ACLU of New York

125 Broad Street
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of Daniel Schwarz

On Behalf of the New York Civil Liberties Union

Before the New York State Assembly Standing Committees on Consumer Affairs and Protection, Governmental Operations, and Local Governments regarding Automatic License Plate Reader Systems

November 9, 2026

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the use of automatic license plate readers in New York State. The NYCLU advances civil rights and civil liberties so that all New Yorkers can live with dignity, liberty, justice, and equality. Founded in 1951 as the state affiliate of the national ACLU, we marshal an expert mix of litigation, policy advocacy, field organizing, and strategic communications. Informed by the insights of our communities and coalitions and powered by 90,000 member-donors, we work across complex issues to create more justice and liberty for more people. The NYCLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure that civil rights and liberties are enhanced rather than compromised by technological innovation.

Automatic license plate readers (ALPRs) capture the movements of millions of innocent New Yorkers every day, building detailed location records that reveal where we go to work, who we meet, which healthcare providers we visit, which places of worship we frequent, and which protests we attend. Under current law, there are no limits on how long this data can be kept, who can access it, or with whom it can be shared. Such warrantless surveillance undermines fundamental constitutional protections, in particular our rights to freedom of association, speech, religion, and privacy under the First and Fourth Amendments.

The dangers from this mass surveillance are not hypothetical: ALPRs have been used to target immigrants,[1] to track abortion-seekers,[2] to monitor protesters,[3] and to stalk domestic partners,

[1] Jason Koebler & Joseph Cox, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404 Media (May 27, 2025), https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/.
[2] Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404 Media (May 29, 2025), https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/.
[3] Dave Maass & Rindala Alajaji, *How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists*, Electronic Frontier Foundation (Nov. 20, 2025), https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists.

exes, and other people.[4]

The NYCLU urges the Legislature to enact the common sense guardrails that would be established by A.10808-A/S.9890-A. It would protect privacy and mitigate abuse by limiting when ALPRs can be used, dramatically reducing data retention periods, and prohibiting ALPR data sharing without explicit judicial oversight.

I. The Need to Curtail ALPR Use

ALPRs have become ubiquitous across the state, densely covering our roads from Buffalo to the Hamptons and from the Adirondacks to Staten Island. They collect snapshots of every vehicle in view, including information on the license plate, make, model, color, and other characteristics, alongside the specific time and location. Centrally aggregated in vast vendor databases for excessively long periods that contain billions of movement records, the systems allow for highly invasive searches about people's past travel histories, provide heat map visualizations, analyze behavior, and even predict where drivers may be in the future.

A core product feature of all major ALPR vendors is their extensive, nationwide data sharing capabilities. Flock Group Inc. ("Flock") and others specialize in enabling the most extreme forms of sharing, removing any semblance of local control. Although vendors claim customers own and control their data, their platforms and user interfaces are designed to incentivize sharing to the greatest extent possible. They do this through a range of modalities and semantic jugglery such as national lookup tools, *regional* data sharing tools (a misleading term for a sharing regime that often still covers most of the country), direct sharing relationships, and other pathways. Once access is granted, taking back control is even more difficult. Vendors rely on the same dark patterns and time-consuming opt-out regimes we have grown accustomed to from Big Tech and social media giants. Most law enforcement customers are unaware that they have granted thousands of agencies across the country pre-authorized, unrestricted access to their databases, only discovering the true extent of their sharing in response to external pressure and investigations. In Syracuse, for example, when police "inadvertently" opted in to data sharing, officers from across the country searched Syracuse drivers' information 4.4 million times between June 2024 and July 2025, of which 2,097 were labeled as immigration-related.[5] In Troy, more than 5,000 individual agencies across the country queried the town's ALPR database over 12 million times from 2024 to 2026.[6]

---

[4] Institute for Justice, *The IJ Database of ALPR Abuse* (Aug. 12, 2026) (continuously updated; last visited Nov. 7, 2026), https://ij.org/the-ij-database-of-alpr-abuse/.

[5] Patrick McCarthy, *Syracuse Police "Inadvertently" Exposed Driver Data to Thousands of Cops Around the Country*, Central Current (July 4, 2025), https://centralcurrent.org/syracuse-police-exposed-driver-data-to-thousands-of-cops-around-the-country/.

[6] Sean Cavanaugh, *Audit: Troy Police Flock Cameras Scan 159,000 Plates Daily; 5,000 Access Data*, CBS 6 Albany (Aug. 24, 2026), https://cbs6albany.com/news/local/audit-troy-police-flock-cameras-scan-159000-plates-daily-5000-access-data.

The consequences of this data sharing can be devastating. In Texas, police used out-of-state ALPR data to track down a woman they believed had self-administered an abortion.[7] In Denver, audit logs show law enforcement searched the city's data on behalf of Immigration and Customs Enforcement (ICE) over 1,400 times between 2024 and 2025.[8] In California, law enforcement agencies shared ALPR data with ICE over 100 times in a single month, in direct violation of state law.[9] Furthermore, data reviewed by the Electronic Frontier Foundation (EFF) revealed that more than fifty law enforcement agencies conducted hundreds of searches on Flock's national surveillance network targeting protest activity, including No Kings protests.[10]

Further, overreliance on ALPRs causes additional harm since the technology remains error-prone and leads to bad policing practices. Dozens of innocent people have been pulled over, detained at gunpoint, or jailed.[11] A woman in Florida recently spent thirteen days in jail after police wrongly accused her of causing a deadly crash based on information from a plate reader.[12]

The mass surveillance technology is also frequently abused for personal reasons. Across the country, there have been more than 80 documented incidents of officers stalking their domestic partners, exes, domestic violence survivors, and other women.[13] In New York State, an Albany County Sheriff's Office investigator was charged with running more than 4,000 unauthorized searches to track her ex-girlfriend and other acquaintances.[14] Meanwhile in Western New York, three Cheektowaga Police Department dispatchers spied on a female co-worker over several months.[15]

For all these reasons, there is a wave of successful opposition to ALPRs. Nationwide, more than 500 localities have pumped the brakes on Flock.[16] Yet, Flock is only one of many providers that pose similar harms and it will be critical to prevent another vendor from coming in and

---

[7] Leah Hope, *Giannoulias Speaks on Reports Texas Police Illegally Accessed IL License Plate Reader Data*, ABC7 Chicago (June 12, 2025), https://abc7chicago.com/post/secretary-state-alexi-giannoulias-speak-reports-texas-police-illegally-accessed-illinois-license-plate-reader-data/16732423/.
[8] Coalition of Civil Rights and Advocacy Organizations Deeply Concerned about Use of Flock Cameras for ICE Surveillance, https://www.aclu-co.org/app/uploads/2025/08/Flock-ICE-Statement.pdf.
[9] Khari Johnson & Mohamed Al Elew, *California Police Are Illegally Sharing License Plate Data with ICE and Border Patrol*, CalMatters (June 13, 2025), https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/.
[10] Maass & Alajaji, supra note 3.
[11] Christopher Ingraham, *Dozens of Innocent Motorists Have Been Pulled Over, Detained at Gunpoint, or Jailed Due to AI License Plate Camera Errors*, Institute for Justice (July 1, 2026), https://ij.org/dozens-of-innocent-motorists-have-been-pulled-over-detained-at-gunpoint-or-jailed-due-to-ai-license-plate-camera-errors/.
[12] Kurt Knutsson, Innocent Woman Says Police Use of Flock Camera Led to 13 Days in Jail, Fox News (Sept. 9, 2026), https://www.foxnews.com/tech/innocent-woman-says-police-use-flock-camera-led-13-days-jail.
[13] IJ Database of ALPR Abuse, supra note 4.
[14] Geoff Herbert, *NY Sheriff's Investigator Arrested, Accused of Misusing Flock Cameras to Track Ex-Girlfriend*, Syracuse.com (Sept. 10, 2026), https://www.syracuse.com/us-news/2026/09/ny-sheriffs-investigator-arrested-accused-of-misusing-flock-cameras-to-track-ex-girlfriend.html.
[15] Ian Caskie, *3 Cheektowaga Police Dispatchers Suspended for Misusing Flock Cameras*, WGRZ (Sept. 30, 2026), https://www.wgrz.com/article/news/crime/3-cheektowaga-police-dispatchers-suspended-for-misusing-of-flock-cameras/71-8e4596d5-a7b6-47ac-afd0-ad60213c65f3.
[16] Secure Justice, *Flock Termination Tracker* (last visited Nov. 7, 2026), https://secure-justice.org/flock-termination-tracker.

recreating the same harms under a different name and platform.[17] Fortunately, several New York municipalities have taken the important step of enacting local laws to ban or limit the use of ALPR technology. For example, Orange County passed a law prohibiting cloud-operated ALPR sharing platforms on its roads and, in Troy, lawmakers unanimously passed a law to restrict use, limit retention, and prohibit any warrantless sharing.[18]

But New Yorkers should not have to wait on each individual town, city, and county to pass its own safeguards. Unregulated license plate readers are a statewide problem, and New Yorkers need a statewide solution. Lawmakers must pass legislation to curtail ALPRs by significantly limiting when they can be used, dramatically reducing data retention periods, and prohibiting data sharing without a judicial warrant.

II. A Comprehensive Regulatory Framework Must Be Adopted to Prevent the Abuse of ALPR Technology

The NYCLU strongly supports comprehensive ALPR guardrails legislation, **A.10808-A (Hunter) / S.9890-A (Hinchey)**. This bill would create the necessary framework to rein in reckless mass surveillance capabilities while allowing the technology to be used for legitimate purposes. The legislation would ensure that ALPRs can only be used for specific scenarios such as felony investigations, locating stolen vehicles, finding missing persons, parking and traffic enforcement, secured area access, and toll collection. It would limit data retention to 48 hours unless the data is used as evidence in an investigation or pursuant to a warrant. It would prevent any out-of-state access or sharing unless judicially authorized and stop any potential commercial circumvention by requiring a warrant to access ALPR information from data brokers. These protections are complemented by mandatory public disclosure, detailed audit logs pertaining to use and operation, and a private right of action for individuals harmed by rogue ALPR use.

A. Use Restrictions

Given the immense mass surveillance powers ALPRs provide, legislation must limit ALPR use to narrowly defined purposes: felony investigations, locating stolen vehicles, finding missing people, parking and traffic enforcement, secured area access, and toll collection.

ALPRs collect data on everyone, not just suspects of specific crimes. This indiscriminate surveillance infrastructure enables searching for anybody, at any time, for any reason. ALPRs have been used to spy on people's lawful activities from visiting a doctor to attending a protest. Furthermore, unregulated ALPR operation has resulted in mission creep, where these systems are over-relied on and used far beyond their original scope. Research has shown the widespread use for extremely low-level investigations, in some instances even for school residency

[17] Jay Stanley, *Beware of Other License Plate Surveillance Companies Besides Flock*, ACLU (Aug. 25, 2026), https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/other-alpr-vendors.
[18] Press Release, *Troy Passes First Local Law Regulating Automatic License Plate Readers in New York*, New York Civil Liberties Union (Oct. 2, 2026), https://www.nyclu.org/press-release/troy-passes-first-local-law-regulating-automatic-license-plate-readers-in-new-york.

verification, noise complaints, employment background checks, or ticketing a motorcyclist for holding a cell phone.[19] And while police claim that they limit their use of ALPR data to solving crimes, there is a long track record of officers abusing their access for personal reasons or stalking domestic partners, exes, or others.[20]

The use restrictions in A.10808-A/S.9890-A would ensure that ALPRs are only used for clearly defined purposes and prevent the widespread abuse of the powerful surveillance technology.

B. Retention Limits

A.10808-A/S.9890-A would set strict retention limits, requiring the deletion of ALPR data within 48 hours unless it is used as evidence in an investigation or pursuant to a warrant.

This is an essential guardrail because the longer location records are kept, the more ways they can be misused. Historical ALPR records have been used to investigate abortion seekers traveling across state lines, to identify participants at protests,[21] and to reveal people's associations and movements. Retaining ALPR data for days or weeks also enables predictive use: identifying where people will drive in the future based on their past travel patterns. ICE and other federal agencies have used aggregated plate data to identify where to find and detain immigrants. And keeping data for longer periods makes such database an attractive target for bad actors as well as federal overreach.

The argument that we should keep data just in case it becomes useful is precisely the logic of mass surveillance and incongruent with any democratic society. Data minimization is a fundamental principle of privacy protection, and it is the right approach for any data generated from ALPRs.

C. Preventing Unrestricted Sharing

One of the most consequential and harmful aspects of current ALPR systems are the platformization that led to the central aggregation and sharing of data that was previously held and controlled locally. Vendors like Flock specialize in building nationwide networks that allow police departments across the country to query each other's data without restrictions or individual approval. The platform's user interface is designed to encourage expansive sharing through various modalities that obscure the vast access users grant outside entities, maximizing data flow rather than protecting privacy and oversight.

A warrant requirement ensures that New York finally closes the floodgates on rampant ALPR sharing and that out-of-state access is subject to independent judicial review. Without this

---

[19] Dave Maass & Rindala Alajaji, *More License Plate Reader Mission Creep: School Residency Verification, Background Checks, and Noise Complaints*, Electronic Frontier Foundation (May 26, 2026), https://www.eff.org/deeplinks/2026/05/more-license-plate-reader-mission-creep-school-residency-verification-background.

[20] IJ Database of ALPR Abuse, supra note 4.

[21] Maass & Alajaji, supra note 3.

guardrail, ALPR systems built with local tax dollars become instruments of federal overreach and out-of-state prosecution, circumventing local sanctuary and shield laws.

A.10808-A/S.9890-A would require judicial authorization for any out-of-state access. It would also prevent government entities from commercially circumventing the guardrails by requiring a warrant to access ALPR information from data brokers.

D. Accountability and Oversight

Because the misuse of ALPR data threatens our fundamental rights, it is critical that legislation curtailing ALPR usage include accountability and oversight measures. To this end, A.10808A/S.9890A would require mandatory audit logs of every query, including who, when, and why; as well as annual public reporting on ALPR practices and usage, such as camera locations, system statistics, and privacy policies. And critically, the bill would provide a private right of action for individuals harmed by unlawful ALPR use.

Let's be clear, a private right of action is not a financial burden on good-faith law enforcement but an important deterrent for bad actors and help ensure our local laws are followed. Police departments, Flock, and others have violated state ALPR laws repeatedly in California,[22] Illinois,[23] Virginia,[24] and Washington.[25] The threat of civil liability is one of the most effective tools to ensure compliance and allow people who are harmed by violations to hold offenders accountable.

Conclusion

The NYCLU thanks the Committees for the opportunity to provide testimony and for your focus on this critical and timely issue. We strongly urge the legislature to pass A.10808-A/S.9890-A to create necessary, comprehensive ALPR guardrails. Nobody wants to live in a world where pervasive surveillance tracks where you go, who you meet, which services you access, and how you exercise your rights.

Thank you for your attention to these urgent matters. For any questions or further discussion, please contact Senior Privacy & Technology Strategist, Daniel Schwarz at dschwarz@nyclu.org.

---

[22] Press Release, *Attorney General Bonta Continues Legal Challenge to Stop El Cajon from Illegally Sharing License Plate Data*, Cal. Attorney General (Jan. 21, 2026), https://oag.ca.gov/news/press-releases/attorney-general-bonta-continues-legal-challenge-stop-el-cajon-illegally-sharing.

[23] Press Release, *Giannoulias' Audit Finds License Plate Reader Company in Violation of State Law*, Ill. Secretary of State (Aug. 25, 2025), https://www.ilsos.gov/news/2025/august-25-2025-giannoulias-audit-finds-license-plate-reader-company-in-violation-of-state-law.html.

[24] Va. State Crime Commission, *Law Enforcement Use of Automatic License Plate Recognition (ALPR)* Update (Jan. 2026), https://vscc.virginia.gov/2026/VSCC%20ALPR%20Report%20January%202026%20FINAL%20REVISED%20Jan%2021%202026.pdf.

[25] *Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement*, Univ. of Wash. Ctr. for Human Rights (Oct. 21, 2025), https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/.