

Automatic license plate reader (ALPR) cameras are rapidly being installed throughout Pennsylvania but are virtually unregulated in our state. Many ALPR cameras, such as those made by the brand Flock Safety, are continuously collecting data that can be kept and accessed by law enforcement agencies across the country. In short, our daily movements are being tracked as we travel throughout the state.

What are automatic license plate readers (ALPRs)?

Automatic license plate readers (ALPRs) are mobile and stationary cameras that record and digitize license plate numbers and run them against hot lists to identify vehicles and persons suspected of criminal activity. These cameras capture the movements of every driver who passes them, recording their plate, location, and time.

This data is then uploaded to a national database, where it can be searched by thousands of other law enforcement agencies, including out-of-state police and, in some cases, federal agencies like ICE.

Are ALPRs the same as automated traffic enforcement cameras?

No, they're not the same. Automated traffic enforcement cameras (ATEs), such as speed cameras, toll cameras, school bus or red-light cameras, are **triggered by traffic violations**. They only snap a picture when a driver breaks a law, such as speeding or running a red light.

In contrast, ALPR cameras **continuously record** every single vehicle in view of a camera. That data is then entered into a database, where it is run against “hot lists” to identify potential criminal suspects.

ALPRs aren't triggered by you doing something wrong. They track your movements any time they see you, regardless of legal behavior.

Why are ALPRs uniquely problematic?

ALPRs are mass surveillance tools. They are computer-controlled cameras that automatically capture all license plates (and more) that come into view, store that data, and allow it to be compared to external watch lists and databases. Over time, ALPRs function like a location tracker the government places on your car to monitor your movements—just in case you do something of interest to them.

Creating patterns of behavior, ALPR data can reconstruct where people have been, when, and how often, all without a warrant. This data can reveal personal details about our lives—our religious practices, medical visits, political activities, personal relationships, and daily routines.

This is not targeted surveillance of suspects. It is mass warrantless tracking of every driver, regardless of whether they are suspected of any crime.

What is Flock Safety and are they the only ALPR company to worry about?

While license plate readers have been around for some time, the private company Flock Safety is the first to create a nationwide mass surveillance database out of its customers' ALPR data. This means Flock customers in Texas or New York can access ALPR data from PA and can even do so on behalf of a non-Flock customer like ICE. In Pennsylvania, Flock cameras account for the vast majority of contracts.

But make no mistake, Flock Safety is not the only company in the mass surveillance business. Beware of other leading companies selling ALPRs to police and private companies, such as Axon, Motorola/Vigilant, Genetec, PlateSmart, Innova Systems, Rekor, ELSAG, Perceptics, and Jenoptik.

Simply switching from Flock to one of these vendors does NOT solve the problem.

Why have we seen a recent explosion in the number of ALPR cameras?

ALPRs have been in use in America since the late 1990s. But there are two reasons why ALPR use has exploded in the last several years:

- **The entry of venture capitalist funding into the mass surveillance industry:** Scaling up ALPR use through greater camera deployment, tracking, data retention, and data sharing is the only way to produce the massive profits investors expect. In other words, ALPR companies are in the business of trading our privacy for profits.
- **The advent of artificial intelligence:** The massive deployment of ALPRs generates an unimaginable amount of location data, and AI has made it possible to go through billions of ALPR scans and use them to identify drivers' intimate patterns of life. For example, Flock Safety is now using AI to allow law enforcement to search through ALPR data even more quickly with even more detail, including images of vehicle occupants, bumper stickers, and bystanders. Flock Safety ALPRs collect more than *20 billion license plate scans* per month. That's *57 scans per person in America every month*. And that's just Flock.

Don't ALPRs help keep our communities safer?

ALPRs, like all surveillance technologies, do not prevent crime or keep people safe. While in some cases, ALPRs have helped to capture criminal suspects, their limited effectiveness in this area does not justify their cost or undermining the privacy of everyone in your community.

Law enforcement often claim that since Flock cameras were installed in their community, crime in the community has gone down. But there is little conclusive evidence that can connect ALPRs to reductions in crime. In fact, a recent study in Atlanta found that despite an eightfold increase in the number of cameras integrated into the city's surveillance program, clearance rates by the Atlanta Police Department for crimes like homicide, robbery, miscellaneous larceny, and shoplifting actually *decreased* between 2021 and 2025.

How have ALPR data been abused by law enforcement?

ALPRs pose a significant threat to privacy because amassing data on vehicle locations can reveal very private details about our lives. Flock's nationwide data sharing system has made local ALPR data available to virtually any law enforcement officer who wishes to access it throughout the nation—without a warrant or public knowledge.

There have been numerous documented incidences of abuse and misuse of the Flock database resulting in violations of civil rights and civil liberties.

- A former Kansas police chief used Flock cameras to track his ex-girlfriend's vehicles 228 times over more than four months—and even followed her and her new boyfriend in his police car.
- A Texas police officer used 83,000 cameras to track a woman seeking abortion care.
- In South Carolina, a former police lieutenant admitted to using city-owned surveillance cameras to monitor his wife.
- Among numerous similar examples, a former police chief in Georgia was arrested for allegedly using ALPR systems to stalk and harass people who were not being investigated for crimes.
- Even though ICE does not have a contract to work with Flock, local law enforcement has been caught conducting national searches on behalf of ICE for immigration purposes.
- The DEA and ATF collaborated on plans to monitor gun show attendees using ALPR data.
- Kansas police officers used ALPR technology to pursue a man who wrote an op-ed critical of the police department.
- More than 50 federal, state, and local agencies ran hundreds of searches through Flock's national network of surveillance data in connection with protest activity.

ALPR systems can also make mistakes when logging and flagging vehicles for law enforcement. And when ALPR cameras get it wrong, the consequences can be dangerous.

- A 12-year-old girl in New Mexico was handcuffed after an ALPR camera misread the license plate on the car her older sister was driving.
- In Colorado, a mother and her family were held at gunpoint because ALPR cameras wrongfully flagged their car as stolen.
- A Colorado police officer wrongfully accused a woman of theft based on a Flock hit, and then refused to look at evidence proving her innocence.

If I'm not doing anything wrong, why should I care about ALPR tracking?

Unlike speed cameras or red-light cameras that only take a photo when a specific violation has occurred, ALPR cameras are always on and constantly photographing any car that drives past, making it possible to create comprehensive records of everybody's comings and goings. And that data can reveal very private details about our lives.

Police and anyone else who has access to the database can use it to track you and piece together information to use against you, ***without a warrant*** and ***whether you've broken a law or not***.

How do ALPRs infringe on our privacy rights?

It's true that if you're driving or parked in a public space, your license plate is in public view. Anyone can look at it and take a picture. ALPRs, however, take “public view” and put it on steroids. They take thousands of images a minute and pour them into a massive database for anyone with access to see it. Suddenly your license plate—and *all its movements*—are in “public view” in Texas and Florida and everywhere else, and not just in real time, but for as long as the data is retained.

Our concern about ALPRs is not that they are being used to, say, catch a car thief (although we are concerned when they improperly label an innocent person as a suspect). Our concern is that in the process of tracking down a legitimate car thief, the government is vastly overreaching and creating a massive national database that tracks all of us all day long.

A nationwide video surveillance network is contrary to the guarantees of the Constitution. This dragnet surveillance threatens the freedoms the Fourth Amendment was adopted to protect.

It is a core principle that our government does not invade people's privacy and collect information about citizens' activities, just in case they do something of interest to them. In fact, this type of “just in case” information collection would essentially treat every person in America like a potential criminal suspect.

The 4th Amendment of the U.S. Constitution protects us all from “unreasonable searches and seizures” by the government and guarantees “the right of the people to be secure in their persons, houses, papers, and effects.” This means the government needs permission, based on probable cause and individualized suspicion, not only to search your home but also to monitor the data we all produce constantly and mostly involuntarily, like your cell phone location data.

Today, new and emerging technologies are outpacing the privacy protections on which we have long relied. The explosion of government surveillance programs and technologies are sweeping up ever more data about the most intimate aspects of our lives—our whereabouts and our communications, the websites we visit, what we buy, information about our health, our bodies, and more.

We can't trust every government agency nationwide to use this data in a constitutional way. Protecting our personal data and limiting surveillance are essential to safeguarding freedom, safety and equity.



For more information, visit aclupa.org/GTFO-PA.