3 (M.D. Fla. Oct. 17, 2025), *appeal docketed*, No. 25-13913 (11th Cir. Nov. 6, 2026) (dismissing for failure to state Fourth Amendment claim because ALPRs are "hardly comparable" to the facts in *Carpenter* where "ALPRs do not track the whole of Plaintiffs' physical movements—or anything analogous").

NEW YORK

Rinaldi v. Sylvester, No. 24-272, 2025 WL 2682691, at *16-18 (S.D.N.Y. Sept. 19, 2025) (finding that use of ALPR involving 111 searches of the subject vehicle over two-and-a-half years does not constitute a Fourth Amendment search).

OKLAHOMA

United States v. Brown, No. CR-25-188-D, 2025 WL 2444596, at *3-5 (W.D. Okla. Aug. 25, 2025) (finding no reasonable expectation of privacy, and therefore no Fourth Amendment violation, because use of Flock system "falls short of the pervasive, continuous, and intimate tracking of the individual defendant in *Carpenter*").

ALABAMA

United States v. Slaybaugh, No. 3:25-CR-104, 2025 WL 2123781, at *1-2 (M.D. Ala. July 29, 2025) (denying motion to suppress because use of seventy-two ALPR images of defendant's truck travelling on public roads over three weeks "does not implicate a reasonable expectation of privacy in 'the whole of [his] physical movements'").

KANSAS

United States v. Jackson, No. 24-cr-10010, 2025 WL 1530574, at *7-9 (D. Kan. May 29, 2025) (finding no reasonable expectation of privacy and no Fourth Amendment violation for use of Flock system and distinguishing it from the "stark contrast" of the continuous and personally invasive data in issue in *Carpenter*).

INDIANA

United States v. Griffin, No. 1:24-CR-00190, 2025 WL 1474679, at *8-9 (S.D. Ind. May 22, 2025) (denying motion to suppress because no reasonable expectation of privacy and noting that defendant's "movements were not tracked and this case does not rise to the level of the GPS tracker in *Jones* or the AIR Program in *Leaders of a Beautiful Struggle*").

LOUISIANA

United States v. Cooper, No. CR 23-131, 2025 WL 35035, at *5-7 (E.D. La. Jan. 6, 2025) (rejecting a Fourth Amendment challenge to ALPR evidence noting that "only a small amount of information is collected and retained" that that "the data collected by the ALPR system is far more limited than CSLI" at issue in *Carpenter*).

VIRGINIA

United States v. Martin, 753 F. Supp. 3d 454, 476 (E.D. Va. 2024) (finding no Fourth Amendment search from Flock ALPR use that produced three images over relevant thirty-day period and distinguishing discrete vehicle observations like this from the comprehensive, detailed tracking held unconstitutional in *Carpenter*).

CALIFORNIA

United States v. Butler, No. 23-cr-00449-SI-1, 2024 WL 3447505, at *2 n.3 (N.D. Cal. July 16, 2024) (noting in dicta that "the query of the Flock database did not constitute a Fourth Amendment search under the facts

of this case because the 42 images provided by Flock did not permit law enforcement to 'track every movement that [defendant] made in the vehicle' during the time period searched").

UTAH

United States v. Salcido-Gonzalez, No. 4:23-CR-00049, 2024 WL 2305478, at *12 (D. Utah May 21, 2024), *aff'd*, No. 25-4015, 2026 WL 1164559 (10th Cir. Apr. 29, 2026) (denying motion to suppress because "the LPR system . . . used was unlike GPS Tracking or cell phone tower data information because the LPR system at issue did not operate at the granular level of detail that would expose the intimate details of an individual's life").

NEBRASKA

United States v. Jiles, No. 8:23-CR-98, 2024 WL 891956, at *19 (D. Neb. Feb. 29, 2024) (finding that accessing ALPR data was not a Fourth Amendment search because its limited volume and utility differed fundamentally from GPS and cell-site location information).

ALABAMA

United States v. Toombs, 671 F. Supp. 3d 1329, 1340-42 (N.D. Ala. 2023) (finding that accessing DEA ALPR data did not violate the Fourth Amendment and distinguishing a discrete ALPR observation from the 12,898 location points collected in *Carpenter*).

LOUISIANA

United States v. James, No. 6:21-CR-00176-01, 2023 WL 3370421, at *6 (W.D. La. Jan. 30, 2023), *report and recommendation adopted*, No. CR 21-00176, 2023 WL 3369491 (W.D. La. May 10, 2023) (denying motion to suppress and finding that "LPR systems do not constitute an unconstitutional invasion of privacy").

NEW JERSEY

United States v. Graham, No. CR 21-645, 2022 WL 4132488, at *4-5 (D.N.J. Sept. 12, 2022), *aff'd*, No. 23-3197, 2025 WL 342190 (3d Cir. Jan. 30, 2025) (denying motion to suppress ALPR data because defendant "failed to meet his burden to show that he has a reasonable expectation of privacy in his location and physical movement as captured through ALPR").

ILLINOIS

United States v. Porter, No. 21-cr-00087, 2022 WL 124563, at *3 (N.D. Ill. Jan. 13, 2022) (finding that use of ALPR did not trigger Fourth Amendment protections where it "produced limited images of Porter's vehicle at public locations over a period of approximately eight weeks, which reveals little about the intimate details of his life").

CALIFORNIA

United States v. Rubin, 556 F. Supp. 3d 1123, 1129-30 (N.D. Cal. 2021) (finding that law enforcement's access to historical ALPR data did not constitute a Fourth Amendment search because it did not provide a detailed log of the defendant's movements).

ILLINOIS

United States v. Brown, No. 19 CR 949, 2021 WL 4963602, at *2-4 (N.D. Ill. Oct. 26, 2021) (denying motion to suppress because agents "did not conduct a search under the Fourth Amendment when they queried the automatic license plate reader databases").

PENNSYLVANIA

United States v. Bowers, 2:18-CR-00292, 2021 WL 4775977, at *3-4 (W.D. Pa. Oct. 11, 2021) (holding that ALPR data did not approach the comprehensiveness of the location information in *Carpenter* or implicate similar privacy concerns).

NEW YORK

Chaney v. City of Albany, 6:16-CV-1185, 2019 WL 3857995, at *8-9 (N.D.N.Y. Aug. 16, 2019) (granting summary judgment and finding that the "use of the LPR technology did not violate Plaintiff's Fourth Amendment rights because he had no reasonable expectation of privacy in his license plate information while traveling on public roads").

STATE COURT CASES

ARIZONA

State v. Sidor, 558 P.3d 621, 629-32 (Ariz. Ct. App. 2024) (holding that ALPR database query, which was supported by reasonable suspicion and returned one photo of the defendant's license plate, did not constitute an unconstitutional search where it produced only a limited snapshot of the vehicle's travel).

MASSACHUSETTS

Commonwealth v. McCarthy, 142 N.E.3d 1090, 1101-06 (Mass. 2020) (holding that ALPR use did not invade a reasonable expectation of privacy because the limited network did not reveal the whole of the defendant's movements or "the privacies of life").

PENNSYLVANIA

Commonwealth v. Watkins, 304 A.3d 364, 369-72 (Pa. Super. Ct. 2023) (holding that there is no reasonable expectation of privacy in a license plate displayed in plain view and therefore use of a license plate reader was not a search).

SOUTH CAROLINA

State v. Faile, No. 2023-001055, 2026 WL 1894722, at *3-4 (S.C. Ct. App. July 1, 2026) (per curiam) (holding no privacy interest, and therefore no Fourth Amendment violation, in two license plate photos taken by Flock camera that "did not allow officers to obtain any intimate details related to Faile's movements" where "the police did not use the Flock photos to track Faile's location" and further noting that use of Flock was "comparable to searching . . . DMV records").

TEXAS

Uhunmwangho v. State, No. 09-19-00119-CR, 2020 WL 1442640, at *6-9 (Tex. App. Mar. 25, 2020) ("The license plate displayed on a vehicle while traveling on a public roadway is not typically an area where a person has a reasonable expectation of privacy, and we conclude that taking a picture of a license plate displayed on a vehicle that is traveling on a public road would not be subject to Fourth Amendment protection nor would it constitute a search.").

VIRGINIA

Robinson v. Commonwealth, 927 S.E.2d 822, 825-28 (Va. Ct. App. 2026) (holding that police use of a Flock ALPR database was not a Fourth Amendment search and emphasizing that the system captured publicly visible characteristics of vehicles traveling on public roads and did not continuously monitor the defendant's movements).

VIRGINIA

Commonwealth v. Church, No. 0737-25-1, 2025 WL 2908089, at *2-4 (Va. Ct. App. Oct. 14, 2025) (reversing trial court finding that warrant was required to access Flock system comprising of 172 cameras because they "are not as intrusive as cell towers and aerial surveillance equipment. The camera images are of vehicles, not persons, and the only information collected—license plates and physical characteristics of the vehicle—is already publicly viewable to anyone who sees the vehicle on the street.").

WASHINGTON

State v. Simonson, 36 Wash. App. 2d 1041, 2026 WL 242157, at *6-7 (2026) (reversing trial court suppression of ALPR data, holding that "[w]hile the Flock system as a whole potentially provides broader tracking capabilities than an officer's manual notation of a license plate, the amount of photographs taken of a license plate is inconsequential as, again, one does not have an expectation of privacy in their license plate while on public roadways").

Law enforcement remains committed to responsibly using ALPR in compliance with the Constitution and applicable federal and state laws. Law enforcement is also committed to preventing misuse of ALPR without preventing legitimate use.