

Report

Automatic License Plate Readers: Benefits, Risks, and Sensible Regulation

Charles Fain Lehman

Senior Fellow
Manhattan Institute

Rafael Mangual

Nick Ohnell Fellow
Manhattan Institute

Executive Summary

Automatic License Plate Readers (ALPRs) are a popular policing technology that uses cameras and integrated software to identify cars by their license plates (and, in some cases, other identifying characteristics). ALPRs have become the subject of sustained online and offline furor in recent months, prompting calls to ban or physically destroy them.

These calls are mistaken. ALPRs are not a new technology—police have used them for decades. While the research is still developing, the best available evidence supports the proposition that ALPRs help reduce crime. And while doctrine is still evolving, there is a strong argument that their use does not contravene the Fourth Amendment as the courts today understand it.

While there are legitimate concerns about the abuse of ALPRs, the best approach for policymakers is not to ban the technology altogether, but to mitigate those risks through sensible regulation. Specifically, departments and state lawmakers should implement rules mandating:

- logging of access;
- criminal penalties for misuse;
- supervisory approval;
- restrictions limiting the use of police ALPRs to major crimes; and
- limits on data retention;
- prohibitions on placing ALPRs near sensitive places, like churches or medical facilities.
- audits;

These reasonable rules will preserve ALPRs as a crime-solving tool, while mitigating the risk of abuse that is inherent in any policing technology. We conclude this report with model legislation that achieves these aims.

About Us

The Manhattan Institute is a community of scholars, journalists, activists, and civic leaders committed to advancing economic opportunity, individual liberty, and the rule of law in America and its great cities.

Introduction

Many Americans have become scared of Automatic License Plate Readers (ALPRs). In the past several months, a social media panic over the cameras produced by Flock Safety—the nation’s largest ALPR distributor—has provoked real life consequences. Polling consistently finds Americans now unfavorable toward the cameras, a reversal from just a year ago.¹ Hundreds of ALPRs have been torn down, vandalized, or otherwise destroyed in a vigilante campaign that has enjoyed tacit support from some even in the mainstream commentariat.² Most pertinently, policymakers are reacting by endorsing effective bans on the technology. That includes gubernatorial action to limit their use in Texas and Florida and federal legislation introduced or promised that would effectively ban federal funding recipients from using ALPRs.³

While the backlash has often been emotional, people of good will have reasonable questions about this policing technology. Some are concerned by the specter of a mass-surveillance state, in contravention of the Fourth Amendment and posing a fundamental threat to our privacy. Others fear the risks of abuse, from police officers stalking ex-girlfriends to the use of ALPRs to enforce a future pandemic lockdown.

While we understand these concerns, we think that the reaction—bans and acts of property destruction—is unmerited. Far from how they have been depicted in the media and by some politicians, ALPRs are a valuable tool of the modern police force, one that has been in use for decades. Far from a dragnet, they are usually a targeted means to keep people safe. Moreover, where there are valid concerns, prudent regulation—a template for which we lay out in this report—is the better way forward than bans.

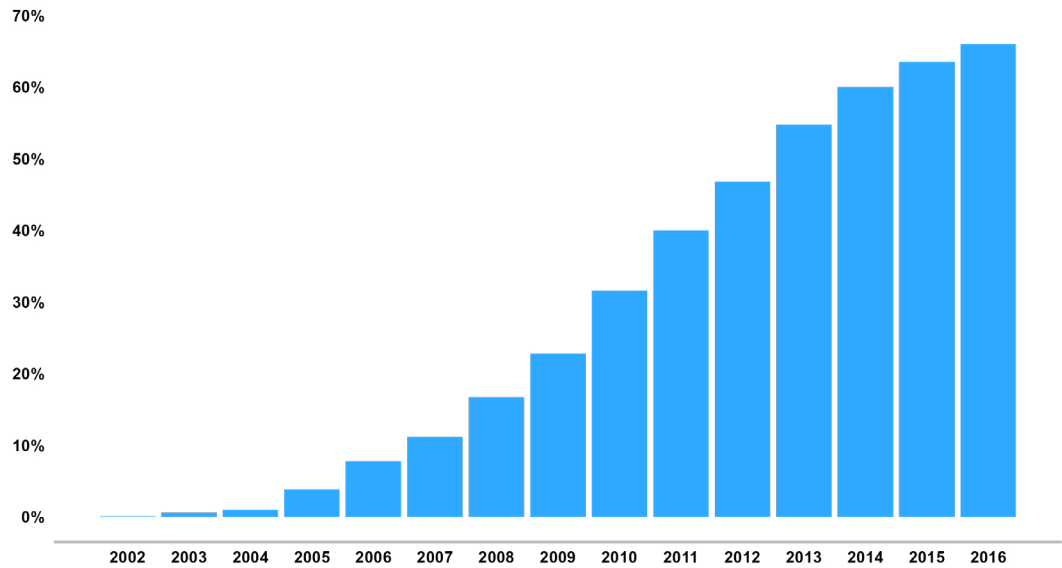
What Are ALPRs? History and Background

Automated License Plate Readers (ALPRs) are computer-connected cameras utilized by law enforcement agencies to recognize and thereby assist with the location of vehicles of interest. Early versions of these cameras were capable of scanning dozens of vehicles at a time,⁴ reading their alpha-numeric license plates, and logging those reads in a database accessible by police. The technology inside ALPRs dates back to the mid-1970s, though American police departments did not begin to use them at significant levels until the early 2000s.⁵ In 2006, the NYPD began deploying mobile ALPRs mounted to police vehicles. Soon thereafter, the department, along with others around the country, began erecting fixed ALPRs, strategically placed at high-traffic intersections and key points of jurisdictional ingress and egress.

By 2010, nearly 40% of large police agencies (defined as those with at least 100 officers) were deploying ALPRs (**Figure 1**).⁶ By 2016, that share had risen to more than two-thirds.⁷

FIGURE 1

Two-thirds of large police agencies had adopted license plate readers by 2016
Cumulative Percentage of Police Agencies Adopting LPR, 2002–16



Note: Weighted estimates for agencies with 100+ officers (n=902).

Source: Cynthia Lum et al., “The Rapid Diffusion of License Plate Readers in US Law Enforcement Agencies,” Figure 3, *Policing: An International Journal* 42, no. 3 (2019): 376–93

The case for the technology’s integration into law enforcement operations was straightforward: In a mobile society, a significant share of crimes involve motor vehicles as either the object of the crime (as in the case of a stolen car) or as a tool of the criminals (e.g., a drive-by shooting). Police will often get descriptions of these vehicles from victims, witnesses, or standard surveillance cameras. But finding them—particularly in large, dense urban areas—can be a difficult task. ALPRs supplement human police—who are fallible and at risk of confusion—with more reliable and impartial information to act upon.

Police departments can place vehicles of interest on a “hot list” for ALPRs readers. That yields an alert if and when the vehicles in question are photographed by an ALPR. In addition to real-time alerts, the storage of information captured by ALPRs allows investigators to do post-hoc searches for vehicles of interest that were identified *after* a crime took place. Think, for example, of a detective investigating a recent shooting. That detective can log into an ALPR system to check what vehicles were scanned by cameras in the vicinity with the hope of developing a lead on a potential suspect.

Over the last decade, ALPRs have become—like most tech products—both cheaper and more advanced. Modern ALPRs can not only recognize alpha-numeric license plate characters, but can now also recognize, thanks to advancements in AI, a vehicle’s make, model, color, direction of travel, and any other distinctive features that would help identify the vehicle (e.g., bumper stickers, visible damage, etc.). This makes it possible to identify vehicles whose license plates might be switched out by savvy criminals seeking to avoid detection.

Police departments deploy ALPRs every day, often to help solve high-profile cases. For example, ALPRs are commonly used to help solve abductions, as in the case an Atlanta-area woman whose car was stolen with her two-year-old daughter in the backseat. With a description of the car and its license plate, the police were able to use license plate readers to begin searching for the vehicle, which allowed them to locate the car within 15 minutes, leading to the arrest of the kidnapper as well as the safe recovery of the toddler.⁸ ALPRs have also been used to apprehend abusers after the fact, as, for example, in the case of Juan Calo Lopez, an alleged illegal immigrant arrested in an ALPR-enabled traffic stop for engaging in a sexual relationship with an underage boy.⁹ The investigative benefits extend as well to violent crimes, like the murder of North Carolina teacher and coach Sheremy Dillard; her boyfriend and alleged killer was apprehended after fleeing the state thanks to an ALPR.¹⁰

ALPRs and Crime: Theory and Evidence

Do ALPRs help stop and solve crime? The above anecdotes suggest they do. One of the authors of this report (Lehman) maintains a database of over 1,700 news stories and court records covering the past six years and detailing times just one brand of ALPRs (Flock) has been used to help fight crime.¹¹ Still, data is not the plural of anecdote. What do we know about the effects of ALPRs on crime?

There are several ways, in theory, that ALPRs could reduce crime in the area of their deployment. First, they can act as a direct deterrent. If a would-be offender sees a camera in the place he would like to offend, then he is less likely to do so, all else equal. If a would-be offender knows that his car's location is likely to be recorded, he should be less likely to commit a crime using that car, all else equal.

Second, ALPRs can contribute to police officers' investigations of crime. An ALPR and the records it generates can help to identify a perpetrator both at the time of the offense and for some period afterward. That can, in turn, both lead to conviction—reducing crime through the incapacitation channel—and increase the certainty that future crime will result in punishment, further breeding deterrence.

This second channel is particularly important for many American police departments. American clearance rates—the proportion of reported crimes that result in arrest or other resolution—have steadily declined over the past six decades and are often compared unfavorably with other developed nations.¹² In 2025 departments nationwide cleared roughly half of all violent crimes and just 18 percent of all property crimes. That includes just 10.5 percent of motor vehicle thefts—the kind of offense ALPRs are most obviously likely to assist with.¹³

Does the evidence support the idea that ALPRs reduce crime on any or all of these channels? While the research base is still developing, the early indications generally point to “yes.”

As of this writing, there are three kinds of studies that provide insight into how fixed ALPRs work. The first is quasiexperimental research on the roll-out of ALPRs specifically: just one such study currently exists. The second is quasiexperimental research on the

effects of cameras generally: several studies exist, all supporting a beneficial effect on crime. The third is non-experimental research on ALPRs. This research is more mixed, but is reviewed below for completeness's sake.

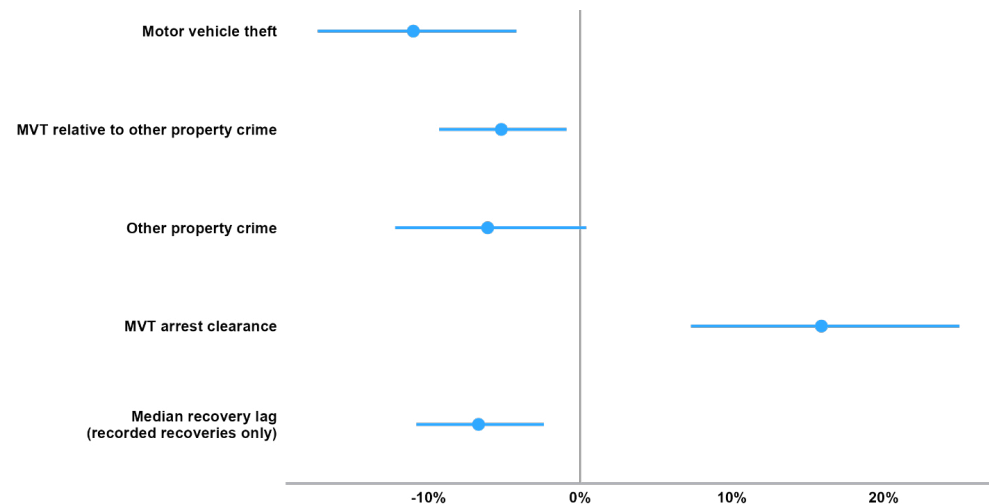
To date, the sole quasiexperimental study of fixed ALPRs is a working paper by University of South Carolina criminologists Ian Adams and Scott Mourtgos.¹⁴ They use data on the dates of deployment of Flock ALPRs in 216 police departments, merged with data on rates of motor vehicle theft and other property crimes reported under the FBI's National Incident Based Reporting System (NIBRS). They use these data in a staggered difference-in-difference specification, comparing departments with Flock at a given time to departments that either do not yet or never have Flock as a control group. In principle this design recovers the *causal* effect of ALPR deployment on crime rates. It also, the authors note, is almost certainly an underestimate of the true effect, as at least some of the control departments likely deployed non-Flock ALPRs during the period of study.

Their top line finding is that deployment of Flock's ALPRs reduces motor vehicle theft across adopters by 11 percent (**Figure 2**). Clearance rates for motor vehicle arrests rise by 16 percent. The authors identify a pre-trend for both outcomes in the months leading up to deployment, suggesting that at least some of the effect is attributable to other police activity or some other factor that also causes the deployment of ALPRs. But they corroborate the direction of their estimate of the total crime-reduction effect by showing a clean reduction in car thefts relative to other property crime offenses. While they find no significant change in the share of vehicles recovered, they do report that the median time to recovery declines about 7 percent conditional on any recovery occurring.

FIGURE 2

Effects of fixed ALPR deployment on vehicle theft outcomes

Percent change, months 0–12 after deployment vs. months –12 to –1, with 95% CIs.



Note: Figure shows percent change in months 0–12 after deployment vs. months –12 to –1, with 95% confidence limits.

Source: Scott M. Mourtgos and Ian T. Adams, “Working Paper: Automated License Plate Readers, Vehicle Theft, and Clearance,” Table 2, *CrimRxiv*, Aug. 16, 2026

In short, Adams and Mourtgos's study provides strong evidence that ALPRs reduce motor vehicle theft. It is unclear by which channel—deterrence or clearance—those effects obtain. But they certainly have those effects.

The second set of studies suggestive of ALPRs' benefits are those that provide quasiexperimental evidence on the effects of cameras generally. These studies are informative by analogy: license plate readers are a form of camera, and the effects of one should tell us something about the effects of the other. This is especially so insofar as either one works by being a visible deterrent. The analogy is less informative in the case of contributing to clearance: ALPRs almost certainly generate less information than security cameras generally, both because they only record information about vehicles and because they are only deployed on public thoroughfares.

At least four quasiexperimental studies speak to the effects of cameras in general on crime. All exploit the roll-out of cameras in their jurisdiction of interest, with all four finding that they reduce crime:

- Priks (2015) exploits the roll-out of surveillance cameras in the Stockholm subway system.¹⁵ He reports a 25 percent reduction in crime in city center subway stations, concentration among planned crimes like pickpocketing and robbery.
- Munyo and Rossi (2020) use the roll-out of surveillance cameras in Montevideo, Uruguay.¹⁶ They report a 20 percent reduction in crime in treated areas relative to a control group outside the city.
- Gómez, Mejiá, and Tobón (2021) study the roll-out of cameras in Medellín, Colombia.¹⁷ They find that camera deployment reduces overall crime in a treated area by 19 percent, property crimes by 17 percent, and violent crimes by 26 percent.
- Ma et al. (2026) study the roll-out of cameras in China.¹⁸ They estimate that doubling the number of cameras in a jurisdiction reduces crime by about 10 percent.

In sum, camera deployment is consistently associated with a reduction in crime in quasiexperimental specifications. While security cameras are not perfectly analogous to ALPRs, this evidence should increase our assumed likelihood that ALPRs also reduce crime.

Finally, there are several non-quasiexperimental studies of fixed ALPRs. These provide less useful evidence, but are reviewed here for comprehensiveness.¹⁹

- Wheeler and Phillips (2017) evaluate the deployment of vehicle-mounted ALPRs as temporary fixed ALPRs at road blocks in Buffalo, New York.²⁰ They match treated locations to locations with similar levels of crime using propensity score matching. Their results are highly sensitive to model specification, implying a reduction or increase in violent crime depending on model used. Their evaluation is of limited generalizability, as it focused on the temporary installation of fixed ALPRs in a small number of crime hot spots.
- Koper and Lum (2019) evaluate the deployment of a fixed ALPR network in Charlotte-Mecklenburg, North Carolina.²¹ They use survival analysis methods to estimate the likelihood of case closure before and after deployment of the ALPRs. They report improvements in the clearance rate for auto theft and robbery, especially in parts of the city with high rates of LPR concentrations.

However, these effects were highly sensitive to the inclusion of control variables. Moreover, the pre-post nature of the study limits the ability to make causal claims from it.

- Shjarback and Sarkos (2025) evaluate the deployment of fixed ALPRs monitoring the entrances and exits to Atlantic City, New Jersey.²² In the most useful specification, they compare observed trends in shootings, motor vehicle thefts, and property crime to the pre-intervention trend. All three crime types report a significant reduction. However, the use of the pre-trend to represent the counterfactual in which ALPRs were not deployed provides limited causal information, as the observed decline may be attributable to unobserved confounders.

As mentioned previously, the literature on ALPRs is still developing. More quasiexperimental research, using other data sets and covering longer periods of time, would contribute substantially to understanding of the technology's crime-fighting efficacy. Many outcomes, too, remain unexplored. The Shjarback and Sarkos analysis is suggestive of effects on certain kinds of violent crime, but more certainty requires stronger designs. There has also been no analysis whatsoever of the effects of fixed ALPRs on abductions—a key claimed benefit of the technology.

Still, the research such as it exists tends to point in the direction of ALPRs reducing crime. The role of social scientists is to reserve judgment for as long as and as comprehensively as possible. But policymakers need to make decisions before all evidentiary avenues have been explored. Given that, we think policymakers should be eager to learn more, but should feel comfortable acting on the assumption that ALPRs reduce crime given what we know so far.

One useful way to validate this intuition is through cost-benefit analysis. Modern ALPR systems are relatively cheap: Flock's ALPR cameras, for example, cost \$2,500 to \$3,000 per year (part of the reason for its widespread adoption).²³ Crime is an expensive proposition, to both the victim and the criminal justice system. A single motor vehicle theft, for example, costs the victim roughly \$10,000 and the criminal justice system another \$6,000 on average.²⁴ That implies five to six cameras pay for themselves, in social cost terms, simply by preventing a single motor vehicle theft. Reductions in violence or other property theft—while more speculative—would also almost certainly cover their own costs.

In other words: even if the case that ALPRs reduce crime is not ironclad, the case that they reduce crime is strong enough that, at current cost levels, their use is clearly justified. Policymakers can invest in ALPRs, comfortable in the knowledge that they are probably getting their money's worth.

ALPRs and the Fourth Amendment

While the pushback has intensified in recent months, civil libertarians have been registering their objections to the use of this technology by law enforcement for more than a decade. In 2012, the publication *Ars Technica* reported that a single company had by then sold some 35,000 ALPR units to law enforcement agencies throughout North America and the

United Kingdom. Many of those units were acquired by police departments in more than 100 American cities.²⁵ The article detailed, for example, the National Vehicle Location Service, which it described as “likely the largest single LPR database in the country, with over 550 million entries.” The proliferation of this technology by the early 2010s, *Ars Technica* noted, had drawn the ire of groups like the ACLU and Electronic Frontier Foundation, as well as that of local politicians—one of whom was quoted as asking, rhetorically, “Do we really want to live in a culture where the law-abiding movements of everyday citizens are tracked and accumulated in perpetuity?”

Those early critiques echo many of the concerns being voiced today. So too do the early legal challenges of the use of this technology by law enforcement mirror the legal debates continuing to play out in courts across the United States.

One major thread of criticism of ALPRs pertains to their risk to privacy, and threat to the freedoms guaranteed by the Fourth Amendment. Senator Rand Paul, for example, has repeatedly argued that Flock and similar products violate the Fourth Amendment, calling their deployment “unconstitutional.”²⁶ Yet courts have repeatedly rejected the argument that the deployment of ALPR networks, or the accessing of those networks for investigative purposes, violates the Fourth Amendment—and with good reason.

In constitutional challenges raised under the Fourth Amendment, the general standard against which courts have evaluated the state action in question is whether the individual or entity asserting a Fourth Amendment right has a reasonable expectation of privacy that the government invaded. Expectations of privacy are, for obvious reasons, diminished when out in public. “What a person knowingly exposes to the public, even in his own home or office,” the Supreme Court has held “is not a subject of Fourth Amendment protection.” That is especially so with respect to vehicles, in which any subjective privacy interests are “further diminished by the obviously public nature of automobile travel.”²⁷ In 1974, the Supreme Court expounded on this idea:

One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one’s residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.²⁸

In its 1983 decision in *U.S. v. Knotts*, the Supreme Court reiterated this principle, stating that, “A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.” The practical implications of this legal reality were further illustrated by the Supreme Court’s 2005 decision in *Illinois v. Caballes*, which held that “the use of a well-trained narcotics-detection dog” to sniff the outside of a vehicle during a traffic stop “generally does not implicate legitimate privacy interests,” and therefore, “does not rise to the level of a constitutionally cognizable infringement.”²⁹

These holdings do not constitute a blank check for the government to surveil citizens in public, however. In *U.S. v. Jones*, the Court ruled constitutionally infirm the government’s warrantless physical intrusion on a motor vehicle via the attachment of a GPS tracking device to the undercarriage of the defendant’s Jeep to track his movements over nearly a month.³⁰ The Court in *Jones* specifically declined to answer the question of whether continuously tracking a vehicle “through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy.” Six years later, the Court would rule in *Carpenter v. U.S.* that the government must obtain a warrant in order to acquire a criminal suspect’s cell site location information (CSLI), holding that by doing so, the

government invades a reasonable expectation of privacy “in the whole of [one’s] physical movements.”³¹ In that case, the government had acquired 127 days-worth of location data that catalogued nearly 13,000 location pings—over 100 points per day—though the Court held that the acquisition of just seven days of such data was enough to trigger the Fourth Amendment’s warrant requirement.

This is the backdrop against which the most recent ALPR-related cases to reach appellate courts have been litigated. So far, those courts have been unanimous in their rejection of constitutional challenges to the use of ALPR systems by police. In 2020, the Massachusetts Supreme Judicial Court ruled in *Commonwealth v. McCarthy* that “while [defendants have] a constitutionally protected expectation of privacy in the whole of [their] public movements,” referring to the standard articulated in *Carpenter*, “that interest is not invaded by the limited extent and use of ALPR data” involved in the case.³² The court in *McCarthy* did leave the door open to the possibility that a more pervasive camera network could cross the line drawn in *Carpenter*, noting that such a privacy interest “potentially could be implicated” at some point.

The court in *McCarthy* also went on to explain that even if a jurisdiction were to reach a point at which a warrant requirement would attach, the Fourth Amendment would not apply to other uses of ALPRs by law enforcement, including for the purposes of investigating a report of a stolen car, as “the driver of a stolen vehicle does not have a reasonable expectation of privacy in the location of someone else’s automobile.” That same year, the Ninth Circuit Court of Appeals in *U.S. v. Yang*,³³ rejected a defendant’s Fourth Amendment challenge to a postal inspector’s use of an ALPR database to locate him based on a finding that the defendant was not lawfully in possession of the vehicle in question.

In 2025 and 2026, two Virginia appellate courts upheld the use of the Flock ALPR system in Fourth Amendment cases—*Commonwealth v. Church* and *Commonwealth v. Robinson*. In *Church*,³⁴ the court distinguished the use of a Flock Safety database to identify the defendant’s vehicle from what the government did in the *Carpenter* case, reasoning that “the Flock system provides only short-term monitoring of a vehicle’s movements on public thoroughfares,” rather than “a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.” Similarly in *Robinson*,³⁵ the court found “that the use of the Flock system in this case is similar to *Knotts*, but significantly factually distinguishable from [] *Carpenter*,” noting in relevant part:

The 172 Flock cameras situated throughout Norfolk are not as intrusive as the cell towers in *Carpenter* that monitor the movement of cell phones both inside and outside of homes and buildings—or the surveillance of a city from the air in *Leaders of a Beautiful Struggle*. The images captured by the Flock cameras are of vehicles, not persons, and the only pieces of information collected—license plates and physical characteristics of the vehicle—are already publicly viewable to anyone who sees the vehicle on the street. The search of the Flock system yielded a photo of Robinson’s car as it passed down a public highway. The cameras did not continuously monitor all of his travels around the city and did not create an “intimate window” of Robinson’s overall movements and associations.

A Washington state appellate court reached the same conclusion for similar reasons in *State v. Simonson* earlier this year. In that case, the court found “uncompelling Simonson’s comparison of Flock photographs to GPS monitoring or cellular phone data from towers.”³⁶

This unanimity across both federal and state appellate courts during this decade is noteworthy, and at least suggestive of a lower likelihood of a future finding of constitutional infirmity. That suggestion is reinforced by the fact that earlier challenges to the use of ALPRs were similarly unsuccessful. These include:

- the Ninth Circuit’s 2014 decision in *Green v. San Francisco*, in which the court rejected a challenge to a stop based on what turned out to be a false-positive generated by the city’s ALPR system;³⁷ and
- the Sixth Circuit’s 2005 opinion in *U.S. v. Ellison*, in which the court upheld the use of a license plate database to discover a criminal warrant, holding that “using a license plate number — in which there is no expectation of privacy — to retrieve other non-private information” *does not* “somehow create[] a ‘search’ for the purposes of the Fourth Amendment.”³⁸

Some critics of ALPRs have suggested that the Supreme Court’s 2026 decision in *Chatrie v. U.S.* may change how courts treat ALPR networks in the future. *Chatrie* extended the holding in *Carpenter*, which dealt with cell site location information, to historical geographic location data. In an opinion delivered by Justice Elena Kagan, the Court held the acquisition of historical geographic location data to constitute a search under the Fourth Amendment (remanding to the lower court the question of whether the peculiar geofence warrant relied on by the government rendered the search reasonable). The Court seemed to be especially compelled by the similarities of the data at issue in *Chatrie* to the CSLI at issue in *Carpenter*, writing that:

The resemblances between CSLI and Location History, in their relationship to personal privacy, practically leap off the page. Everything *Carpenter* relied on to find that law enforcement officers conducted a Fourth Amendment search when they accessed wireless carriers’ CSLI records applies as well or better to the police’s accessing of Google’s Location History data.³⁹

Fourth Amendment scholar and Stanford University law professor Orin Kerr recently gave a thorough overview of his impressions of how *Chatrie* might change Fourth Amendment analyses moving forward in a forthcoming *Notre Dame Law Review* article.⁴⁰ Among other notable observations that this report does not address, Kerr suggests—rightly, we think—that the Court in *Chatrie*:

effectively drops the notion of the relevant expectation of privacy being in the “whole” of a person’s movement. Instead, the new expectation of privacy seems to be in any records of a person’s physical location using certain kinds of technology that are *capable* of being used to engage in large-scale tracking. It’s the *capacity* to easily obtain the whole of a person’s physical movements, not actually obtaining the whole of a person’s physical movements, that seems to make accessing the records a search.⁴¹ (emphases added)

What’s unclear, however, is whether this shift from the Fourth Amendment focusing on the scope of the data obtained to focusing on the technological capacity of the system obtaining the data makes it more or less likely that challenges to modern ALPR systems will be found to implicate the Fourth Amendment by future courts. Even less clear is whether modern, networked ALPR systems are in fact *capable* of capturing the whole of one’s movements, even over a short period of time. It is worth noting on this point that the Court in *Chatrie* took specific note of the facts that, in *Carpenter*, the CSLI at issue logged the defendant’s location “an average of 101 times a day,” and that the location data before the Court in *Chatrie* “records a person’s location every two minutes.” ALPR networks are currently incapable of collecting data with this degree of granularity, which could prove dispositive in future challenges.

Even in jurisdictions with relatively expansive ALPR coverage, the overwhelming majority of road space falls outside the sight picture of a network of standard ALPRs. Start with the fact that the stationary ALPR cameras made by the most popular provider of these products as of this writing—Flock Safety—have a sight picture that is approximately 75' x 20' (or 1,500 SqFt).⁴² In essence, this amounts to 1.5 standard traffic lanes over a 75-foot distance. By comparison, there are roughly 4.2 million miles of roadway in the United States.⁴³

Nor are ALPRs particularly dense in cities where they are deployed. Consider the city of Houston, Texas, which had, according to a June 2024 *Houston Chronicle* report, more than 3,800 ALPR cameras operating within the city.⁴⁴ The city, according to Houston Public Works,⁴⁵ has approximately 16,000 lane miles within its limits, which amounts to just over one billion square feet of roadway—not including highways maintained by the state and county but within the city limits. Assuming the city is currently operating 4,000 ALPR cameras with 75' x 20' sight pictures, those cameras cannot see more than six million square feet—less than one percent of the total square footage of Houston's roadways.

Even if a future court were to rule the use of modern ALPRs a search under the Fourth Amendment, it remains the case that there will be many applications for the technology that fall within the well-established exceptions to the Fourth Amendment's warrant requirement or outside the Fourth Amendment's scope entirely. The Ninth Circuit's decision in *Yang* already constitutes an example of the latter, insofar as it reiterates the principle that car thieves cannot claim a privacy interest in vehicles that they do not rightfully possess. There are also the hot pursuit and exigency exceptions that would likely apply to the use of ALPRs to (a) help track vehicles in the act of fleeing from police as well as (b) to find an abducted child, as in the car theft case described in the section above.

Why and How to Regulate ALPRs

To the extent law enforcement's utilization of modern ALPR systems remains constitutionally permissible, the debate about the propriety of police utilization of modern ALPR systems shifts to one of costs and benefits. As discussed above, the benefits of modern ALPR systems are clear.

But as with any other law enforcement tool, with access comes the risk of misuse and abuse. This risk is not unique to ALPRs,⁴⁶ but the tenor of the current debate suggests that the public finds such cases especially concerning. In general, there are four types of concerns we think worth addressing.

One is fear of "mass" or "dragnet" surveillance—a fear we think unmerited based on the foregoing analysis.

The second is a fear of more specific surveillance of places with a strong interest in privacy. Some have pointed, for example, to police surveillance of churches during Covid lockdowns, worrying that ALPRs would enhance potential abuses of the First Amendment right to worship. Others might be concerned about privacy in their medical or voting decisions.

The third concern is a fear of abuse. The press has documented dozens of stories of police officers fired or arrested for misusing ALPRs, especially to keep tabs on ex-girlfriends, ex-wives, and others. We think these cases objectively rare—one of us (Lehman) has estimated that the officers identified engaging in any misconduct (not just stalking, but other objectionable behaviors as well) make up less than half a percent of officers in their departments.⁴⁷ And many of these stories often represent success at detecting abusers using auditing technology—implying that their other misconduct would have gone unnoticed absent modern policing tech. Nonetheless, police misconduct, no matter how rare, is never acceptable; those who engage in it should face the full brunt of possible sanctions.

The fourth concern we might term petty use of ALPRs. Some worry that, far from being used as a major-crime fighting tool, more ALPRs will be used primarily to harass the law-abiding public, through petty traffic enforcement or the overcriminalization of day-to-day activities. Such fears are generally based on anecdotes, rather than systematic evidence. Still, we agree that police ALPRs should be reserved for serious crimes, especially because using them for petty matters risks further undermining their public legitimacy.

Firms like Flock have recently taken steps to try to impose some of these protections on departments unilaterally. While this is a nice signal, the correct venue for such policy change is ultimately government itself. Some changes need to be a matter of departmental policy. Others should be taken up by state legislature, which can impose by law what a company like Flock can ultimately only attempt to do.

For policymakers, weighing the costs and benefits of ALPRs technology does not require costs to be treated as fixed and unmalleable. Indeed, costs can be reduced and risks mitigated through targeted regulation. What follows are recommendations for policy makers aimed at reducing the potential harms associated with government access to modern ALPR systems while preserving the benefits of the technology's deployment in the policing context.

- **Logging requirements:** Departments using ALPR databases should be required to log all access to the database, with individual user IDs so that auditors can review who did what when. Access should also require case codes, with a requirement that officers clearly articulate the reason for the query—providing detailed specifics, not a general explanation—at the time of access.
- **Supervisory approval:** Access to ALPR databases should require written and logged approval from a supervisor for any non-investigator queries that are not related to crimes in progress;⁴⁸ and for any personnel not on duty when the query was made.⁴⁹
- **Data retention limits:** To protect privacy, ALPR databases should retain recorded images and associated data for no more than 30 days, except for cases involving ongoing prosecution or criminal investigation with supervisory approval.
- **Audits:** In addition to making use of automated abuse/misuse flags offered by providers, audits of ALPR databases departments should conduct on a quarterly basis. Audits should cover both system efficacy and evidence of abuse. Results should be made available to the public in a summary form on an annual basis.
- **Criminal penalties and exclusion:** Abuse of an ALPR system—misusing it for unofficial purposes in the name of personal gain or harm to another—should carry stiff criminal penalties as well as exclusion from future police employment. ALPR data obtained in violation of any of these regulations should not be admissible in a court.

- **Major crime investigation restriction:** Investigative use should be restricted to offenses involving violent felonies, thefts, burglaries, arsons, gun offenses, drug offenses, hit-and-runs, or kidnappings/abductions (not to cover emergency circumstances and BOLO/hot list requests). Under no circumstances should police-operated ALPRs be used to issue fines, or other penalties for non-felony speed enforcement, parking violations, and other non-red-light-related moving violations.
- **Sensitive places:** ALPRs should be prohibited within 100 feet of any place of worship, polling place, or medical facility without the permission of the owner or operator of aforesaid location. ALPR databases should not be permitted to retain images that include a significant portion of the interior of a private residence or other establishment.

These steps, we think, address the legitimate concerns some Americans have about ALPRs without, pivotally, getting rid of the technology or severely curtailing their crime-fighting efficacy. The reality is that abuse of ALPRs is relatively rare, while their ability to solve and reduce crime is clear in both the academic literature and in the hundreds of reports from police departments and local news. With smart regulation, we feel assured that Americans can be kept safe both from potential misuse of ALPRs and from the criminals that they regularly help apprehend.

Model Legislation

A Bill

To ensure the responsible use of automated license plate reader (ALPR) systems by law enforcement actors to protect the public and control crime, to prohibit the use of ALPRs to enforce certain traffic-related violations, and to establish penalties for the abuse and misuse of ALPRs by state actors.

SECTION I. System Access and Use Restrictions.

1. **Personnel Limits.** State, county, or municipal government employee access to any automated license plate reader (ALPR) system shall be limited to employees of police agencies, sheriff's offices, city and county prosecuting attorneys' offices, and the office of the Attorney General.
2. **Supervisor Approval Requirement.** Law enforcement agencies shall adopt, maintain, and enforce an administrative procedure for conditioning historical queries of ALPR databases by
 - a. non-investigators, except as to crimes in progress, and
 - b. agency employees not on duty at the time of the query,
 on supervisor approval, which shall be documented in auditable logs.
 - i. The covered entity shall, prior to its deployment of an ALPR system, adopt administrative policies and procedures regarding supervisory approval for the uses outlined in this subsection.



3. ***Limits on Enforcement Type.*** ALPR cameras shall not be relied on as a basis for the issuance of fines or other civil or criminal penalties for
 - a. Parking violations;
 - b. Non-felony speeding violations; or
 - c. any minor traffic infraction relating to the function, registration, or outward appearance of a vehicle, including, but not limited to
 - i. window tints,
 - ii. tail, break, or indicator lights,
 - iii. exhaust types, and
 - iv. decorative flair.
4. ***Sensitive Location Restrictions.*** ALPRs shall not be placed within 100 feet of an entrance to, or exit from
 - a. A hospital;
 - b. A church, temple, mosque, or other house of religious worship; or
 - c. polling place.
5. ***Data Retention Limits.*** Images recorded by an ALPR camera that are unrelated to an active criminal investigation or prosecution may not be stored in a database for longer than 30 days.
6. ***Exceptions.***
 - a. State government employees outside of the entities listed in subsection (1) may be granted access by such an entity after receiving the express written approval of the Attorney General or a member of that office vested by the Attorney General with the authority to grant such approvals;
 - b. ALPRs may be placed within 100 feet of the locations enumerated in subsection (4)(a)-(b) if the agency in question has received the express written permission of the owners or owners agents of privately owned locations within those categories, which permission may be revoked at any time requiring the prompt disabling or removal of the ALPR cameras in question within 10 business days of the revocation of permission.

SECTION II. Logging and Audit Requirements.

1. ***User Identification.*** Every employee granted access to an ALPR system pursuant to subsections (1) and (6)(a) of SECTION I of this Act shall be issued a unique ID to access such a system by the entity that employs them.
2. ***Data Log Requirement.*** All entities listed in subsection (1) of SECTION I of this Act shall maintain a running log of every query and “hot-list” addition or subtraction.
3. ***Documentation of searches.*** All queries and “hot-list” additions or subtractions shall be accompanied by an explanation of the reason for the query or other action that shall be included in the logs. (a) Providing a false explanation for the query shall be a Class A misdemeanor, punishable in accordance with SECTION III (1)(b) of this Act.



4. **Log retention.** All logs of historical queries maintained pursuant to this section shall be maintained for the duration of the contract with the ALPR provider, plus one-year.
5. **Audits.** To ensure that ALPR systems are not being misused or abused, any entity covered by SECTION I of this Act which makes use of an ALPR system shall conduct regular audits of a selected sample of ALPR system queries at least once every fiscal quarter, and shall adopt administrative policies and procedures for such audits prior to their deployment of an ALPR system.

SECTION III. Prohibitions and Penalties.

1. Misuse and Abuse—Prohibition and Penalties.

- a. Unauthorized use of an ALPR system is defined as the unauthorized—for personal or other reasons unrelated to the user's official duties—
 - i. historical query of an ALPR system, or
 - ii. addition or subtraction of a vehicle to or from an ALPR system “hot list” by an employee of any entity covered by SECTION I of this Act, or
 - iii. the facilitation by such employee of the unauthorized use of an ALPR system by any other.
- b. Unauthorized use of an ALPR system shall constitute a Class A misdemeanor punishable by a fine not to exceed \$10,000, and/or a sentence not to exceed 60 days in jail.
- c. Five or more unauthorized uses of an ALPR system by a single employee of an entity covered by SECTION I of this Act shall constitute a Class D felony, punishable by a fine not to exceed \$50,000, and/or a term of imprisonment not to exceed 13 months.

SECTION IV. Definitions.

1. **Terms Defined.** When applying this Act, the following terms shall have the following meanings, which shall not be overridden by the definitions of similar terms set forth in other sections of the laws of {insert state}:
 - a. ALPR System is a system that utilizes a network of cameras primarily used to photograph and identify vehicles by their license plates or other visible features.
 - b. Hot-List refers to an ALPR system feature through which specific vehicles can be flagged as stolen, wanted, or of specific interest so that they generate an alert whenever photographed by an ALPR camera.
 - c. Hot-List Addition or Subtraction refers to the addition or removal of a specific vehicle or license plate to or from the hot-list.

About the Authors



Charles Fain Lehman is a senior fellow at the Manhattan Institute and senior editor of *City Journal*. He focuses primarily on the public policy of antisocial behavior, including issues of crime, drugs, and public disorder. His work has appeared in outlets including the *New York Times*, *Atlantic*, *Wall Street Journal*, and *National Review*. He has discussed policy issues before the Senate, House of Representatives, and the U.S. Commission on Civil Rights. Prior to joining the Manhattan Institute in 2021, Charles was a staff writer at the Washington Free Beacon. Charles is originally from Pittsburgh, Pennsylvania, and now lives outside Washington, D.C., with his wife and sons.



Rafael Mangual is the Nick Ohnell Fellow at the Manhattan Institute, a contributing editor of *City Journal*, and a member of the Council on Criminal Justice. His first book, *Criminal (In)Justice*, was released in July 2022. He has authored and coauthored a number of MI reports and op-eds on issues ranging from urban crime and jail violence to broader matters of criminal and civil justice reform. His work has been featured and mentioned in a wide array of publications, including the *Wall Street Journal*, *The Atlantic*, *New York Post*, *The New York Times*, *The Washington Post*, *Philadelphia Inquirer* and *City Journal*. Mangual also regularly appears on Fox News and has made a number of national and local television and radio appearances on outlets such as C-SPAN and Bloomberg Radio. In 2025, he was appointed to serve a second term as a member of the New York State Advisory Committee of the U.S. Commission on Civil Rights.

Prior to joining MI in 2015, Rafael worked in corporate communications for the International Trademark Association. He holds a B.A. in corporate communications from the City University of New York's Baruch College and a J.D. from DePaul University in Chicago, where he was president of the Federalist Society and vice president of the Appellate Moot Court team. After graduating from law school, Mangual was inducted into the Order of the Barristers, a national honor society for excellence in oral and written advocacy.

Endnotes

- ¹ Drew Harwell et al., “Americans Have Turned Against Police Cameras That Track License Plates, New Survey Shows,” *Washington Post*, Aug. 28, 2026; “Polling on Flock Cameras (August 2026),” Data for Progress, Aug. 27, 2026.
- ² NlckySolutions, “FlockStats: Flock Camera Destruction Tracker,” accessed Sept. 3, 2026; J.D. Tuccille, “Surveillance Camera Saboteurs Are Getting Government Officials’ Attention,” *Reason*, Aug. 26, 2026.
- ³ Ayden Runnels, “Gov. Abbott Blocks State Agencies from Spending Money on Flock Cameras,” *Texas Tribune*, Aug. 28, 2026; Kathryn Varn, “After DeSantis Order, Florida Police Drop Flock Cameras—but Not in Tampa Bay,” *Axios Tampa Bay*, Sept. 1, 2026; “Reps. Massie, Burlison Introduce the ‘Flock-Off Act’ to Defund Surveillance State Cameras,” press release, Office of Rep. Thomas Massie, Sept. 2, 2026; Sharon Zhang, “Sanders Vows to Introduce Legislation to Stop Flock’s ‘AI Mass Surveillance,’” *Truthout*, Aug. 27, 2026.
- ⁴ Cyrus Farivar, “Your Car, Tracked: The Rapid Rise of License Plate Readers,” *Ars Technica*, Sept. 27, 2012.
- ⁵ Kristin Finklea, *Law Enforcement and Technology: Use of Automated License Plate Readers*, CRS Report R48160 (Washington, DC: Congressional Research Service, Aug. 19, 2024).
- ⁶ Cynthia Lum et al., *License Plate Recognition Technology (LPR): Impact Evaluation and Community Assessment* (Fairfax, VA: Center for Evidence-Based Crime Policy, George Mason University, September 2010), 18.
- ⁷ Cynthia Lum et al., “The Rapid Diffusion of License Plate Readers in US Law Enforcement Agencies,” *Policing: An International Journal* 42, no. 3 (2019): 376–93.
- ⁸ Stepheny Price, “HEAR IT: Mom’s Frantic 911 Call after Thief Steals Instacart Driver’s Car with Toddler Inside,” *Fox News*, Aug. 3, 2026.
- ⁹ WJHG Newsroom, “BCSO Arrests Suspect Accused of Abuse of a Minor,” WJHG, Aug. 25, 2026.
- ¹⁰ “Details Emerge from Out-of-State Capture of Man Charged in Wake County Coach’s Death,” ABC11 (WTVD), Aug. 19, 2026.
- ¹¹ Charles Fain Lehman, “Flock Crime Prevention Tracker,” accessed Sept. 3, 2026.
- ¹² Philip J. Cook and Ashley Mancik, “The Sixty-Year Trajectory of Homicide Clearance Rates: Toward a Better Understanding of the Great Decline,” *Annual Review of Criminology* 7 (2024): 59–83; Rachel Schilke, “Half of US Homicides Go Unsolved, Ranking Last among Western Nations,” *Washington Examiner*, March 6, 2023.
- ¹³ Federal Bureau of Investigation, *Crime in the United States*, 2025.

- 14 Scott M. Mourtgos and Ian T. Adams, “Working Paper: Automated License Plate Readers, Vehicle Theft, and Clearance,” CrimRxiv, August 16, 2026.
- 15 Mikael Priks, “The Effects of Surveillance Cameras on Crime: Evidence from the Stockholm Subway,” *Economic Journal* 125, no. 588 (2015): 289–305,.
- 16 Ignacio Munyo and Martín A. Rossi, “Police-Monitored Cameras and Crime,” *Scandinavian Journal of Economics* 122, no. 3 (2020): 1027–44.
- 17 Santiago Gómez, Daniel Mejía, and Santiago Tobón, “The Deterrent Effect of Surveillance Cameras on Crime,” *Journal of Policy Analysis and Management* 40, no. 2 (2021): 553–71.
- 18 Hong Ma et al., “Keeping an Eye on the Villain: Assessing the Impact of Surveillance Cameras on Crime,” *Journal of Development Economics* 178 (2026); working paper version at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4937339.
- 19 We omit two randomized controlled trials—Lum et al. 2011 and Koper, Taylor, and Woods 2013—because they focus on mobile ALPRs, use outdated technology, and are interested only in the effects on hot spots. We also omit the studies published by Flock itself, both the provenance and methods of which render them uninformative.
- 20 Andrew P. Wheeler and Scott W. Phillips, “A Quasi-Experimental Evaluation Using Roadblocks and Automatic License Plate Readers to Reduce Crime in Buffalo, NY,” *Security Journal* 31, no. 1 (2018): 190–207.
- 21 Christopher S. Koper and Cynthia Lum, “The Impacts of Large-Scale License Plate Reader Deployment on Criminal Investigations,” *Police Quarterly* 22, no. 3 (2019): 305–29.
- 22 John A. Shjarback and James A. Sarkos, “An Evaluation of a Major Expansion in Automated License Plate Reader (ALPR) Technology,” *Justice Evaluation Journal* 8, no. 2 (2025): 225–42.
- 23 Ned Donovan, “A Cop’s Case for Flock,” *Works in Progress*, 2026; City of Campbell, “How Much Does a Flock Safety Camera Cost?” FAQ, accessed Sept. 3, 2026.
- 24 Kathryn E. McCollister, Michael T. French, and Hai Fang, “The Cost of Crime to Society: New Crime-Specific Estimates for Policy and Program Evaluation,” *Drug and Alcohol Dependence* 108, nos. 1–2 (2010): 98–109, adjusted for inflation.
- 25 Farivar, “Your Car, Tracked.”
- 26 Rand Paul (@RandPaul), X post, August 28, 2026,; Rand Paul (@RandPaul), X post, August 30, 2026.
- 27 *South Dakota v. Opperman*, 428 U.S. 364 (1976).
- 28 *Cardwell v. Lewis*, 417 U.S. 583 (1974).
- 29 *Illinois v. Caballes*, 543 U.S. 405 (2005).
- 30 *United States v. Jones*, 565 U.S. 400 (2012),.

- 31 *Carpenter v. United States*, 585 U.S. 296 (2018).
- 32 *Commonwealth v. McCarthy*, 484 Mass. 493 (2020).
- 33 *United States v. Yang*, 958 F.3d 851 (9th Cir. 2020).
- 34 *Commonwealth v. Church*, No. 0737-25-1 (Va. Ct. App. Oct. 14, 2025).
- 35 *Robinson v. Commonwealth*, No. 1912-24-1 (Va. Ct. App. Apr. 7, 2026).
- 36 *State v. Simonson*, No. 40732-2-III (Wash. Ct. App. Jan. 29, 2026) (unpublished).
- 37 *Green v. City & County of San Francisco*, 751 F.3d 1039 (9th Cir. 2014).
- 38 *United States v. Ellison*, 462 F.3d 557 (6th Cir. 2006).
- 39 *Chatrie v. United States*, 609 U.S. ____ (2026), slip op. at 16.
- 40 Orin S. Kerr, “The Fourth Amendment after Chatrie,” *Notre Dame Law Review* 101 (forthcoming).
- 41 *Ibid.*
- 42 Flock Safety, “FAQ,” accessed Sept. 3, 2026.
- 43 Bureau of Transportation Statistics, “U.S. Public Road and Street Mileage by Functional System,” accessed Sept. 3, 2026.
- 44 “Houston Leads Nation in License Plate Cameras amid Police Staff Shortages,” *Government Technology Insider*, June 6, 2024..
- 45 Houston Public Works, “Transportation & Drainage,” accessed Sept. 3, 2026..
- 46 See, e.g., Sadie Gurman and Eric Tucker, “Across US, Police Officers Abuse Confidential Databases,” Associated Press, Sept. 27, 2016. (“[T]he AP, through records requests to state agencies and big-city police departments, found law enforcement officers and employees who misused databases were fired, suspended or resigned more than 325 times between 2013 and 2015. They received reprimands, counseling or lesser discipline in more than 250 instances, the review found.”).
- 47 Charles Fain Lehman, “Stop Freaking Out about Flock,” *City Journal*, Sept. 2, 2026.
- 48 For example, a police officer running a query looking at past hits on a vehicle in relation to a report taken on a burglary that occurred the day before.
- 49 This would prohibit, for example, a police department employee whose shift ended at 4 p.m. accessing the database to run a query at 7 p.m.