epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

November 9, 2026
New York State Assembly
Hamilton Hearing Room B
Legislative Office Building
Albany, NY 12210

Re: Testimony of EPIC on Automated License Plate Readers in New York

Dear Chair Rozic, Chair McDonald, and Chair Solages,

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC has long advocated for sensible limits on potentially dangerous surveillance technologies, particularly those which reveal location information.[2] EPIC studies advanced surveillance technologies including traffic enforcement systems and automated license plate readers, the flaws and dangers of these systems, and their impacts on society.[3]

People do not voluntarily relinquish their rights as soon as the back out of their driveway. EPIC urges members of the Assembly to protect the privacy of New Yorkers and join the states that have enacted guardrails on this dangerous technology. EPIC supports the passage of Assembly Bill 10808 and its companion Senate Bill S.9890 to create effective guardrails using data minimization, purpose limitations, robust auditing, public reporting, and a private right of action for New Yorkers to enforce their constitutional rights.

To start, modern ALPRs are more than just simple cameras. ALPR companies now offer surveillance as a service. Their product is not just a set of cameras, but also a highly sophisticated retroactively searchable database of images of cars, their drivers, and the surroundings with a sophisticated vehicle fingerprinting algorithm that can identify cars based on license plate or natural language queries. These cameras are not only placed in static locations on public roads around a community, but also affixed to police patrol cars, in retail parking lots, and even neighborhoods governed by homeowners associations.[4] The database allows law enforcement to extensively track peoples' movements and de-anonymize your movements in day-to-day life. ALPR systems also offer AI integrations that generate suspicion through the creation of leads. ALPR software allows officers to combine the ALPR platform with public data or submit 3rd party footage to analyze with

[1] *About*, EPIC, epic.org/about/.
[2] *See e.g.* Brief for EPIC as Amicus Curiae in Support of Plaintiffs-Appellants and Urging Reversal, *Schmidt v. City of Norfolk et al*., No. 26-1227 (4th Cir. filed Apr. 20, 2026); Brief of Restore the Fourth, Inc. & EPIC as Amici Curiae Supporting Defendant-Appellant, *United States v. Chatrie*, No. 22-4489 (4th Cir. Filed Sep. 8, 2026)(on remand); Brief of CDT, Defending Rights & Dissent, The Surveillance Technology Oversight Project, & EPIC as Amici Curiae in Support of Defendant-Appellant and Reversal, *United States v. Spurlock*, No. 26-689 (9th Cir. filed Nov. 3, 2026).
[3] Michael De Dora & Maria Villegas Bravo, *A Flock of Problems with Mass Surveillance*, Tech Pol. Press (Sep. 23, 2026), https://www.techpolicy.press/a-flock-of-problems-with-mass-surveillance/.
[4] *See e.g. Go beyond basic detection*, Motorola Solutions, https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems.html (describing various camera placements).

the vehicular fingerprinting algorithms. Finally, law enforcement have the ability to download footage. Importantly, this intrusive surveillance system is not limited to Flock Safety—other companies offering vehicle recognition systems and license plate recognition systems work on the exact same business model.

I. The Legal Reality: ALPRs are Incompatible with the Fourth Amendment

The principles of the Supreme Court's decision in *United States v. Carpenter* compel the conclusion that creating a database of location information that allows reidentification of individuals is a Fourth Amendment search that would require a warrant. The Court in *Carpenter* asserted that individuals have a reasonable expectation of privacy in the whole of their movements because location information, especially over a long period of time, reveals the intricacies of the private life.[5] Just a few data points can tell law enforcement at what time you drop off your children at school, which political rallies you attend, and when you seek healthcare. This information reveals more than just where you were physically based, but also what you were doing, who you were with, and what your daily routines look like.

Beyond *Carpenter*, the courts have consistently reaffirmed this reasonable expectation of privacy in our movements. In *Chatrie v. United States*, the Court found that any amount of historical cell phone location data was sufficiently sensitive to require a warrant. Fourth Amendment protections have never been understood as "kicking in only once an intrusion goes too far[,] . . . [Fourth Amendment protections] apply regardless of the quality or quantity of information the government obtains." [6] Instead, the Court emphasized that "select[ing] the time-limited set of materials [law enforcement] want[s] from an all-encompassing database" triggers the warrant requirement.[7] Lower courts are split as to whether or not queries of ALPR systems constitute a search. A District Court in Oklahoma found that a query of an ALPR system is a search, while a District Court in Virginia found the opposite. The Virginia court case has been appealed to the Fourth Circuit, which recently held that a query of mass, indiscriminate aerial surveillance footage over Baltimore constituted a search under the Fourth Amendment.[8]

ALPR companies affirmatively advertise this type of analysis and the inferences as a valuable contribution of their surveillance systems. Flock Safety advertises various pattern analysis tools, such as its LPR Convoy Search that links certain cars to each other based on how often they travel together.[9] Axon offers a service called AxonFusus which "instantly cross-references the livestream with a dozen other nearby feeds, pulls the path of travel, and pushes it straight to officers in the field." [10] These cameras also record and surveil the community 24/7/365 in real time. The hotlist

---

[5] Brief for EPIC as Amicus Curiae in Support of Plaintiffs-Appellants and Urging Reversal, *Schmidt v. City of Norfolk et al*., No. 26-1227 (4th Cir. filed Apr. 20, 2026) (citing *Carpenter v. United States*, 585 U.S. 296 (2018)).
[6] *Chatrie v. United States*, 146 S. Ct. 2193, 2217 (2026)(internal citations omitted).
[7] *Id.* at 2218.
[8] *Leaders of a Beautiful Struggle v. Baltimore Police Comm'r. et al*., 2 F.4th 330 (4th Cir. 2021).
[9] *Solve Cases Faster, Cut Backlogs, and Avoid Burnout: The Power of a Smarter LPR*, Flock Safety Blog (Oct. 3, 2025), https://www.flocksafety.com/blog/reduce-case-backlogs-and-overtime-with-tech; *see also VehicleManager*, Motorola Solutions, https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems/vehiclemanager-lpr-analytics-software.html#undefined.
[10] *More than just plate reads: vehicle intelligence from Axon is here*, Axon Resource Center, https://www.axon.com/resources/vehicle-intelligence-from-axon-is-here.

integration allows ALPRs to flag cars as they pass cameras in real time.[11] Motorola Solutions even advertises a camera affixed to patrol cars that "detect[s] any vehicle you pass."[12]

Beyond just the nature of the information and the inferences that are made, ALPR companies create staggering quantities of data. A recent Troy Police Department (TPD) audit reported eye watering numbers.[13] Troy has a population of around 52,000 people, and the city employs 26 Flock cameras. Despite these conservative numbers, the report found 25,367,366 scans between January 1st and June 8th, 2026, or, on average, 159,543 daily scans—triple the population of the city. Beyond Flock, though, TPD also has a contract with Axon for their license plate recognition system. TPD reported, in a 90-day period, that Axon cameras captured 6.5 million plate scans, with an average of 72,802 plate scans per day. The Troy Police Department queried the Flock database 19,241 times since the cameras were installed in 2024. What's staggering is the agencies aside from the Troy Police Department that searched that same Flock data. Over 5,300 agencies, including 5,143 out of state and 12 federal agencies, queried that same pool of data between April 2024 and March 2026 an incredible12.2 million times. In fact, Houston, Texas PD alone ran 1,135,831 queries of Troy's Flock data. TPD has since reduced the agencies it shares data with to 130 agencies, half of whom are still outside a 100-mile radius of the city.

Importantly, though, policymakers cannot wait until communities reach a critical mass of cameras where the scans outnumber the population 3-to-1 on a daily basis. Setting a limit to the number of cameras in a community simply incentivizes communities and companies to sit just below that limit and continue to engage in the 24/7 surveillance of individuals and track their whereabouts. Important guardrails must be implemented, such as purpose limitations to specific types of crime most affected by the use of this kind of technology.

II. Beyond Misuse and Misidentification

Some of the biggest news stories discussing ALPRs have focused on the rampant misuse and abuse by law enforcement to use ALPRs to stalk former spouses. The Institute for Justice (IJ) tracks the misuse and abuse of ALPRs, as well as lawsuits where ALPR systems misidentified cars leading to law enforcement contact. IJ collected at least 301 incidents of police officers abusing their access to ALPR systems and wrongful stops based on misidentifications. At least 88 of them related to the stalking an ex-romantic partner,[14] including an Albany County investigator Laurie Moore who was criminally charged after running 4,000 unauthorized queries for her ex-girlfriend's vehicle.[15] There are even 37 incidents of car misidentifications that lead to harrowing encounters between law

---

[11] *Id.*

[12] *L5M Mobile LPR Camera System*, Motorola Solutions, https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems/l5m-mobile-lpr-camera-system.html

[13] Flock Audit Logs Report Data Source; Troy Police Department documents, https://www.troyny.gov/AgendaCenter/ViewFile/Item/528?fileID=2182

[14] Christopher Ingraham, *Police Have Reportedly Used License Plate Readers to Stalk Romantic Interests Dozens of Times in Recent Years*, Inst. for Justice (Apr. 27, 2026), https://ij.org/police-have-reportedly-used-license-plate-readers-to-stalk-romantic-interests-at-least-14-times-in-recent-years/#list-of-known-alpr-romantic-stalking-cases.

[15] Benjamin Gorenstein, *Sheriff's investigator charged, accused of using Flock cameras to track ex-girlfriend*, CBS6 News (Updated Sep. 10, 2026), https://cbs6albany.com/news/local/sheriffs-office-employee-arrested-accused-of-unauthorized-access-to-law-databases-albany-county-sheriffs-office-press-conference-case-enforcement-wednesday-sept-9-2026-craig-d-apple-sr-district-attorney-lee-c-kindlon-cbs6-wrgb .

enforcement and innocent civilians.[16] In September 2026, police officers in Lexington, Kentucky arrived at the home of a couple at 4 in the morning, guns drawn, after the couples' truck was erroneously flagged by Flock in an investigation of a late night road rage assault.[17] Misuse and abuse occur with many different police technologies, though, and is often related to human error, not necessarily flaws of the ALPR systems. Assembly bill 10808 addresses the concerns of misuse and abuse by addressing the critical need for ALPRs to harden their software to insider threats, increase training on the part of law enforcement, and increase oversight with audit logs, transparency, and enforceable rights for the surveilled individuals.

Another aspect of the misuse of ALPRs are searches on behalf of other law enforcement agencies who may not otherwise have access. New York law enforcement officers recently came under fire for querying Flock databases on behalf of immigration authorities.[18] According to an investigation of public records by S.T.O.P. and LatinoJustice PRLDEF, officers in Nassau County, Beacon, Glen Cove, and Cheektowaga cited the reason for submitting a search as "Immigration (civil/administrative)" or "Wanted by ICE" despite the individuals not being suspected of any crimes.[19] And in many instances, immigration-related searches may not be obvious because the "reason" field was left blank. Indeed, the report by the Troy Police Department on their use of Flock and Axon cameras stated that the most common reason entered into ALPRs systems is "(blank)" (39% of queries between 2024 and 2026) or "generic investigation / unspecified" (27.37% of queries between 2024 and 2026).[20] While New York recently passed a law that would ban the formal and informal cooperation with immigration enforcement, "the Attorney General's new Office of Immigration Trust can enforce [the law] only on immigration searches it can *see.*"[21] In regulating ALPRs, policymakers must ensure that not only are audit logs required, they are actually detailed and enforced. Assembly bill 10808 provides the infrastructure to do just this.

Database sharing between law enforcement puts New Yorkers at risk due to the difference in state laws. A Texas sheriff's office submitted over 83,000 queries to over 6,000 ALPR databases across state lines. In a statement to the press, the sheriff's office claimed it was investigating a missing person,[22] but the real reason for the search was that she was suspected of self-managing an abortion. These queries extended beyond Texas to Washington and Illinois, where abortion care is

---

[16] Christopher Ingraham, *The IJ Database of ALPR Abuse*, Inst. For Justice (Aug. 12, 2026), https://ij.org/the-ij-database-of-alpr-abuse/.

[17] *Lexington man says Flock camera hit on truck mistakenly led police to his home*, WKYT (Sep. 28, 2026), https://www.wkyt.com/video/2026/09/28/lexington-man-says-flock-camera-hit-truck-mistakenly-led-police-his-home/

[18] Eleni Manis & Andrew Case, *Flock Favors: Police Across New York Search Flock on Behalf of ICE*, S.T.O.P. and LatinoJustice PRLDEF (Aug. 25, 2026), https://static1.squarespace.com/static/6786da0226ec38320c099635/t/6abd7b977f64c6461be1e46f/1790802839361/2026-09-30_Flock+Favors_STOP-LatinoJustice_Report.pdf.

[19] *Id.* at page 3.

[20] Flock Audit Logs Report Data Source; Troy Police Department documents, at 12 https://www.troyny.gov/AgendaCenter/ViewFile/Item/528?fileID=2182

[21] Eleni Manis & Andrew Case, *Flock Favors: Police Across New York Search Flock on Behalf of ICE*, S.T.O.P. and LatinoJustice PRLDEF at 5 (Aug. 25, 2026), https://static1.squarespace.com/static/6786da0226ec38320c099635/t/6abd7b977f64c6461be1e46f/1790802839361/2026-09-30_Flock+Favors_STOP-LatinoJustice_Report.pdf.

[22] Dave Maass & Rindala Alajaji, Fl*ock Safety and Texas Sheriff Claimed License Plate Search Was for a Missing Person. It was an Abortion Investigation*, EFF Deeplinks Blog (Oct. 7, 2025), https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it.

protected by law. The audit logs even show that the reason for the search was "had an abortion, search for female." Similarly, Wisconsin police used Flock to track a man across state lines to search his car for marijuana, even though when they searched his car he was in Michigan where recreational use and possession is legal.[23] Even if New York creates strict regulations on the use of ALPRs, the act of sharing databases across state lines creates a net of surveillance that New York cannot control. Assembly bill 10808 requires judicial authorization to share data across state lines, mitigating this threat.

Finally, due to the sensitive nature of the data in these systems, ALPR cameras are a major cybersecurity and national security risk. Earlier this year, hackers stole a Flock camera and broke into its system, finding troves of unencrypted data including visual media.[24] The hackers reportedly reverse engineered the software and leaked various details of how the software works. The lack of security on these cameras creates vulnerabilities that allow individuals to get sensitive data, including the location data of thousands of residents. The data stored on the cameras and accessible through cloud storage must be secured to the strongest extent possible and routinely deleted to ensure it remains safe from bad actors. Assembly bill 10808 provides such retention and deletion policies.

III. The State Assembly Must Act Now to Protect New Yorker's Privacy

EPIC urges New York to pass Assembly bill 10808 to limit the use of ALPRs and instill safeguards to protect New Yorkers. The bill provides common sense privacy protections that keep the daily lives of New Yorkers out of the hands of law enforcement.

Thank you for the opportunity to testify. Please reach out with any questions to EPIC Counsel Maria Villegas Bravo at villegasbravo@epic.org.

Respectfully submitted,

Maria Villegas Bravo
Counsel
Electronic Privacy Information Center (EPIC)

[23] Jason Koebler, *Cops Used Flock to Track a Man Across State Lines to Create Pretext to Search His Car for Weed*, 404Media (Aug. 5, 2026), https://www.404media.co/cops-used-flock-to-track-a-man-across-state-lines-to-create-pretext-to-search-his-car-for-weed/.

[24] Joseph Cox, *Hackers Got Inside a Flock Camera. Its Data Shows How the System Really Works*, Wired (Sep. 16, 2026), https://www.wired.com/story/hackers-flock-camera-data-shows-how-system-works/.