

1. Mark your confusion.
2. Show evidence of a close reading.
3. Write a 1+ page reflection.

What Is Happening with License Plate Readers?

Source: Matt Burgess, MalwareBytes.com, November 20, 2025

You're driving home after another marathon day of work and kid-shuttling, nursing a lukewarm coffee in a mug that's trying too hard. As you turn onto your street, something new catches your eye. It's a tall pole with a small, boxy device perched on top. But it's not a bird-house and there's no sign. There is, however, a camera pointed straight at your car.

It feels reassuring at first. After all, a neighbor was burglarized a few weeks ago. But then, dropping your kids at school the next morning, you pass another, and you start to wonder: *Is my daily life being recorded and who is watching it?*

That's what happened to me. After a break-in on our street, a neighborhood camera caught an unfamiliar truck. It provided the clue police needed to track down the suspects. The same technology has shown up in major investigations, including the "Coroner Affair" murder case on ABC's 20/20. These cameras aren't just passive hardware. They're everywhere now, as common as mailboxes, quietly logging where we go.

So if they're everywhere, what do they collect? Who's behind them? And what should the rest of us know before we get too comfortable or too uneasy?

A mounting mountain of surveillance

ALPRs aren't hikers in the Alps. They're Automatic License Plate Readers. Think of them as smart cameras that can "read" license plates. They snap a photo, use software to convert the plate into text, and store it. Kind of like how your phone scans handwriting and turns it into digital notes.

People like them because they make things quick and hands-free, whether you're rolling through a toll or entering a gated neighborhood. But the "A" in ALPR (automatic) is where the privacy questions start. These cameras don't just record problem cars. They record every car they see, wherever they're pointed.

What exactly is Flock?

Flock Safety is a company that makes specialized ALPR systems, designed to scan and photograph every plate that passes, 24/7. Unlike gated-community or private driveway cameras, Flock systems stream footage to off-site servers, where it's processed, analyzed, and added to a growing cloud database. At the time of writing, there are probably well over 100,000 Flock cameras installed in the United States and increasingly rapidly. To put this in perspective, that's one Flock camera for every 4,000 US citizens. And each camera tracks twice as many vehicles on average with no set limit.

Think of it like a digital neighborhood watch that never blinks. The cameras snap high-resolution images, tag timestamps, and note vehicle details like color and distinguishing features. All of it becomes part of a searchable log for authorized users, and that log grows by the second. Adoption has exploded. Flock said in early 2024 that its cameras were used in more than 4,000 US cities. That growth has been driven by word of mouth ("*our HOA said break-ins dropped after installing them*") and, in some cases, early-adopter discounts offered to communities.

A positive perspective

Credit where it's due: these cameras can help. For many neighborhoods, Flock cameras make them feel safer. When crime ticks up or a break-in happens nearby, putting a camera at the entrance feels like a concrete way to regain control. And unlike basic security cameras, Flock systems can flag unfamiliar vehicles and spot patterns, which are useful for police when every second counts. In my community, Flock footage has helped recover stolen cars and given police leads that would've otherwise gone cold. After our neighborhood burglary, the moms' group chat calmed down a little knowing there was a digital "witness" watching the entrance.

In one Texas community, a spree of car break-ins stopped after a Flock camera caught a repeat offender's plate, leading to an arrest within days. And in the "Coroner Affair" murder case, Flock data helped investigators map vehicle movements, leading to crucial evidence.

Regulated surveillance can also help fight fake videos. Skilled AI and CGI artists sometimes create fake surveillance footage that looks real, showing someone or their car doing something illegal or being somewhere suspicious. That's a serious problem, especially if used in court. If surveillance is carefully managed and trusted, it can help prove what really happened and expose fabricated videos for what they are, protecting people from false accusations.

The security vs overreach tradeoff

But there are real concerns too. ALPRs collect sensitive data, often stored by third-party companies, which creates risk if that information is misused or hacked. And then there's "surveillance creep," which is the slow expansion of monitoring until it feels like everyone is being watched all the time. So while there are clear benefits, it's important to think about how the technology could affect your privacy and the community as a whole.

What's being recorded and who gets to see it

Flock's system is laser-focused on license plates and cars, not faces. The company says they don't track what you're wearing or who's sitting beside you. Still, in a world where privacy feels more fragile every year, people wonder how much these systems quietly log.

What's recorded?

License plate numbers, vehicle color/make/model, time, location. Some cameras can capture broader footage; some are strictly plate readers.

How long is it kept?

Flock's standard is 30 days, after which data is automatically deleted (unless flagged in an active investigation).

Who has access?

This is where things get dicey. Using Flock's cloud, only "authorized users", which can include community leaders and law enforcement, ideally with proper permissions or warrants, can view footage. Residents can make requests for someone to determine privileges. Flock claims they don't sell data, but it's stored off-site, raising the stakes of a breach. The bigger the database, the more appealing it is to attackers. Unlike a home security camera that you can control, these systems by design track everyone who comes and goes.

And while these cameras don't capture people, they do capture patterns, like vehicles entering or leaving a neighborhood. That can reveal routines, habits, and movement over time. A neighbor was surprised to learn it had logged every one of her daily trips, including gym runs, carpool, and errands. Not harmful on its own, but enough to make you realize how detailed a picture these systems build of ordinary life.

The place for ALPRs... and where they don't belong

If you're feeling unsettled, you're not alone. ALPRs are being installed at lightspeed, often faster than the laws meant to govern them. Will massive investment shape how future rules are written? Consider the surveillance and data collection laws:

Federal: There's no nationwide ban on license plate readers; law enforcement has used them for years. (We've also reported on police using drones to read license plates, raising similar concerns about oversight.) However, courts in the US increasingly grapple with how this data impacts Fourth Amendment "reasonable expectation of privacy" standards.

Local: Some states and cities have rules about where cameras can be placed on public and private roadways. They have also ordained how long footage can be kept. Check your local ordinances or ask your community for policy. A good example is Oakland, where the City Council limited ALPR data retention to six months unless tied to an active investigation. Only certain authorized personnel can access the footage, every lookup is logged and auditable, and the city must publish annual transparency reports showing usage, access, and data-sharing. The policy also bans tracking anyone based on race, religion, or political views. It's a practical attempt to balance public safety with privacy rights.

What if the footage is misused or hacked?

This is the big one. If footage leaves your neighborhood, such as handed to police, shared too widely, or leaked online, it can create liability issues. Flock says its system is encrypted and tightly controlled, but no technology is foolproof. If you think footage was misused, you can request an audit or raise it with your HOA or local law enforcement.

As neighborhood ALPRs like Flock cameras become more common, a growing set of advocacy and educational sites has stepped in to help people understand the technology, and to push back when needed: Deflock.me is one of the most active. It helps residents opt their vehicles out where possible, track Flock deployments, and organize local resistance to unwanted surveillance. Meanwhile, haveibeenflocked.com has an almost playful approach to a very real issue: it lets people check whether their car has appeared in Flock databases. That simple search often surprises users and highlights how easily ordinary vehicles are tracked.

For folks seeking a deeper dive, Eyes on Flock and ALPR Watch map where Flock cameras and other ALPRs have been installed, providing detailed databases and reports. By shining a light on their proliferation, the sites empower residents to ask municipal leaders hard questions about the balance between public safety and civil liberties. Together, these initiatives paint a clear picture: while ALPRs spread rapidly in the name of safety, an equally strong movement is demanding transparency, limits, and respect for privacy. Whether you're curious, cautious, or concerned, these sites offer practical help and a reminder that you're not alone in questioning how much surveillance is too much.

• Possible Response Questions

- What are your thoughts about the use of ALPRs? Explain.
- Did something in the article surprise you? Discuss.
- Pick a word/line/passage from the article and respond to it.
- Discuss a "move" made by the writer in this piece that you think is good/interesting. Explain.