Testimony Regarding Automatic License Plate Reader Systems

Submitted to: The New York State Assembly; ASSEMBLY STANDING COMMITTEE ON CONSUMER AFFAIRS AND PROTECTION, ASSEMBLY STANDING COMMITTEE ON GOVERNMENTAL OPERATIONS, ASSEMBLY STANDING COMMITTEE ON LOCAL GOVERNMENTS; Automatic License Plate Reader Systems Hearing, November 9th, 2026

Submitted by: Matthew Brockbank, NY Statewide Coordinator, DeFlock

Introduction

Chair and Members of the Committee, thank you for the opportunity to submit my testimony. My name is Matthew Brockbank, and I represent the DeFlock movement as their statewide coordinator in New York. By trade I am a software engineer, as well as the chairman of the Artificial Intelligence Committee for my labor union's division. I therefore hope to bring expertise and perspective to what I consider a very important issue.

Through my testimony, I hope to effectively convey why I am asking the Assembly to enact comprehensive legislation that bans the use of license plate readers (LPRs) and automated license plate recognition (ALPR) systems in New York State. That ban should cover state agencies, local governments, and police departments, and it should bar them from buying or accessing ALPR data collected by private companies.

I make this request for two reasons: first, the technology itself is a tool of mass surveillance that records the movements of millions of innocent people, shares that data far beyond our borders, and has been abused again and again; second, its use raises serious and growing constitutional concerns under both the Fourth Amendment and Article I, Section 12 of the New York State Constitution.

What ALPR is and how it actually works

An ALPR camera, which is running 24/7, photographs every vehicle that passes it. Those photos are then fed into an A.I.-assisted program which converts aspects of the photo into searchable text, and logs the time, location, and direction of travel; it does not wait for suspicion. It records the commuter, the parent on a school run, and the patient driving to a clinic exactly as it records a suspect.

The largest vendor, Flock Safety, told the Washington Post it now operates more than 120,000 cameras in more than 6,000 communities and records about 20 billion plate scans every month [1]. Its cameras also build a "vehicle signature" from a car's make, model, color, and

distinguishing features such as bumper stickers, markings, dents, and other unique characteristics [2].

The defining feature of Flock and others like it, is the network they build. Customers of these surveillance companies can share their data locally, statewide, or nationally (with varying degrees of control) and that data can be searched without a warrant by officers at participating agencies [3]. When one Texas sheriff's office ran a single search in 2025, it swept 83,345 cameras across 6,809 networks nationwide. A Flock camera on a pole in a New York town may not be just a local tool, it could be a node in a national tracking system.

Why the technology itself is the problem

The harm of ALPR does not depend on a bad officer or a bad policy. It is built into what the system is designed to do because it surveils the innocent by default. In Saratoga Springs, the city's own Flock audit showed its cameras logged more than 249,000 unique vehicles in a 30-day period, and 95% of them had no connection to any law enforcement purpose (Saratoga Springs Flock audit, as analyzed by local advocates). In San Jose, 474 cameras detected almost 2.8 million vehicles in 30 days, and the system collected over 360 million images in 2024 alone [4].

This is a problem because it reveals the most private parts of our lives**.** A record of where a car goes is a record of where a person worships, which doctor they see, and who they visit. An Institute for Justice attorney made exactly this point about plate readers in Kansas. From there, the collected data does not stay local. More than 1,000 different entities have searched Saratoga Springs' Flock data, only 15 of them in the Capital Region, and 83% of queries came from out of state (Saratoga Springs Flock audit, as analyzed by DeFlock Troy). Once a camera joins the national network, New Yorkers lose any say over who looks at their movements, or why.

Section 4.1 of Flock's own Terms and Conditions grants the company a "limited, non-exclusive, royalty-free, irrevocable, perpetual, worldwide license" to use and disclose customer data [5]. The ACLU warns that this perpetual right lets Flock keep using driver data even after a town ends its contract. Police may say they "own" the data, but a perpetual, irrevocable license to a private company is not local control.

The record shows a pattern; it spans stalking, political retaliation, immigration enforcement, reproductive health, and misconduct. A Washington Post investigation published in August of 2026 found that at least 50 law enforcement officers nationwide have been accused of or charged with misusing plate readers, 46 of them involving Flock [6]. In 26 cases, officers allegedly tracked wives, girlfriends, exes, or women they wanted to meet. A former Costa Mesa, California officer pleaded guilty after using law enforcement databases, including Flock, to track his wife, his mistress, and her romantic interests. A Haines City, Florida officer allegedly ran his estranged ex-wife's plate through Flock 717 times over less than two years. And in our own

backyard, an Albany County Sheriff's Office investigator has been arrested after allegedly misusing Flock cameras to access information about a former girlfriend.

Of course, the problems are not just with law enforcement. Public records showed Flock employees accessed cameras in Dunwoody, Georgia, including feeds in a children's gymnastics room, a pool, a playground, and a school, as part of sales demonstrations [7]. Logs later showed more than 480 employee accesses to those feeds of children.

Constitutional and legal problems

Warrantless ALPR tracking is on a collision course with the Fourth Amendment and with Article I, Section 12 of the New York Constitution. It also quietly undermines laws this Legislature has already passed.

In *Carpenter v. United States* (2018), the Court held that police generally need a warrant to obtain historical cell-phone location records, recognizing a reasonable expectation of privacy in the whole of a person's physical movements. On June 29, 2026, in *Chatrie v. United States* (2026), the Court held 6–3 that obtaining a person's location history through a geofence warrant is a Fourth Amendment search. As already pointed out, an ALPR network builds that same kind of historical location record, for everyone, with no warrant at all.

More presently, a federal court has now applied that reasoning to Flock. On October 1, 2026, U.S. District Judge Sara Hill ruled in *United States v. Kyle*, that a Tulsa County deputy's warrantless Flock search violated the Fourth Amendment, and she suppressed all evidence that followed. The deputy followed the car only because it had a California plate; his Flock query returned more than 50 sightings across several states. Judge Hill called the system "a type of indiscriminate mass surveillance". She wrote that freedom from "persistent, dragnet-style surveillance while in public" is an expectation society already accepts.

In fact, New York's Constitution already goes further, and our highest court has applied it to vehicle tracking. In *People v. Weaver* (2009), the Court of Appeals held that attaching a GPS device to a van and tracking it for 65 days without a warrant violated Article I, Section 12. The Court decided the case on state grounds, years before the U.S. Supreme Court reached a similar result. It warned that such tracking reveals "trips to the psychiatrist, the plastic surgeon, the abortion clinic," the union meeting, and the house of worship, and observed that matching it by other means would require "cameras on every street lamp."

To be clear, New York laws already stand in opposition to ALPR technology. The ***Green Light Law*** bars the DMV from giving records to agencies that primarily enforce immigration law without a court order or judicial warrant, and a federal judge upheld it in December 2025. A national ALPR network lets federal agents follow the same cars without ever asking the DMV. The ***Local Cops, Local Crimes Act***, enacted in the 2026–27 budget, bars local police from formal or informal agreements to assist federal immigration enforcement. Researchers argue that routine Flock searches run at ICE's request may be exactly the informal cooperation the law forbids. Finally, New York's ***Shield Law*** protects people who provide or receive reproductive

health care here from out-of-state investigations. The Attorney General's guidance says the protected information includes state and local databases such as license plate readers [8]. Yet once a New York agency joins Flock's national network, a search like the one run in Texas can reach its cameras directly, without any New York official being asked.

Why regulation is not enough: the case for a ban

Some will urge the Assembly to regulate ALPR rather than ban it. The record shows that rules on paper have not protected people in practice. Illinois law bars sharing plate reader data for immigration enforcement, yet a state audit found a company had shared Illinois data with federal immigration agencies, prompting Evanston to shut its cameras off [9]. California has barred out-of-state and federal sharing since 2015, yet San Francisco's own audit found its data was queried about 300 times on behalf of out-of-state and federal agencies [10].

The main issue here is that local governments cannot control the vendor. Flock, for instance, changed its standard terms at least four times in seven months. It routinely misstated its system's capabilities, and it has reinstalled cameras that cities had ordered removed. However the collection of taxpayer data–because it’s our taxes that go to police departments that pay for these cameras–is itself an injury**.** Even a short retention rule still means every car is photographed, analyzed, and logged.

Law enforcement will credit LPRs with helping solve serious crimes, and I do not dismiss that. But usefulness has never been a reason for stripping constitutional rights from citizens; a camera in every living room would be useful too, as would not requiring law enforcement to get a warrant before entering your home. A ban on automated, networked mass collection would not prevent an officer from lawfully doing their job effectively. What it would stop is the warrantless, suspicionless logging of millions of innocent New Yorkers, and the stalking, retaliation, and out-of-state tracking that logging has enabled.

What the legislation should do

New York currently has no ALPR statute. The strongest pending bill, S9890/A10808, would bar government use except for listed purposes, require deletion within 48 hours, and require a warrant to share data outside New York state government or to obtain privately captured plate data. I urge the Assembly to start there and go further. Comprehensive legislation should:

1. Ban government use outright. Prohibit every state agency, county, city, town, village, and police department from installing, operating, or using ALPR systems, whether fixed, mobile, or trailer-mounted.
2. Prohibit government entities from buying, accessing, or receiving plate data from vendors, national networks, private businesses, homeowners' associations, or other states, including searches run by one agency on another's behalf.
3. Bar any sharing of data collected in New York with out-of-state or federal entities from the day the law takes effect.

4. Require removal of all existing cameras within a fixed period, void auto-renewal clauses, and require certified deletion of stored data by agencies and vendors, including copies held under vendor licenses.
5. Before decommissioning, each agency should publish a complete audit of every search of its data since deployment, showing who searched, from which agency, and why, and file it with the Attorney General.
6. Exclude unlawfully obtained ALPR evidence from any proceeding, give New Yorkers a private right of action with statutory damages, and authorize the Attorney General to enforce against agencies and vendors.
7. If the Assembly preserves plate cameras for cashless tolling, speed enforcement, or parking billing, police access to that data should require a warrant for a specific vehicle.

—

Respectfully submitted,

Matthew Brockbank

DeFlock, NY Coordinator

SOURCES

[1] Anchorage Daily News - How Rogue Officers Turned a Nationwide Camera Network Into a Tool for Stalking; By Drew Harwell, Douglas MacMillan, Aaron Schaffer, The Washington Post; Published: August 2, 2026

[2] The Hill - Federal judge rules warrantless Flock camera searches may violate 4th Amendment; By Mira Bhakta; 10/03/26 05:43 PM ET

[3] NBC Washington - Drivers sue San Jose over nearly 500 police cameras used to track drivers across the state; By Kevin Collier | NBC News; Published April 15, 2026 • Updated on April 16, 2026

[4] Case 5:26-cv-03181 UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN JOSE DIVISION

[5] Flock Safety's Terms & Conditions re: Data Ownership; August 21st, 2026

[6] Cybernews.com; Dozens of officers accused of using Flock system to track women they know personally; Eglė Krištopaitytė, Senior Journalist; August 4, 2026

[7] 404media.co; City Learns Flock Accessed Cameras in Children's Gymnastics Room as a Sales Pitch Demo, Renews Contract Anyway; Jason Koebler; Apr 30, 2026 at 9:25 AM

[8] https://ag.ny.gov/sites/default/files/2025-01/oag-shieldlaw-letter.pdf; RE: New York's Shield Law protections Relevant to state and local law enforcement; Letitia James, Attorney General; January 27, 2025

[9] Illinois Press Association; Impact: Evanston shuts off license plate readers after report of Illinois data shared with feds; By Richard Requena, Pioneer Press

[10] Fox 4 News; SFPD audit shows Flock cameras accessed on behalf of federal, out-of-state agencies; By Ian Bradley, KTVU FOX 2 News; June 17, 2026