Automated License Plate Readers: A Roadmap for Regulation

Policing Project
NYU School of Law

Introduction

Across the country, policing agencies are adopting automated license plate readers, or "ALPRs." ALPRs are camera-based devices which capture and store license plate numbers and other information about passing vehicles, along with the location and time. This data, once collected, can be used to track individuals and monitor their movements. Some vendors claim that their ALPR systems also can identify associations between individuals, and even detect criminal activity.

The use of ALPRs by police can have significant implications for civil rights and civil liberties. Potential risks resulting from ALPR use include incursions upon privacy, overenforcement of low-level offenses, and false positive alerts leading to unwarranted police contact. It is imperative that if lawmakers approve the purchase

and use of ALPRs, they enact robust regulation to help mitigate the potential ethical risks.

The purpose of this document is to offer guidance to state and local policymakers who are deciding (a) whether to authorize police to use ALPRs and, (b) if so, on what terms.

- Part 1 gives a brief overview of ALPR technology and discusses the potential benefits and costs. A more detailed discussion on the benefits and costs of ALPRs can be found in our report on ALPRs.
- Part 2 discusses potential regulatory strategies for jurisdictions choosing to authorize police use of ALPRs, including suggested legislative language regarding the use, retention, and sharing of ALPR data. Several of these provisions have been adapted from our comprehensive model ALPR statute.

  Although most of the guidance in this Part applies to ALPRs generally, some provisions are specific to ALPRs produced by the vendor Flock Safety. We offer this vendor-specific guidance because Flock differentiates itself from other ALPR vendors in important ways, including the fact that Flock markets its products to private entities (such as homeowner associations), which in turn share their ALPR data with police. As discussed below, this private-public data-sharing has critical implications for democratic accountability around police use of ALPRs. More information about police use of privately-owned surveillance can be found in our model lateral surveillance statute.

In developing this policy guide, the Policing Project engaged with a wide range of stakeholders, including law enforcement and civil society groups. We also engaged with personnel from the ALPR vendor Flock Safety, who provided us with some of the information included in this guide, and to whom we offered feedback on Flock's products and services in line with the recommendations set forth below.

Part 1: ALPRs, their benefits, and their costs

ALPRs are camera-based devices which capture and store license plate numbers and other information about passing vehicles, along with the location and time. Originally, ALPRs only collected license plate information. Today they can be used to locate, identify, and track vehicles based on features such as make, model, and color. Given the rapid advances in ALPR technology, it might be more accurate to call them by some other name, such as Vehicle Tracking Technology. For this guide, however, we will continue to call them ALPRs.

Generally, police use ALPRs in three ways:

- ***Hotlists.*** ALPRs can compare passing license plates to a database of sought-after plates called a "hotlist." For example, the National Crime Information Center maintains several hotlists, including ones related to stolen vehicles, missing persons, fugitives, and those wanted for immigration violations. When an ALPR detects a vehicle on a hotlist, police are notified in real-time.

- ***Historical data.*** ALPRs can store the data they collect (such as license plate numbers, vehicle characteristics, and the location and time of the scan) in a database. This "historical data" can later be searched by police. For example, police might search for the plate of a known vehicle to see where it has been detected over time. Police can also search historical data to help identify an unknown vehicle — for example, a search for vehicles matching a witness's description (e.g., a "yellow Ford truck") so as to identify the license plate or the location of the vehicle at various times.

- ***Analytics.*** Finally, vendors are developing a variety of novel analytics using captured ALPR data. For example, some vendors claim that their ALPRs can detect when vehicles are engaged in "casing activity." A feature known as "convoy analysis" is said to identify associations between vehicles (this feature is discussed in greater detail below). Some agencies have deployed ALPR systems claiming to be able to identify suspicious vehicle movements, such as those purportedly associated with drug trafficking.

Benefits. Proponents of ALPRs claim that these tools can help police solve past crimes and deter future ones. Some vendors claim that their products can help reduce crime by as much as 70%. There are a number of anecdotal examples of police using ALPRs to generate leads and resolve cases. It is likely the case that, as with any surveillance technology, the information collected, retained and used could help aid with investigations.

Despite this, the true value of ALPRs is largely unknown. Rarely are vendor claims about ALPR efficacy vetted by independent researchers and, to date, there has been little systematic study of the use and efficacy of ALPRs. Indeed, a recent review of the relevant literature concluded that "[d]espite their spread, the evidence base for the effectiveness of ALPRs is extremely limited." This is not to state that ALPRs provide no public safety benefit — rather, it is to say that much is still unknown, and policymakers should take with a grain of salt any claims made about the crime-fighting benefits of these tools. As discussed below, there is even less evidence supporting the efficacy of many ALPR analytics. It is understandable to latch on to any solutions, including technological ones, in addressing serious crime. But before adopting such technologies, it is important to have clear evidence of benefits.

Costs. Policymakers should consider not only the potential benefits of ALPRs, but also the potential costs, which are detailed in brief below. As with the benefits, the magnitude of these costs is uncertain, and more study is needed.

- ***Privacy:*** ALPRs enable police to collect and store data about our location and movements as we go about our daily lives, with profound implications for privacy. This location data can reveal a wealth of sensitive information — from where we pray or seek healthcare to the people with whom we associate. As ALPRs are enhanced with new AI-enabled features, the capacity to use this technology in ways that limit our privacy increases.
- ***Over and counterproductive policing:*** Some agencies use ALPRs to pull over individuals with warrants or license suspensions resulting from unpaid fines and fees, which can have a devastating impact on individuals unable to make the payments. Indeed, some courts have held that automatic suspensions of licenses for failure to pay fines and fees are unconstitutional. Additionally, the use of ALPRs to enforce low-level, non-violent offenses (which often are disproportionately enforced against marginalized populations) can diminish trust in law enforcement without corresponding public safety benefits.

- ***Misuse:*** ALPRs, like all surveillance technologies, carry the potential for misuse. There are documented cases in which police have used access to law enforcement databases for personal reasons — such as checking on a romantic partner. There also are cases in which police have used ALPRs in ways that violate applicable law — for example, police sharing ALPR data with immigration enforcement agencies in violation of state and local sanctuary laws.
- ***False alerts:*** There are several documented cases in which ALPRs have led to wrongful stops; this has resulted in innocent individuals being arrested and even held at gunpoint. One jurisdiction recently settled a lawsuit over such a wrongful stop for $1.9 million.
- ***Equity:*** Police-owned surveillance technologies often are deployed disproportionately in communities of color and lower socioeconomic status. In fairness, these often are the communities that have the most crime; but disproportionate placement inevitably is going to lead to disproportionate enforcement. At the same time, privately-owned ALPRs often are found in wealthier areas, turned against (among others) those performing labor in those communities.
- ***Transparency:*** For the above reasons, and for others, it is essential that police be fully transparent about their use of ALPRs, including siting decisions. Nonetheless, agencies often refuse to disclose where or even whether they deploy ALPRs, how much data they collect and how long they retain it, and what offenses they use ALPR data to investigate. This is unfortunate because, at our urging, technology companies such as Flock and others have built dashboards that can display this information to the public easily.

In light of the benefits and costs, the decision whether to authorize police to deploy ALPRs is one that should be made with great care and only after meaningful engagement with the public. For those jurisdictions that do choose to authorize ALPR use, it is essential that robust regulation be enacted to minimize potential harms to civil rights and civil liberties. The following Part details some key harm mitigation strategies.

Part 2: The Regulation of ALPRs

1. Legislation should specify how ALPRs may and may not be used.

Although proponents often cite instances in which ALPRs have been used to solve serious crimes and locate missing persons, in many other cases ALPR use has minimal benefit and could even prove harmful. In some jurisdictions, ALPRs have been used to apprehend undocumented immigrants, investigate low-level non-violent offenses, and/or generate fines and fees revenue. These practices often are inequitable and can diminish trust in law enforcement, undermining public safety.

For this reason, legislation should make clear which uses for ALPRs are permitted and which are prohibited. For example, legislation might provide as follows:

(A) ***Non-investigative purposes.*** Agencies may use ALPRs and ALPR data for the following non-investigative purposes:
   1. Performing weigh station duties;
   2. Monitoring or maintaining an agency's own vehicles or equipment;
   3. Assisting in the control of access to a secured area; or
   4. Collecting electronic tolls.

(B) ***Investigative purposes.*** Agencies may use ALPR hotlists and access ALPR historical data for the following investigative purposes:
   1. Pursuing information relevant to an ongoing criminal investigation of a felony, violent crime, or terrorist act;
   2. Apprehending an individual with an outstanding felony warrant;
   3. Locating a missing or endangered person; or
   4. Locating a lost or stolen vehicle.

(C) Agencies shall not use ALPRs or ALPR data for any purpose not expressly authorized in this Section.

Additional provisions relating to offense-type limitations can be found in Section III of our Model ALPR Statute.

2. Legislation should include safeguards to protect against false positive ALPR alerts.

On several occasions, hotlist alerts generated by ALPRs have led to wrongful traffic stops. There are a few reasons why this occurs. First, if hotlists are not updated regularly, they can come to contain outdated or "stale" information. Second, because some states use similar numbering schemes for license plates, the same license

plate number could be assigned to different vehicles in different states, leading to erroneous alerts. Third, the use of partially obscured or non-standard license plates can result in plate misreads.

Policing agencies should be required to ensure that ALPR hotlists are kept up-to-date, and officers should be required to confirm visually the information about a vehicle before conducting a stop. Legislation might provide as follows:

> (A) An agency shall update all hotlists on a daily basis and each time that new bulletins are issued or canceled.
>
> (B) Prior to stopping a vehicle on the basis of a hotlist alert, a law enforcement officer shall visually confirm that the license plate number of the vehicle and the state from which the license plate was issued match the information in the ALPR alert.

Additional provisions relating to hotlists can be found in Section IV of our Model ALPR Statute.

3. Legislation should restrict how police use ALPR data to track the locations and movements of vehicles.

Stored ALPR data ("historical data") can be used by police in a variety of ways. Police can use historical data for vehicle identification — for example, finding all vehicles which match a witness's description. Historical data also can be used to determine the location of a known vehicle. Or, it can be used to track a vehicle's movements over time.

The use of ALPRs to track vehicle movements has especially significant implications for individual privacy. As the Supreme Court has observed in the context of GPS and cell-phone tracking, location data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (cleaned up).

For this reason, legislation should include procedural safeguards around the use of historical data. This is especially crucial when ALPR data is being used to track a vehicle's locations or movements. Legislation might permit police to use ALPR data to determine a vehicle's present or recent location, but only for narrow, specified purposes, and with clear limits on how much data may be accessed. When police

seek to access ALPR data to track a vehicle's movements over time, stronger restrictions may be warranted. For example, legislation might provide as follows:

(A) ***Use of historical data to determine the present or recent location of a known vehicle.*** An agency may search recent historical data, no older than six hours, to assist in effectuating an arrest, rendering aid to a missing or endangered person, or recovering a lost or stolen vehicle.

(B) ***Use of historical data to track the movements of a vehicle over time.*** An agency may access historical data to track the movements of a vehicle over time only in the following circumstances:

1. Upon issuance of a warrant by a court of competent jurisdiction authorizing such access based upon probable cause that the data is relevant and material to an ongoing criminal investigation; or
2. Where officers have probable cause that the data is relevant and material to an ongoing criminal investigation and exigent circumstances justify accessing the data without first obtaining a warrant.

The six-hour limitation is meant to ensure that police may access only the most recent ALPR data in attempting to determine where a vehicle is presently located; this limit can be adjusted upwards or downwards as policymakers see fit. Understand, however, that because vehicles are mobile, the six-hour window seems a reasonable one. Notably, these provisions are intended to address how ALPR data may be accessed, not how long ALPR data may be retained (retention is addressed in the following section).

Additional provisions relating to the use of historical data can be found in Section IV of our Model ALPR Statute.

4. Legislation should limit how long agencies may retain historical data.

In some jurisdictions, historical data is subject to a "retention period" which specifies how long ALPR data may be held by the agency before it must be deleted. Retention periods serve to limit the amount of historical data that police can access. Without a retention period, agencies could aggregate vast quantities of data on individuals' locations and movements and hold this information permanently.

This type of data retention, and the long-term tracking that it enables, raises profound privacy concerns. Consequently, many states have implemented retention

periods, which range from weeks to years. Some jurisdictions, such as New Hampshire, functionally prohibit the retention of historical data altogether.

To limit how long agencies may retain ALPR data, while ensuring that valuable evidence is not lost due to deletion, policymakers should consider the use of a "data trust." Under this approach, agencies are subject to a limited retention period, but have the option of transferring data to a state agency or some other entity for longer-term storage. If police seek to access data in longer-term storage, they should be required to obtain a warrant or court order.

The following example sets the retention period at seven days and names the State Attorney General as the holder of the data — although both of these might vary depending on feasibility and the specific needs of the jurisdiction:

> (A) An agency shall permanently destroy ALPR data no later than [seven] days after it is collected, unless such data is evidence that is stored in a casefile.
>
> (B) An agency may transfer ALPR data to [the State Attorney General or designee] within seven days of its collection. [The State Attorney General or designee] shall securely store such data for a period of one year.
>
> (C) An agency that seeks to access ALPR data in the possession of [the State Attorney General or designee] shall apply for a warrant authorizing such access in a court of competent jurisdiction. The court shall issue the warrant upon the applicant's showing of probable cause that the requested data is relevant and material to an ongoing criminal investigation, and the applicant's certification that all practicable steps will be taken to minimize access to or use of any data that is not relevant or material to the investigation.

Additional provisions relating to data retention and data trusts can be found in Sections V and VI of our Model ALPR Statute.

5. Legislation should set rules around how agencies share ALPR data.

Many ALPR vendors have developed features which enable police to share data with other agencies. Often, agencies seek to share data with specific agencies in neighboring or nearby jurisdictions. Many agencies also participate in regional, statewide, or national ALPR databases, through which dozens or hundreds of agencies can share and access ALPR data.

This data-sharing can potentially undermine accountability in two ways. First, even if a jurisdiction enacts stringent rules regulating an agency's use of ALPR data, there is no guarantee that those rules will be followed by other agencies with whom this data has been shared. Second, individuals may have no practical way of knowing which external agencies are accessing the data collected by their local policing agency, and for what purpose.

For these reasons, agencies should be required to disclose any sharing of ALPR data and to enter into publicly-available data-sharing agreements. Legislation might provide as follows:

(A) Agencies shall not share ALPR data or access to ALPR data with any private entity.

(B) Agencies shall not share ALPR data or access to ALPR data with another public agency unless both agencies have entered into a publicly-available data-sharing agreement, which shall provide that:

1. The agency receiving ALPR data or access to ALPR data will comply with all laws, regulations, and policies pertaining to such data that are applicable to the agency sharing the ALPR data or access to ALPR data;
2. If the agency receiving ALPR data or access to ALPR data violates any laws, regulations, or policies relating to such data, all sharing of ALPR data or access to ALPR data between the agencies shall immediately cease;
3. Each agency will publish and maintain a public list containing the specific offenses or incident types for which shared ALPR data may be used; and
4. A record of any data shared or received will be included in the audit logs of both agencies.

The provision restricting the sharing of data with private entities is intended to address situations in which police have shared data with entities such as private towing companies. Additional provisions relating to private-public data-sharing can be found below. More information about data-sharing in general can be found in Section VI of our Model ALPR Statute.

6. Legislation should restrict the use of analytics.

As discussed above, ALPR vendors are developing a variety of novel analytics. Some of these features claim to automatically detect casing activity or other suspicious behavior. Notably, a feature developed by multiple vendors known as "convoy analysis" is intended to identify associations between vehicles.

The use of these analytics raises a litany of concerns. To start, there is little evidence supporting the efficacy of ALPRs in general; there is even less supporting the efficacy of these new analytics. The touted benefits remain unproven. At the same time, errors could have significant consequences, including unwarranted police contact and wasted officer resources. Moreover, the use of these analytics could have profound impacts on individual privacy — for example, although the purported purpose of convoy analysis is to find accomplices by detecting vehicles that travel together to commit crimes, it is possible this tool could be used to identify an individual's friends, family members, romantic partners, and other associates.

Until more has been done to understand the efficacy of these analytics and attendant ethical risks, regulation should restrict their use. Legislation might provide:

> (A) No [AGENCY] ALPR user shall access any feature which (1) identifies or seeks to identify associations between different vehicles, (2) predicts future crimes or patterns of movement or conduct, or (3) detects anomalous, suspicious, or criminal conduct.

Additional provisions relating to analytics can be found in Section IV of our Model ALPR Statute.

7. Legislation should limit police access to privately-owned ALPRs.

As discussed, some vendors such as Flock market their ALPRs to a variety of private entities, including homeowner associations, universities, and private businesses. Nearly all of Flock's private users share access to their ALPR data with their local policing agency. This private-public data-sharing allows agencies to dramatically increase their surveillance capabilities at no cost and without any public debate.

To address this, lawmakers should regulate how police access privately-owned ALPRs, with a focus on ensuring that there is meaningful public engagement around long-term or ongoing data-sharing. Legislation might provide:

> (A) Agencies shall not access any privately-owned ALPR or ALPR network, or any data derived therefrom, unless:
>
> 1. An agency user has requested access to a privately-owned ALPR or ALPR network, or data derived therefrom, on a temporary basis not to exceed twenty-four hours in any thirty-day period;

2. Circumstances involving a serious risk of death or injury to an individual exist and the Chief of the agency has authorized access to a privately-owned ALPR or ALPR network, or data derived therefrom, for a period of up to seven days; or
3. The agency has provided notice to the public of its intent to access a privately-owned ALPR or ALPR network, or data derived therefrom, for a period longer than seven days or on an ongoing basis, and has provided an opportunity for public comment at a hearing held in accordance with [State Open Meeting Law].

For information about police use of privately-owned surveillance, see our model lateral surveillance statute.

8. Legislation should require agencies to be transparent about their use of ALPRs.

Transparency is the foundation of democratic governance. Without adequate information, the public cannot have informed opinions, and legislatures cannot make informed decisions. Yet policing agencies often fail to disclose basic information about their use of ALPRs, including how long data is retained and with whom data is shared.

Legislation should require agencies to disclose various information about their ALPR use. Compliance with such transparency requirements can be facilitated through the use of "transparency portals," which are publicly-accessible webpages that some ALPR vendors offer to agency customers at no additional cost (such as this one, used by the Piedmont Police Department). Agencies should be required to enable these portals or to provide equivalent information through another means. Legislation might provide as follows:

A. "Transparency Portal" shall mean a publicly-accessible online webpage disclosing information about an agency's use of ALPRs.
B. An agency using ALPRs shall disclose the following information through a Transparency Portal or through another means:
    1. The agency's ALPR policy;
    2. The agency's retention period for ALPR data;
    3. The total number of ALPRs in use by the agency;
    4. Each agency or other organization with access to the agency's ALPR data;
    5. Each ALPR hotlist in use by the agency;

6. The total number of vehicles detected by the agency's ALPRs in the previous thirty days;
7. The total number of hotlist alerts generated by the agency's ALPRs in the previous thirty days;
8. The total number of searches of ALPR historical data conducted by the agency in the previous thirty days; and
9. The agency's audit logs for the previous thirty days.

Additional provisions relating to transparency can be found in Section VII of our Model ALPR Statute.

9. Legislation should require documentation of ALPR searches.

ALPR users should be required to record the specific reasons for each search of historical data. This serves both to deter misuse and to facilitate auditing and reporting. (Some vendors, such as Flock, already prompt users for this information in the search interface.) Legislation might provide as follows:

(A) For each search of ALPR data, an agency user shall record the following information:
   1. The case number associated with the search, if one exists;
   2. The type of incident or offense associated with the search; and
   3. For searches of a particular vehicle, the specific reasons why the user believes the vehicle to be relevant to the incident under investigation.

(B) On a monthly basis, an agency using ALPRs shall publish, on its website or the Transparency Portal, the total number of searches of historical data broken down by offense and/or incident type.

Additional provisions relating to audit logs can be found in Section VII of our Model ALPR Statute.

10. Legislation should require routine audits of ALPR use.

Legislation should institute auditing procedures to ensure that agency use of ALPRs complies with applicable law. Such auditing should be conducted on a routine basis and the results of all audits should be disclosed publicly. Legislation might provide as follows:

(A) The State Attorney General or designee shall audit each agency that uses an ALPR or ALPR data annually for compliance with all applicable laws and policies.

(B) An agency that is being audited shall provide to the State Attorney General or designee access to any ALPR device, any ALPR data, any system for accessing ALPR data, and any records of ALPR or ALPR data use.

(C) The State Attorney General shall issue a public report with the results of each audit.

(D) If the State Attorney General determines that there is a pattern of substantial noncompliance with this Act by an agency, the agency shall immediately suspend use of all ALPRs and ALPR data until the State Attorney General has determined that the agency has taken sufficient action to remedy such noncompliance.

Additional provisions relating to auditing can be found in Section VIII of our Model ALPR Statute.

11. Legislation should prohibit agencies from bulk-downloading ALPR data.

Many agencies use ALPR systems that process and store data in the cloud. A key advantage of this approach is that it helps to ensure the effectiveness of vendor safeguards. For example, Flock ALPR data is deleted automatically after thirty days — because the data is held in Flock's cloud, Flock can delete this data itself with no action required on the user's part. Likewise, Flock requires users to provide a reason for searches of historical data; it can do so because Flock ultimately controls access to the data.

Agencies seeking to evade such restrictions might download ALPR data in bulk, taking it outside of the vendor's system. For this reason, agencies should be prohibited from downloading ALPR data unless there is reason to believe that the particular data sought is relevant to an investigation. Legislation might provide as follows:

(A) ALPR data stored on a vendor's cloud server shall not be copied, downloaded, or otherwise transferred from the cloud server unless reasonable suspicion exists that such data is relevant to an active investigation.

Additional provisions relating to data retention can be found in Sections V and VI of our Model ALPR Statute.

* * *

This guide has outlined potential strategies to regulate police use of ALPRs. For more information about ALPRs, please see our report on ALPRs and our model ALPR statute. For information about police use of privately-owned surveillance, see our model lateral surveillance statute.