October 13, 2026

PPSA
PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY

Countering the Privacy Threat from Flock Safety and Other ALPR Vendors

ALPRs as a Feature of the Surveillance State

From congressional hearings to city council meetings, Americans are voicing their anger over automated license-plate readers (ALPRs) provided by Flock Safety and other vendors.

The public understands that ALPRs are a major tool helping build an emerging American surveillance state by recording where we drive and revealing our personal, political, and religious associations and activities.

ALPRs are thus a major part of a broader network of warrantless surveillance that includes purchased geolocation, internet search history, and other sensitive personal data, as well as abusive FISA Section 702 backdoor searches that give the FBI and other agencies access to Americans' emails and texts. These systems operate under different legal authorities. Woven together by AI, they can reconstruct a person's movements, communications, associations, and private life, often without the government first obtaining a warrant, as required by the U.S. Constitution. Our government thus now has the capacity to operate as a surveillance state.

The danger is not merely that any one database will be abused. It is that data from ALPRs, communications surveillance, data brokers, social media, facial recognition, drones, and other systems can be fused to create comprehensive dossiers. The constitutional concern is not principally that a camera can see what an officer standing beside the road could see. It is that these cameras can retrospectively reconstruct movements that no officer actually followed. They can magnify this effect at a scale that far outstrips a police department's normal capabilities. A local camera that records a car on a public road may seem modest. A network that enables retrospective searches of where millions of cars have traveled is different in kind.

That distinction matters because the constitutional question cannot be reduced to whether a license plate is visible on a public road. The government has always been able to observe a car as it passes an officer. What is new is the power to collect those fleeting observations across an entire population, preserve them in a searchable archive, and later reconstruct a person's movements with the click of a button.

But scale is not the only concern. There is also a structural difference between (a) using technology to find a vehicle already suspected of involvement in a crime, and (b)

searching records about thousands of innocent drivers to discover whom to investigate. The traditional investigative sequence runs from evidence to a suspect, to legal authorization, and then to a search. A reverse search, which is often how an ALPR is used, flips that sequence: Police search first and identify the target afterward.

For its part, Flock Safety reportedly has deployed more than 120,000 cameras across 49 states, processing more than 20 billion vehicle scans each month. The overwhelming majority of these scans record vehicles whose occupants are suspected of no crime. Flock's systems can capture plates, vehicle characteristics, time, and location, while interconnected networks can make those observations searchable across jurisdictions. Artificial intelligence increases the power of that data by detecting patterns, associations, and routines at a scale no team of human officers could match.

ALPRs may have public-safety value, but the key problem is that they have become a general system for monitoring the American people. Legitimate uses are compatible with constitutional guardrails. But pervasive, suspicionless tracking raises constitutional concerns when it enables the government to reconstruct a person's movements over time.

I. Location Data Reveals the Privacies of Life

An officer may observe a vehicle on a street. And police may use an ALPR system to look for a particular vehicle already connected to a crime. The constitutional problem intensifies when the government retains observations of everyone and later searches those records to determine whom to investigate. In the first case, suspicion identifies the target of surveillance. In the second, surveillance generates the suspicion.

Retrospective surveillance makes that inversion possible because the surveillance has effectively already occurred before police identify the person they want to investigate. Once the database exists, officers can travel backward in time and reconstruct the movements of whoever later becomes a person of interest. Thus, sustained, automated, retrospective surveillance is not merely a faster version of seeing one car at one moment. And scale significantly amplifies the intrusion across the entire population. A human observer forgets; a database remembers, correlates, and searches.

A record of movements can reveal attendance at a church, synagogue, mosque, or political meeting; visits to a medical clinic, addiction-treatment provider, or family-law attorney; participation in a protest; meetings with a journalist; and intimate, romantic relationships.

In *Carpenter v. United States* (2018), the Supreme Court held that obtaining historical cell-site location information is a Fourth Amendment search because the data provides an intimate window into a person's life. More recently, in *Chatrie v. United States* (2026), the Court held that the government's acquisition of protected geofence location data constituted a search. The Court emphasized that probable cause and particularity must constrain each stage of the search. Those principles should inform the treatment of large ALPR databases. But ALPR networks also present a distinct particularity problem. There is an important difference between querying a database for a particular vehicle already

connected to a crime and searching a population's location records to discover which person or vehicle to investigate. The Fourth Amendment's prohibition on general warrants reflects a basic structural principle: the government should identify the object of its search before it searches, rather than use the search itself to select its target. The government should not be allowed to search a population's location records first and decide whom to suspect afterward.

A federal court in Oklahoma applied these distinctions to protect Fourth Amendment rights. In October 2026, U.S. District Judge Sara E. Hill ruled in *United States v. Kyle* that the warrantless search of a driver's historical location data collected by ALPRs violated the Fourth Amendment.

Judge Hill wrote:

"This is a type of indiscriminate mass surveillance. It is a tool that collects information about all vehicles that pass by any network-connected camera at all times, and it serves up the information to law enforcement on demand …

"Freedom from persistent, dragnet-style surveillance while in public is not a foreign concept in our society, and it is a reasonable expectation that society already accepts."

Judge Hill applied the logic of Supreme Court precedents in *Carpenter* and *Chatrie*. It remains to be seen whether other district courts and appellate courts will follow her reasoning.

Those courts may also recognize that the requirement of particularity does not prevent ordinary targeted uses of ALPR technology. Police looking for a stolen car can begin with its specific license plate number and use ALPR cameras to help locate it. Police looking for a vehicle already connected by evidence to a serious crime can do the same. Traditionally, a detective follows clues from the crime to a suspect and then investigates that suspect. A reverse ALPR search can invert that process: the database has already recorded everyone who passed through the area, and the detective searches those records to decide whom to investigate. Technology is no longer being used merely to investigate suspicion; it is being used to generate suspicion.

Without national standards, rules vary by contract, vendor, state, municipality, and police department. Drivers have no practical way to determine the rules under which their movements are recorded in each jurisdiction, how long the records will remain, or who may search or receive them. Constitutional liberty should not depend on a patchwork of private contracts and local settings.

II. Misuse, Error, and Mission Creep Are Already Here

The need for guardrails is not speculative. PPSA's review of ALPR deployments reveals recurring patterns of personal misuse, careless access, discriminatory searches, false matches, and expansion beyond the purposes for which the system was sold.

First, weak search controls can turn a law-enforcement database into a personal search engine. The Electronic Frontier Foundation found officers entering purported justifications

such as “LOL,” “LMAO,” “sexy,” “idk,” and “blah.” Other users entered meaningless keyboard strings. More than 30 agencies conducted over 6,300 searches marked “TBD.” One entry stated: “robbery i don’t remember the case number leave me alone.” These are not harmless clerical defects. If an officer need not state a real investigative reason, supervisors, auditors, courts, and the public cannot determine whether access was lawful.

ALPR systems have reportedly been used to monitor protests; pursue people seeking medical treatment; investigate school-residency disputes, loud-music complaints, and other low-level matters; and stalk former or prospective romantic partners. EFF also found more than 80 law-enforcement agencies using “Roma” and a slur for Romani people as search terms, often without tying the search to a suspected crime. A system capable of locating a dangerous fugitive is equally capable of locating a political dissident, a disfavored minority, or an officer’s former partner.

Second, a false or incomplete ALPR match can become the basis for a traumatic encounter when police fail to verify it. In Fayetteville, North Carolina, second-grade teacher Jacqueline McNeill was driving home with food for her goddaughter’s funeral when police vehicles cornered her car. Officers arrested her for a drive-by shooting because an ALPR image showed a white sedan similar to hers near the scene of that crime. She was innocent, missed the funeral, avoided driving the car afterward, and eventually sold it.

In DeBary, Florida, police investigating a hit-and-run crash that killed three people relied on a witness’s statement that the fleeing vehicle was a Dodge Durango. They located a Durango that had been three miles away and was traveling toward the crash, then arrested its owner, 23-year-old Lindsey Brooke Isaacs, on eight felony charges, including three counts of vehicular homicide. She spent almost two weeks in jail. Basic follow-up – including checking the actual vehicle and readily available evidence – showed that she and her Durango were not responsible. Technology supplied an apparently authoritative lead that officers failed to test against reality.

The accuracy concern is broader. A *Business Insider* investigation reported that Flock software misread plates in 71 percent of stolen-vehicle and felony alerts sent to police in Roseville, California, during 2023 and 2024. Roseville officers independently verified alerts, preventing a false stop or arrest. Elsewhere, errors combined with inadequate verification have reportedly led innocent drivers to be stopped at gunpoint, jailed, or injured. Flock has said that Roseville’s older hardware and unusual camera placement make those results unrepresentative of its system generally. But whatever the nationwide error rate, the Roseville experience demonstrates why an ALPR alert must be treated as a lead, never as probable cause by itself.

Third, access can spread far beyond the officials and purposes presented to the public. In Dunwoody, Georgia, public audit logs showed Flock employees accessing live and recorded feeds connected to the police department. Some cameras were inside the Marcus Jewish Community Center of Atlanta and showed swimming pools, preschool hallways, fitness studios, and gymnastics rooms used by children. One Flock executive reportedly accessed Dunwoody footage 185 times for sales demonstrations since the beginning of 2025; on one occasion, the only feed viewed was inside a gymnastics room.

Sales or business-development personnel should not enjoy casual access to sensitive police-linked feeds. When a private vendor operates surveillance infrastructure for the government, access privileges can themselves become a source of surveillance risk.

Fourth, mission creep is built into a network whose value grows as more data sources are added. Systems initially sold as plate readers increasingly integrate traffic cameras, private video, drones, police databases, vehicle descriptions, and artificial intelligence. School-bus cameras installed to catch motorists who illegally pass a stopped bus have even been proposed as roaming ALPR platforms recording every vehicle the bus passes. A narrow safety program can become a general location database without a meaningful public vote. That expansion can change not merely how much information police possess, but how investigations begin. A system deployed to locate vehicles already identified as suspicious can become a system for searching everyone's movements to generate suspects in the first instance.

These examples demonstrate that surveillance powers migrate. Access expands, exceptional uses become routine, and databases attract new users and rationales. Good intentions cannot substitute for enforceable constitutional standards. Recent efforts by Flock to strengthen auditing, retention, and access controls are welcome. But constitutional protections should not depend on the voluntary policies of a private vendor, which can change with management, technology, or market incentives. Congress should establish rules that follow the data regardless of which company operates the cameras.

Given the potential for ALPR databases to be combined with data collected under other warrantless surveillance authorities and integrated by AI, it is not enough to place guardrails on license plate readers alone. It is also necessary to establish reforms for FISA Section 702, which has seen millions of warrantless U.S.-person queries since the beginning of this decade. This authority allows the government to "incidentally" collect Americans' international communications and enables the government to use Americans' identifying information to search for those messages. Without reform in that domain, guardrails for ALPRs alone would be an incomplete solution to Americans' eroding privacy.

III. Congress Should Establish Enforceable National Guardrails

Former Riverside, Illinois, Police Chief Tom Weitzel, a 37-year law-enforcement veteran, has offered a constructive framework. He rejects leaving ALPR systems without meaningful oversight while recognizing their value in recovering stolen vehicles, finding missing people, and solving violent crimes. His core insight is sound – no system deserves public trust unless it can demonstrate that it is used honestly.

Weitzel proposes an independent civilian oversight board with subpoena power; written justification and case numbers for every search; immutable audit logs; a retention limit for non-hit data; and a public discipline matrix with zero tolerance for personal misuse. He also recommends public dashboards, an "Explain My Stop" portal, community participation in audits, an annual "State of Surveillance" town hall, independent academic review, plain-language policies, and compliance certification.

Congress should consider these proposals as a foundation, while strengthening several elements.

1. **Require a probable-cause warrant for tracking.** Police may respond to a contemporaneous alert that a specifically identified vehicle is stolen, associated with a missing or endangered person, or linked by articulable facts to a serious crime. But searching historical ALPR data to reconstruct an identified person's movements, associations, or pattern of life should require a warrant based on probable cause. Emergency access should be limited to imminent threats to life or safety, followed by prompt judicial review.

The warrant requirement should also distinguish targeted ALPR searches from reverse-identification searches. Police should not be permitted to search location records concerning people or vehicles for whom individualized probable cause is absent in order to discover whom to investigate. Probable cause that a crime occurred at a particular place or time does not itself establish probable cause to search the location records of every person who happened to be there. The warrant must particularize the target of the search; the search itself should not be the mechanism for choosing that target.

In keeping with the need for concurrent reform of FISA Section 702, Congress should also add a probable-cause warrant for searches of Americans' private data, whether conducted by federal authorities in international communications or state and local authorities on the roads.

2. **Prohibit monitoring protected First Amendment activity.** Federal law should expressly forbid the use of ALPR data to identify or track a person solely or substantially because of religious worship, political activity, protest participation, journalism, speech, or lawful association. Any exception must be based on particularized evidence of criminal conduct – not an ideology, faith, ethnicity, viewpoint, or attendance at a protected event. A similar restriction should be added to Section 702 reauthorization to bring searches of Americans' communications into harmony with the Constitution by codifying First Amendment protections. Efforts to require more documentation from authorized users of Section 702 should also inspire more rigor in how local police document their queries of Flock databases.

3. **Minimize collection and retention.** The default should be prompt deletion of non-hit data, meaning routine scans that do not match any vehicle "hot list" or watchlist. Weitzel suggests a limit of 30 days; Flock's chief executive now recommends seven days. Preservation beyond a well-defined period should require a documented connection to a specific investigation, a case number, and supervisory approval. "Evidence mode" or similar features must not permit indefinite retention merely because someone ran a search.

4. **Restrict sharing and federal end-runs.** An agency should not grant open-ended access to other jurisdictions, fusion centers, or federal agencies. Each outside query should meet the same legal standard that would apply if the receiving agency collected the information itself. Federal agencies should not be able to use state or local ALPR systems to circumvent federal statutory or constitutional protections. Congress should

require disclosure of all access, purchases, requests, and data transfers involving federal agencies.

5. **Make every search accountable.** Each user should have an individual credential. Every query should require a case number, suspected offense, factual justification, data scope, and approving authority. Logs should be immutable, preserved long enough for meaningful review, and subject to recurring audits by an independent body. Generic menu selections and entries such as “TBD” cannot satisfy the requirement.

6. **Require human verification before coercive action.** No stop, search, arrest, or use of force should rest solely on an ALPR alert. Officers should verify the plate, jurisdiction, vehicle description, alert status, timeliness, and other available facts. Agencies should train personnel to treat ALPR results as investigative leads and should document that verification before taking coercive action whenever circumstances permit.

7. **Impose access controls, security standards, and breach duties.** Vendor employees should receive access only when necessary for defined technical functions, with role-based permissions and logged activity. Sensitive private-camera feeds should not be used for sales demonstrations without informed consent and heightened protections. Independent security testing should be mandatory. Agencies and vendors should promptly notify affected departments, oversight bodies, and individuals of improper access or a material breach.

8. **Provide transparency, remedies, and consequences.** Communities should receive plain-language notice before deployment and a meaningful opportunity to approve or reject the program. Public reports should state the number and type of searches, matches, preserved records, outside-agency requests, federal queries, audits, violations, and disciplinary actions. Individuals should be able to learn when ALPR evidence materially contributed to a stop, search, arrest, or prosecution, subject to narrow and time-limited investigative delays. Willful misuse should carry employment consequences and appropriate civil or criminal penalties. Evidence obtained through material violations should be subject to suppression, and injured individuals should have a meaningful avenue for redress.

9. **Preserve state and local authority to adopt stronger protections.** Federal standards should be a floor, not a ceiling. States and communities should remain free to impose shorter retention periods, narrower permissible uses, warrant requirements that extend beyond the federal minimum, or bans where residents conclude that the risks outweigh the benefits.

Privacy Is a Precondition for Liberty

Americans do not surrender their constitutional liberties when they drive to work, take their children to school, visit a doctor, attend a political meeting, speak with a reporter, or go to church. A government capable of retrospectively identifying everyone who attended a protest, a campaign meeting, a mosque, a synagogue, or a church possesses a power that will inevitably chill participation – even if officials promise to use it responsibly.

That chilling effect is not incidental. Privacy is a precondition for the exercise of First Amendment rights. When people reasonably fear that the government can retrieve a record of everyone who came and went, their speech and activities are necessarily chilled. The risk falls especially heavily on dissidents, minority faiths, whistleblowers, journalists and their sources, and organizations challenging those in power.

Congress need not choose between public safety and constitutional liberty. Targeted ALPR use can solve serious crimes and rescue endangered people. But the continuous recording of innocent Americans, governed only by private contracts or official discretion, is incompatible with a free society.

The architecture of an all-seeing, ever-present surveillance state is being built now, from ALPRs to FISA Section 702 abuses, to the ever-growing purchase of geolocation, internet search history, and other sensitive personal information about Americans, to financial surveillance, and the list goes on. Artificial intelligence and the government's ability to integrate surveillance data across multiple platforms are turbocharging this dystopian disregard for Americans' constitutional rights. If Congress waits until every system is integrated and every database is searchable by artificial intelligence, the surveillance state may be too entrenched to control. We must should act while guardrails can still shape the technology, rather than after the technology has reshaped American liberty.