INSTITUTE FOR JUSTICE

**Written Testimony of Mitchell Smith, Legislative Counsel, Institute for Justice**
New York State Assembly Standing Committees on Consumer Affairs and Protection, Governmental Operations, and Local Governments
Hearing on Automatic License Plate Reader Systems
November 9, 2026

Chairs Rozic, McDonald, and Solages, and Members of the Committees,

Thank you for the opportunity to testify. My name is Mitchell Smith, and I am Legislative Counsel at the Institute for Justice (IJ). IJ is a nonprofit, nonpartisan public interest law firm that works in courthouses and statehouses around the country to defend constitutional rights. Through IJ's Project on the Fourth Amendment and our Plate Privacy Project, we have challenged the often-unconstitutional use of automated license plate readers (ALPRs), and the vast troves of location data they generate, through litigation, legislative advocacy, and grassroots organizing. We are currently representing people challenging the constitutionality of the government's ALPR use in Norfolk, Virginia, and San Jose, California.

**The Problem: Vast, Warrantless Surveillance**

Modern, AI-driven ALPR technology allows the government to do something it has never been able to do before: travel back in time and reconstruct where people traveled, who they saw, and what they did over weeks or even months. Officers can do this as easily as running a Google search. What they are not required to do first is obtain a warrant based on probable cause that a crime is being or has been committed. And right now, New York has few rules governing who may access this data, how it is stored and shared, or how long it is kept.[1]

Unlike an officer posted at an intersection, ALPRs do not blink, take breaks, or sleep. They work around the clock and capture images of vehicles traveling at high speeds and in the dark.[2] Every picture creates a record of a location and a time, and that record is entered into a searchable database. But these surveillance platforms capture far more than a license plate number. The market leader, Flock Safety, uses artificial intelligence to convert each vehicle's visual features—including the make, model, color, bumper stickers, roof racks, and dents—into what it markets as a searchable "Vehicle Fingerprint."[3] An officer can search for a full or partial plate, filter by those features, or type a description like "blue Mustang with racing stripes." With a few more clicks, the officer can generate a "Vehicle Journey Map" showing everywhere a car has

[1]Press Release, N.Y. State Senate, Hinchey Bill Would Protect New Yorkers from Unwarranted Surveillance by License Plate Readers like Flock (Sep. 22, 2026), https://www.nysenate.gov/newsroom/press-releases/2026/michelle-hinchey/hinchey-bill-would-protect-new-yorkers-unwarranted.
[2]Complaint ¶¶ 19–22, *Schmidt v. City of Norfolk*, No. 2:24-cv-621 (E.D. Va. Oct. 21, 2024), ECF No. 1 [hereinafter Norfolk Compl.]; Complaint ¶¶ 20–23, *Tan v. City of San Jose*, No. 5:26-cv-03181 (N.D. Cal. Apr. 15, 2026), ECF No. 1 [hereinafter San Jose Compl.]; Pls.' Mem. in Supp. of Mot. for Partial Summ. J. at 3, *Schmidt v. City of Norfolk*, No. 2:24-cv-621 (E.D. Va. Nov. 20, 2025), ECF No. 179-1 (Statement of Undisputed Material Facts) [hereinafter Norfolk SJ Mem.].
[3]San Jose Compl., *supra* note 2, ¶¶ 32–34.

been captured, run "convoy analysis" to identify cars frequently seen together, and list every vehicle that visited a set of locations.[4]

Flock alone operates more than 120,000 cameras in 49 states and logs more than 20 billion vehicle scans a month.[5] These cameras sit in front of doctors' and attorneys' offices, places of worship, hospitals, military installations, even homes.[6] The volume of data collected by these cameras is staggering. For example, in San Jose, 474 cameras collected over 360 million photographs in 2024.[7] In Norfolk, Virginia, 176 cameras logged more than 41 million vehicle captures in a single 29-day period; fewer than two percent of detections triggered any alert at all.[8] Norfolk's chief of police remarked, "It would be difficult to drive anywhere of any distance without running into a camera somewhere."[9]

**Tracking the Future, Not Only the Past**

Flock tells the public that the capabilities of its cameras are modest. The company claims that a capture simply "records a vehicle at a single point in time and cannot show where a vehicle went between sightings."[10]

But the materials Flock gives to police describe a product built to anticipate movement. Flock's "Real-Time Routing" feature uses a vehicle's prior camera hits to "[d]etermine [a] possible vehicle path of travel," allowing officers to "infer which route a vehicle is likely to take after passing a Flock camera."[11] In a webinar for law enforcement, Flock put it more directly: "From that, we can then predict the route with our real-time routing."[12] Flock's own post on cross-jurisdictional response describes the next step. When a hot-listed vehicle passes a camera, "FlockOS shows its direction of travel and highlights routes and nearby cameras," so that "[u]nits in neighboring jurisdictions can then position themselves to intercept," with alerts "sent across shared cameras in real time."[13] A Flock demonstration video likewise promotes a "START REAL-TIME ROUTING" button to "help identify where vehicles are traveling in between our various Falcon cameras," a claim difficult to square with the company's assurance that its cameras cannot show where a vehicle went between sightings.[14]

---

[4] *Id.* ¶¶ 34–35; Norfolk SJ Mem., *supra* note 2, at 3–4, 9–10.
[5] Letter from Sen. Josh Hawley, Chairman, Subcomm. on Crime & Counterterrorism, to Garrett Langley, CEO, Flock Safety (Aug. 26, 2026), https://www.hawley.senate.gov/chairman-hawley-investigates-ai-powered-flock-cameras-amidst-privacy-concerns/.
[6] *See* San Jose Compl., *supra* note 2, ¶ 48 & figs. 4–7; Norfolk Compl., *supra* note 2, ¶¶ 53–55.
[7] San Jose Compl., *supra* note 2, ¶ 47.
[8] Norfolk SJ Mem., *supra* note 2, at 1, 4, 11, 22.
[9] *Id.* at 8.
[10] Flock Safety, *Solving Cross-Jurisdictional Crime in Real Time*, https://www.flocksafety.com/blog/solving-cross-jurisdictional-crime-in-real-time-how-flock-safetys-unified-platform-makes-it-possible (last updated Oct. 29, 2026) [hereinafter Flock Cross-Jurisdiction Post].
[11] Norfolk SJ Mem., *supra* note 2, at 4 (quoting Flock materials and citing deposition testimony). The memorandum notes that these features "are available to Norfolk, but it has not purchased them." *Id.* at 4 n.1.
[12] *Id.* at 9 n.3 (quoting Flock webinar).
[13] Flock Cross-Jurisdiction Post, *supra* note 10.
[14] H.C. van Pelt, *Cameras Don't Track People, Flock Does*, Footnote4A (Jul. 27, 2026), https://footnote4a.org/news/trust-job (describing and quoting Flock demonstration video).

The industry is moving further toward automated surveillance that tracks far more than a vehicle's location at a single point in time. Reporting based on Flock's own code describes new AI tools that would let officers "quickly and effortlessly reconstruct people's routes" over extended periods and "compile lists of their likely associates,"[15] as well as an "AI-powered watch list" that lets officers designate part of a city for ongoing monitoring until someone matching a described profile appears.[16] The information collected by these tools do so much more than look back, they are beginning to predict where people will be in the future.

**The Danger of Data Sharing: New Yorkers' Movements Are Searchable Nationwide**

The most valuable feature of this surveillance infrastructure, and one of the most dangerous, is its network effect. Agencies pool their data into multijurisdictional databases that allow officers to track a person's movements across cities, states, and the entire country. Once a New York agency shares its data with a network like Flock's, an officer in Texas, Montana, or anywhere else in the country can see where a New York motorist has traveled.

Agencies need not even subscribe to a company's services to obtain sensitive data. Consider the New York City Police Department's use of this technology. The NYPD has no contract with Flock and says it does not share data with the company. Yet audit logs obtained through public records requests show that NYPD officers ran 1,710 searches of Flock's national database between March 2023 and December 2025. In 614 of those searches, officers either gave no reason for the search or only included a code or shorthand that explained nothing about the purpose. The NYPD has since said it is reviewing "hundreds" of the searches.[17]

The same lack of visibility extends to immigration enforcement. An August 2026 report found Nassau County, Beacon, Glen Cove, and Cheektowaga police searching Flock on behalf of Immigration and Customs Enforcement (ICE). One search listed "Immigration (civil/administrative)" as its reason, and the report found search patterns at the New York State Intelligence Center, the State Police, and Lancaster police suggesting more immigration-related searches hidden behind vague or missing reasons.[18] In Syracuse, federal immigration agents reportedly reached drivers' data through informal cooperation with local officers and a short-

[15]Dhruv Mehrotra & Dell Cameron, *Flock Has a Powerful New AI Tool for Police. We Got Its Code*, Wired (Aug. 19, 2026), https://www.wired.com/story/flock-safety-os-investigate/.
[16]David Nield, *Flock's AI Search Tool for Police Officers Has Been Reverse Engineered—Here's What It Shows*, TechRadar (Sep. 6, 2026), https://techradar.com/tech/flocks-ai-search-tool-for-police-officers-has-been-reverse-engineered-heres-what-it-shows (reporting Wired's analysis).
[17]Rocco Parascandola, *NYPD Reviews Use of Flock Safety AI License Plate Readers*, GovTech (Sep. 30, 2026), https://www.govtech.com/public-safety/nypd-reviews-use-of-flock-safety-ai-license-plate-readers; Claire Carter, *NYPD Officers Accessed Flock Data in Over 1,000 Searches Despite Not Having a Contract*, Wash. Examiner (Sep. 28, 2026), https://washingtonexaminer.com/news/4744825/nypd-accessed-flock-data-despite-no-contract (last visited Nov. 10, 2026).
[18]Eleni Manis & Andrew Case, Surveillance Tech. Oversight Project & LatinoJustice PRLDEF, *Flock Favors: Police Across New York Search Flock on Behalf of ICE* (Aug. 25, 2026), https://www.stopspying.org/flock-favors [hereinafter Flock Favors].

lived Flock pilot.[19] New York has now barred formal and informal cooperation with ICE, but the Attorney General can enforce that ban only against searches it can see.[20]

When agencies are asked to justify these searches, the answers often lack meaningful description. IJ's Norfolk case revealed that the three most common reasons officers typed to justify a search were "cj," "stolen," and "inv," which together accounted for nearly 75,000 of the more than 230,000 searches of Norfolk's data. One officer searched for "protestor identification," and another repeatedly wrote "la la la la."[21]

**ALPR Abuse in New York and Across the Country**

Because there is currently no warrant requirement gatekeeping access to and retention of ALPR data, misuse and abuse of the technology are the predictable products of the system's design. IJ's Database of ALPR Abuse now catalogs more than 300 incidents nationwide, and the categories are disturbingly consistent.[22]

There have already been abuses in New York. In September, a senior investigator with the Albany County Sheriff's Office was arrested and charged with official misconduct and second-degree falsifying business records, accused of running more than 4,000 Flock searches over about two years. About 3,000 of those searches were for a single plate belonging to her ex-girlfriend. A second employee was placed on administrative leave. Following the arrest, the Sheriff's Office cut off Flock access for non-supervisory staff and now requires Internal Affairs audits every 30 days.[23] To be sure, these safeguards are necessary but not sufficient. More effective safeguards, like short data retention periods or warrant requirements, may have mitigated or prevented the abuse from occurring.

**The Constitution's Warrant Requirement**

The Supreme Court has said repeatedly that individuals do not surrender their privacy when they leave their driveway or go about their day in public. The Fourth Amendment protects people from unreasonable searches by requiring government agents to obtain a warrant from a judge before conducting a search of a person or protected place. In *Carpenter v. United States*, for instance, the Court held that "individuals have a reasonable expectation of privacy in the whole of their physical movements" and required a warrant for seven days of cell-site records, which are far less precise than data captured by ALPRs.[24] The Court was troubled that such data lets the

[19]Patrick McCarthy, *State Lawmaker Pam Hunter Pushing to Regulate License Plate Reader Surveillance*, Cent. Current (Jul. 8, 2026), https://centralcurrent.org/state-lawmaker-pam-hunter-pushing-to-regulate-license-plate-reader-surveillance/
[20]Flock Favors, *supra* note 18 (describing the Local Cops, Local Crimes Act and the Attorney General's enforcement role).
[21]Norfolk SJ Mem., *supra* note 2, at 13.
[22]Inst. for Just., *The IJ Database of ALPR Abuse*, https://ij.org/the-ij-database-of-alpr-abuse/ (last visited Nov. 9, 2026).
[23]Joe Wilkins, *Police Investigator Accused of Making Over 4,000 Illegal Flock Camera Searches*, Futurism (Sep. 13, 2026), https://futurism.com/future-society/police-investigator-flock-alpr-abuse-4000-illegal-searches.
[24]*Carpenter*, 585 U.S. at 310 & n.3, 312.

government "travel back in time to retrace a person's whereabouts."[25] In 2012, the Court held that attaching a GPS tracker to a car and following it for 28 days was a search.[26]

This June, in *Chatrie v. United States*, the Court held that police invaded a reasonable expectation of privacy by obtaining only two hours of a suspect's location history from a private company.[27] Crucially, the Court focused on what the technology is capable of revealing, not merely what law enforcement happened to find.[28] *Chatrie* is not an ALPR case, but it dismantles the industry's favorite defense, which is that a government's search of a limited window of data held by a vendor does not trigger a Fourth Amendment violation. Courts are now applying these principles to ALPRs. Weeks ago, in *United States v. Kyle,* a federal judge in Oklahoma became the first to rule since the *Chatrie* decision that a warrantless search of about 30 days of a driver's ALPR data was an unconstitutional search and suppressed the evidence.[29]

**The Solution: Enact A.10808-A and Keep New York's Data in New York**

The Fourth Amendment sets a floor, not a ceiling. So, this State can enact stronger protections to protect the traveling public. Assembly Bill 10808-A would do just that and gives New York the clear rules it now lacks.[30] IJ urges the Legislature to enact it. Its guardrails include:

- Restrictions on government use of ALPRs to a short list of legitimate purposes: comparing plates against hot lists or specific manually entered plates in investigations of stolen vehicles, uninsured or unregistered vehicles, outstanding felony warrants, missing persons, and vehicles used in felonies, along with parking-facility enforcement, secured-area access, electronic toll collection, and enforcement of the Vehicle and Traffic Law.[31]
- Requirements that captured plate data be deleted within 48 hours unless the data is needed as evidence in a proceeding or is subject to a warrant or other court order.
- Limitations on how data is voluntarily shared outside of the state; it keeps New Yorkers' data in New York. Agencies could not sell, share, or transfer plate data to anyone other than a New York government entity, except in response to a warrant or court order.[32]
- Mandates that agencies keep a record of every query for three years and publish an annual public report, including camera locations, plates scanned, and retention beyond 48 hours.[33]

---

[25] *Id.* at 312.
[26] *Jones*, 565 U.S. at 404–05.
[27] *Chatrie*, 609 U.S. at 628–29.
[28] *Id.* at 630 & n.9, 637–38.
[29] *United States v. Kyle*, No. 26-CR-00189-SEH, 2026 WL 2958728 (N.D. Okla. Oct. 1, 2026).
[30] A. 10808-A, 2025–2026 Reg. Sess. (N.Y. 2026), https://www.nysenate.gov/legislation/bills/2025/A10808 (last visited Nov. 10, 2026) [hereinafter A.10808-A]; S. 9890, 2025–2026 Reg. Sess. (N.Y. 2026). Citations to A.10808-A refer to the text as amended on October 23, 2026.
[31] A.10808-A, *supra* note 30, § 1 (proposed N.Y. Gen. Bus. Law § 397-c(2)(a)–(b)).
[32] *Id.* (proposed N.Y. Gen. Bus. Law § 397-c(3)(a)–(b)).
[33] *Id.* (proposed N.Y. Gen. Bus. Law § 397-c(6)(a)).

- A bar on the government introducing evidence obtained in violation of the law. It also gives injured people a private right of action, authorizes the Attorney General to seek injunctive relief, and allows local governments to adopt stricter rules.[34]

These provisions answer the abuses described above. Because the bill confines ALPR use to enumerated purposes, open-ended analytics such as convoy analysis, journey maps compiled for any reason, and pattern-based flagging could not be used outside the specific investigations the bill permits. And, since data is deleted within 48 hours, no officer could ordinarily reconstruct weeks or months of a person's life from a camera network, whether looking backward or trying to predict what comes next. Finally, an officer in Texas could not search New Yorkers' movements without the approval of a judge.

ALPR systems show so much more than a day in the life of a person. They show a person's way of life. And vendors now tell police the technology can predict the route a person will take next. We urge the Legislature to protect New Yorkers from mass surveillance, and to stop their movements from being searched by agencies across the country before these cameras end up on every street corner.

Thank you again for the opportunity to testify.

Respectfully submitted,
Mitchell Smith
Legislative Counsel
Institute for Justice
msmith@ij.org
www.ij.org

[34] *Id.* (proposed N.Y. Gen. Bus. Law § 397-c(7)–(9)).