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 10, 2026
Boston City Council
Boston City Hall 5th Floor
Iannella Chamber
Boston, MA 02201

Re: Testimony of EPIC on Docket #1796 to discuss amending the Ordinance on Surveillance Oversight and Information Sharing.

Dear Chair Santana and Chair Coletta Zapatta,

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 (ALPRs), 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 applauds the City Council for its commitment to surveillance oversight and going back to the drafting board when a gap in enforcement occurs. EPIC supports the changes that would require reporting on ALPRs in the Annual Surveillance Report and encourages the City Council to require further metrics enumerated at the end of this document. These metrics will allow the Council to adequately assess the use of this dangerous surveillance technology, as well as to assess compliance with regulations.

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 in neighborhoods governed by home owners associations.[4] The ALPR software allows law enforcement to extensively track peoples' movements and de-anonymize an individual's movements in day-to-day life. The

[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).

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 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 what time you drop off your children at school, which political rallies you attend, and when and where 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

---

[5] Brief for Electronic Privacy Information Center 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.

field." [10] These cameras also record and surveil the community 24/7/365 in real time. The hotlist 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, located in New York, 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. In Boston's pilot programs, at least 45 cameras were placed around the city.[14] The amount of data that could be collected is exponentially larger, but the figures produced were silent on the actual number of scans.

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 law enforcement's rampant misuse and abuse of ALPRs to stalk former spouses or partners. 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

[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.
[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] Memo from Lieutenant Detective Justin Wood to Superintendent Richard Dahill, Chief, Bureau of Professional Standards regarding Automated License Plate Reader – FLOCK Trial 2025 at 4 (Mar. 10, 2026), https://drive.google.com/file/d/1HPEfwZmiJB1G-tBSZY6LgeLGGqCeo4qv/view.

stalking an ex-romantic partner,[15] including a Braintree, Massachusetts detective Mark Sherrick who is being investigated after running 1,000 unauthorized queries for his ex-girlfriend's vehicle.[16] There are 37 incidents of car misidentifications that lead to harrowing encounters between law enforcement and innocent civilians.[17] 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.[18] The new audit reporting requirements proposed here address the critical need for ALPRs to harden their software to insider threats, increase training on the part of law enforcement, increase oversight with audit logs, and transparency.

Another aspect of ALPR misuse is not just searching for personal use but searching on behalf of other law enforcement agencies that do not have authorization to use ALPRs. New York law enforcement officers recently came under fire for querying Flock databases on behalf of immigration authorities.[19] 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.[20] Beyond these more obvious reasons, police officers seem to obfuscate their searches related to immigrant matters by simply leaving the reason for the query 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)" (at 39% of queries between 2024 and 2026) or "generic investigation / unspecified" (27.37% of queries between 2024 and 2026).[21] While Boston Police does not cooperate with immigration enforcement, as the S.T.O.P. and LatinoJustice PRLDEF report stated oversight bodies "can enforce [the law] only on immigration searches it can *see."*[22] In regulating ALPRs, the City Council is right to ensure that not only are audit logs required, they are actually enforced.

Database sharing between law enforcement puts Boston residents at risk due to the difference in state laws. One particularly salient example of this is a Texas sheriff's office that submitted over 83,000 queries to over 6,000 ALPR databases across state lines. In a statement to the press, the

---

[15] 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.
[16] Abby Patkin, *Former Braintree detective charged with allegedly using Flock, other police tools to harass his ex*, Boston.com (Oct. 16, 2026), https://www.boston.com/news/crime/2026/09/18/former-braintree-detective-mark-sherrick-criminal-harassment-charge/.
[17] Christopher Ingraham, *The IJ Database of ALPR Abuse*, Inst. For Justice (Aug. 12, 2026), https://ij.org/the-ij-database-of-alpr-abuse/.
[18] *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/
[19] 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.
[20] *Id.* at 3.
[21] Flock Audit Logs Report Data Source; Troy Police Department documents, at 12 https://www.troyny.gov/AgendaCenter/ViewFile/Item/528?fileID=2182
[22] 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.

sheriff's office claimed it was investigating a missing person,[23] 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 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 he was in Michigan when they searched his car, where recreational use and possession is legal.[24] Even if Boston creates strict regulations on the use of ALPRs for its own police officers, the act of sharing databases across state lines creates a net of surveillance that Boston cannot control. The City Council must ensure that the reporting requirements in the Annual Surveillance Report includes an investigation on the data erroneously shared during the 2025 Flock pilot program and if any similar incidents occurred with the other ALPR pilot programs.

Finally, due to the sensitive nature of the data in these systems and the unpopular nature of the technology, 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.[25] 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. This could be detrimental, especially in places with military presence. If ALPR cameras are placed near military bases, personnel could be tracked on their commute to work or could be re-identified and exposed to bad actors. 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.

III. Boston Police Department's Audit of Its Flock Pilot Program Leaves Out Crucial Data

The audit published by the Boston Police Department provided meaningfully less information than the audit performed by the Troy Police Department in New York. While Boston PD provided the number of queries they performed, the report did not include the number of scans by the 45 cameras nor how many vehicles were identified. Nor did the audit report include any searches of the data by other law enforcement agencies. Reporting found that Flock, allegedly in error, allowed other law enforcement agencies to query the pilot program data, despite the "clear, contractual agreement prohibiting its use."[26] An investigation should be done to see who was able to access the data, and how often it was accessed.

The audit did note that just over 11,000 queries occurred in the 3-month pilot program. Of those queries, the audit found that nearly half of the queries did not contain an incident number related to

---

[23] 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.

[24] 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/.

[25] 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/.

[26] Eve Zuckoff, Flock Safety failed to secure Boston vehicle data during 2025 pilot, report finds, WBUR News (Sep. 14, 2026), https://www.wbur.org/news/2026/09/14/flock-boston-police-pilot-surveillance-technology-report

an active investigation, showing large gaps in compliance. Of the queries, 425 of them listed the reason for query as merely "investigation."[27] Boston PD must give more in depth detail to ensure that the relevant oversight bodies can meaningfully assess the use of this technology.

The amendments to the City of Boston Code, Ordinances, Chapter XVI, Section 63, Ordinance on Surveillance Oversight and Information Sharing is a great first step to increasing transparency and ensuring that the audit logs of ALPR are meaningful tools for oversight bodies both for assessing compliance as well as assessing the continuing utility of the technology. EPIC applauds the specific information requested, including contracts and vendor names, the total number of scans, and description of any alleged and/or confirmed misuse of ALPR data. The annual report, in regards to ALPRs, should also include the following:

- Which entities (meaning, but not limited to, government agencies) queried the data;
- How often each entity queried the data;
- A comprehensive accounting of the "reason" listed for the query, including tallies of specific reasons such as homicide, as well as any non-standard reasons like "haha," "investigation," or if the field was intentionally left blank;
- How many results were downloaded off of the ALPR software to law enforcement agency storage, including whether it was specifically saved for evidence, pursuant to a warrant, or for another reason to track actual retention of data;
- The training received by law enforcement to use ALPRs, including all staff that received the training, length of training, and an overview of what the training entails;
- How many scans, on average, were responsive to query, i.e., if an officer searches "blue pick-up truck," how many license plate numbers, images, and/or any other outputs are returned by the ALPR software; and
- An estimate of the population in the areas covered by ALPR cameras as a way to approximate how many people, on average, may be captured by the ALPR cameras.

IV. The City Council Must Act Now to Continue Protecting Bostonian's Privacy

EPIC applauds the initiative the City Council is taking to address the gaps in compliance with safeguards and increase transparency on the use of surveillance technology in Boston.

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)

[27] Memo from Lieutenant Detective Justin Wood to Superintendent Richard Dahill, Chief, Bureau of Professional Standards regarding Automated License Plate Reader – FLOCK Trial 2025 at 4 (Mar. 10, 2026), https://drive.google.com/file/d/1HPEfwZmiJB1G-tBSZY6LgeLGGqCeo4qv/view.