LICENSE PLATE READER SURVEILLANCE

Community Advocacy Toolkit

01 LICENSE PLATE READER SURVEILLANCE IN YOUR COMMUNITY

License plate readers (LPRs) are cameras placed on roadways that automatically photograph every passing vehicle — recording the plate, location, and time. This data is then uploaded to a searchable database, where it is often pooled with LPR data from other jurisdictions.

At least 80 Massachusetts police departments have contracts with Flock Safety, a private company that operates nearly 90,000 cameras across the country. Other departments, as well as the Massachusetts State Police, contract with Vigilant Solutions, another major LPR vendor. When a department joins Flock or Vigilant's network, its cameras often feed drivers' location information into national databases that can be searched by thousands of other law enforcement agencies — including departments in states hundreds of miles away, and in some cases, federal agencies like ICE.

This is not targeted surveillance of suspects. It is mass, warrantless tracking of every driver — the vast majority of whom have done nothing wrong.

02 WHY THIS MATTERS

For Immigrants

Documents obtained by the ACLU of Massachusetts through public records requests confirm that ICE agents have direct access to query LPR data in Vigilant Solutions' database. News reports indicate that local police have conducted searches of Flock's database on behalf of ICE agents. When your local department shares its data with a national network of law enforcement agencies, it is helping agencies engaged in civil immigration enforcement and putting local immigrant communities at risk.

For People Seeking Healthcare

Massachusetts has a Shield Law to protect people seeking reproductive or gender-affirming healthcare from out-of-state investigations and prosecution. But if your local police department is sharing LPR data nationally, that protection has a gaping hole. Out-of-state officers can search where Massachusetts residents have been driving — including trips to clinics and hospitals — without a warrant and without any meaningful oversight. Indeed, this has already happened:

A Texas officer searched Flock's national database for a woman he believed had a self-managed abortion. His stated reason in the system: "had an abortion, search for female." Court records show police were considering criminal charges. Massachusetts LPR data was queried as part of that Texas officer's search.

For Targets of Stalking and Survivors of Domestic Abuse

LPR systems don't only threaten the rights and privacy of immigrants, abortion seekers, or political dissidents. Police have also used these databases to spy on people for personal reasons. In Georgia, a police chief and a sheriff's office employee were arrested in separate incidents for using data to stalk individuals. In Milwaukee, a police officer resigned and faces criminal charges after running more than 120 searches on someone he was dating, logging each one as simply "investigation[.]" An April 2026 report found that police have used LPRs to stalk romantic interests at least 14 times in recent years.

For Political Protesters and Religious Communities

Your driving patterns reveal where you worship, which meetings you attend, and which causes you support. And indeed, police are using the technology to do so. The digital rights group Electronic Frontier Foundation found that over 50 police departments in the United States used Flock Safety's database to track people's participation in political rallies like the No Kings protests. Courts have recognized that comprehensive location tracking can chill constitutionally protected activities. Without legal guardrails, there is nothing stopping this data from being used to monitor activists, organizers, or communities targeted by the federal government.

For Everyone Who Values Privacy

Even if none of the above applies to you right now, consider that unregulated LPR surveillance creates a permanent record of your daily life. In today's political climate — where the federal government has shown a willingness to target perceived opponents — that record is a vulnerability for all of us. On a basic level, unregulated LPR surveillance flies in the face of the foundational American concept that if you're not doing anything illegal, the police shouldn't be keeping tabs on you. As it is, license plate reader use in Massachusetts today constitutes warrantless dragnet spying — something every freedom-loving person should reject outright.

03 THE DATA RETENTION PROBLEM

The longer LPR data is stored, the greater the risk of misuse. Many departments retain location data for months or years — not because it's needed for active investigations, but 'just in case.' The serious crimes that LPRs are most useful for investigating — kidnappings, hit-and-runs, stolen vehicles — are almost always reported within hours, or at most, days. A 14-day data retention window is more than sufficient for legitimate police investigations. Allowing police to retain data longer than a few weeks risks the creation of a historical archive of every driver's movements, available for any future purpose — including the abuses and misuses described above.

- More data stored = more risk of a data breach exposing sensitive location information
- More data stored = more opportunity for officers to abuse access for personal reasons
- More data stored = more material available for federal agencies conducting searches
- More data stored = greater chilling effect on protected activities like protest and worship

One Massachusetts department's Flock audit showed over 450,000 searches of the national database in a single 30-day period. At that volume, meaningful case-by-case oversight is impossible.

04 THE DATA SHARING PROBLEM

Flock's system connects your department's cameras to a network of approximately 7,000 agencies and organizations nationwide. You may trust your local police department, but you have no democratic control over police in another town or state, and neither do officials at your local police department.

Ultimately, Flock is a data company, offering tantalizing location data on millions of cars to law enforcement agencies that elect to contribute their data to the national database. Departments that share their data with the full national network get access to search the full national network. The result: a click of a button by a local administrator can expose your driving history, in your town, to thousands of police officers in Texas, Florida, and across the country.

And Flock's ever-evolving contract terms make matters worse. At the time of the ACLU of Massachusetts's public records requests in the middle of 2025, Flock's standard template user agreement granted itself a broad license to use and share data collected by a local department — possibly even when that department has restricted external sharing via Flock's administrative settings. Since then, Flock has repeatedly updated their terms and conditions.

Flock acts reactively rather than proactively; rather than ensuring municipalities remain in control of their own data from the beginning, they have frequently changed their standard terms and conditions after receiving pushback to problematic language that grants the company — not the municipalities it contracts with — control over LPR data. Flock regularly changes its standard terms and conditions without the knowledge or meaningful consent of local leaders. This is a problem for communities that seek to retain full control over their data.

You might trust your local police department's oversight and accountability rules. But when data is pooled with data from outside agencies, it operates beyond any local democratic control. You have zero say over what a department in another town or state does with information about where you drove last Tuesday.

04 STATE LEGISLATION

The Driver Privacy Protection Act, would establish statewide, comprehensive LPR protections in Massachusetts. This legislation would:

- Require deletion of LPR data within 14 days (with an exception for data pertaining to active criminal investigations)
- Prohibit buying, selling, or sharing LPR data without a court order
- Bar law enforcement from accessing third-party LPR databases without a search warrant
- Ban LPR surveillance of individuals based on First Amendment activities (protests, religious gatherings)
- Create an exclusionary rule: illegally obtained data cannot be used in court
- Create a private right of action: individuals can sue for violations
- Create warrant protections for police access to tolling data and vehicle GPS information created and maintained by car companies

This bill does not ban LPR technology. It ensures police can still use LPRs in legitimate criminal investigations, while preventing the limitless, mass surveillance of ordinary Massachusetts motorists. This legislation applies statewide, meaning all Massachusetts residents get the same baseline protection regardless of which department is involved. Local action matters, but creating clear guardrails under state law is essential.

TAKE ACTION

Step 1: Email Your Municipal Leaders

Ask your local officials whether your police department uses Flock or another LPR system, and if so, whether it shares data with outside agencies. The ACLU of Massachusetts has made this easy:

Email your municipal leaders

Step 2: File a Public Records Request

Find out exactly what your local department is doing. The ACLU of Massachusetts has prepared a model records request you can send directly to your local police department:

Download the model records request

Step 3: Share the ACLU's Letter to Municipal Officials

The ACLU of Massachusetts has sent a letter to municipal leaders across the state. Share it with your select board, city council, or mayor:

Read the ACLU-MA letter to municipal officials

Step 4: Pass a Community Control Over Police Surveillance Ordinance

Meet with local elected leaders to encourage passage and implementation of a Community Control Over Police Surveillance (CCOPS) ordinance, which would empower local leaders with approval rights before new surveillance technology is adopted by the local police department. Several Massachusetts municipalities have already enacted a CCOPS-style ordinance: Medford, Boston, Cambridge, Lawrence, Northampton, Newburyport, and Somerville.

Learn more about CCOPS ordinances and read our model policy

Step 5: Contact Your State Legislators

Urge your state representative and senator to support H.3755, the Driver Privacy Protection Act. You can find and contact your legislators through the Massachusetts Legislature's website.

Step 6: Spread the Word

Share the ACLU of Massachusetts' full resource guide with neighbors, community groups, and local elected officials:

Get The Flock Out: Full Resource Guide

ACLUM Blog: Flock Gives Law Enforcement All Over the Country Access to Your Location